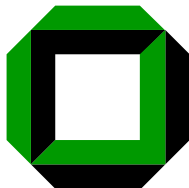


# *Formale Systeme*

Prof. Dr. Bernhard Beckert

Fakultät für Informatik  
Universität Karlsruhe (TH)



Winter 2008/2009



# *Modale Logik*

Im Unterschied zur klassischen Logik,  
in der nur die Wahrheit einer Aussage von Bedeutung ist,  
spielt in der modalen Logik  
die Art und Weise, der Modus,  
in der eine Aussage wahr ist eine große Rolle.



# Modale Logik

Im Unterschied zur klassischen Logik,  
in der nur die Wahrheit einer Aussage von Bedeutung ist,  
spielt in der modalen Logik  
die Art und Weise, der Modus,  
in der eine Aussage wahr ist eine große Rolle.

Eine Aussage ist

- notwendigerweise wahr, zufälligerweise wahr



# Modale Logik

Im Unterschied zur klassischen Logik,  
in der nur die Wahrheit einer Aussage von Bedeutung ist,  
spielt in der modalen Logik  
die Art und Weise, der Modus,  
in der eine Aussage wahr ist eine große Rolle.

Eine Aussage ist

- notwendigerweise wahr, zufälligerweise wahr
- heute, gestern oder morgen wahr



# Modale Logik

Im Unterschied zur klassischen Logik,  
in der nur die Wahrheit einer Aussage von Bedeutung ist,  
spielt in der modalen Logik  
die Art und Weise, der Modus,  
in der eine Aussage wahr ist eine große Rolle.

Eine Aussage ist

- notwendigerweise wahr, zufälligerweise wahr
- heute, gestern oder morgen wahr
- wird geglaubt, gehört zum Wissen einer Person



# Modale Logik

Im Unterschied zur klassischen Logik, in der nur die Wahrheit einer Aussage von Bedeutung ist, spielt in der modalen Logik die Art und Weise, der Modus, in der eine Aussage wahr ist eine große Rolle.

Eine Aussage ist

- notwendigerweise wahr, zufälligerweise wahr
- heute, gestern oder morgen wahr
- wird geglaubt, gehört zum Wissen einer Person
- ist vor/nach einer Aktion wahr, nach Ausführung eines Programms wahr.



## *Einführungsbeispiel*

*Drei Weisen werden Hüte aufgesetzt, jedem genau einer. Die Hüte sind entweder weiß oder schwarz, und jedem ist bekannt, daß mindestens ein schwarzer Hut mit dabei ist. Jeder Beteiligte sieht, welche Hüte die anderen beiden aufsitzen haben und soll erschließen, welchen Hut er aufsitzen hat, natürlich ohne in einen Spiegel zu schauen, den Hut abzunehmen oder ähnliches. Nach einer Weile sagt der erste Weise: „Ich weiß nicht, welchen Hut ich aufhabe.“ Nach einer weiteren Pause des Nachdenkens sagt der zweite: „Ich weiß auch nicht, welchen Hut ich aufhabe.“ „Dann“, sagt der dritte, „weiß ich, daß ich einen schwarzen Hut aufhabe.“*



# Mögliche Welten

w  
b  
w

b  
b  
w

b  
w  
w

w  
b  
b

b  
b  
b

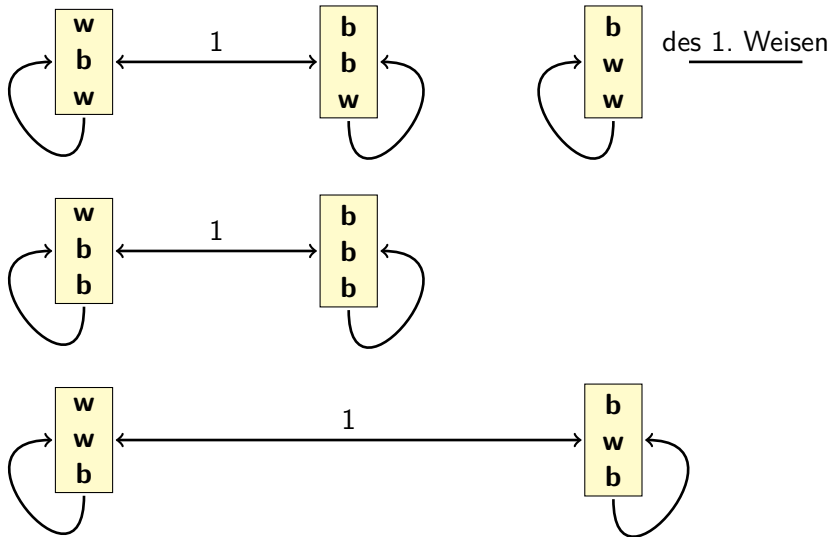
w  
w  
b

b  
w  
b

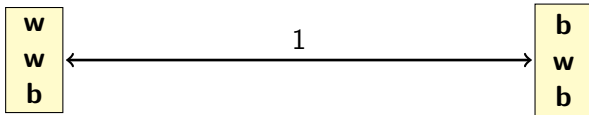
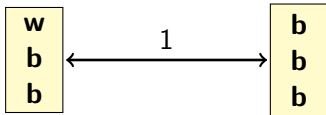




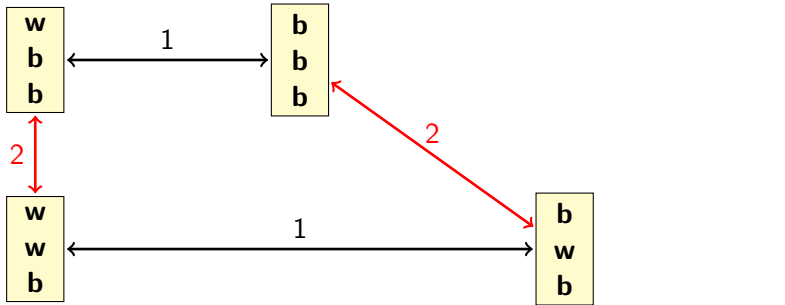
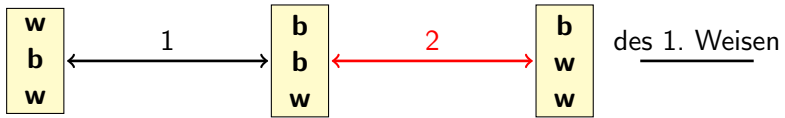
## Mögliche Welten



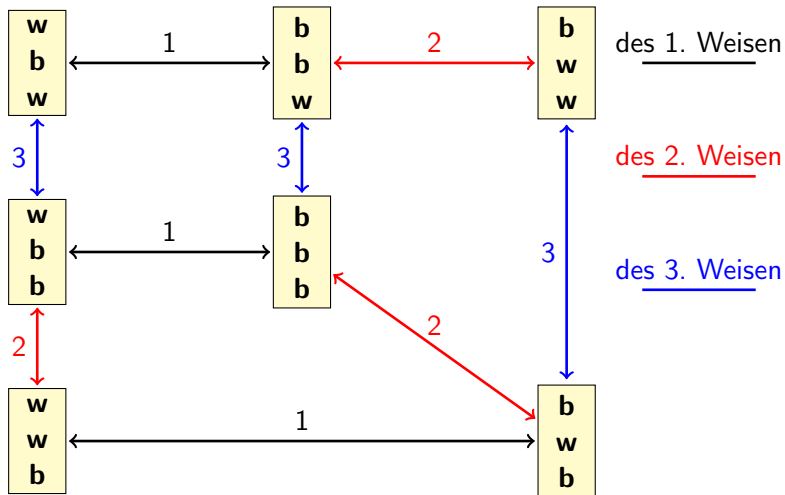
# Mögliche Welten



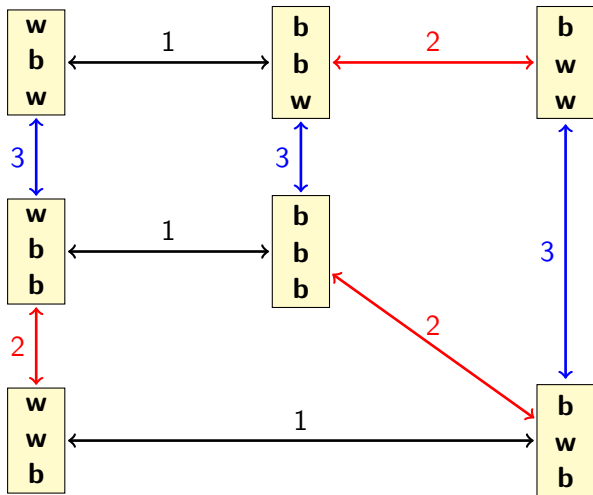
# Mögliche Welten



# Mögliche Welten



# Erster Schritt

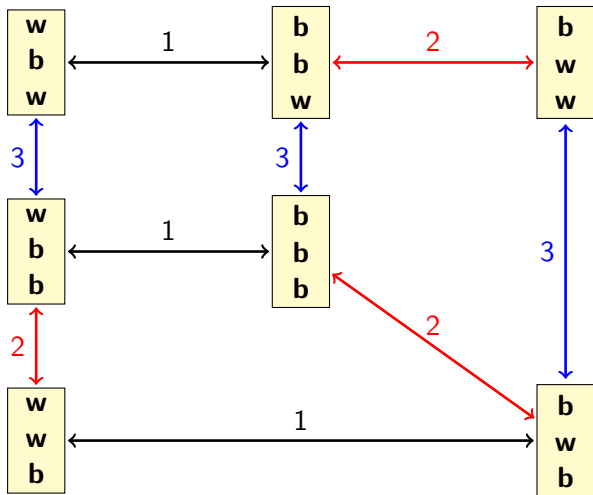


## Erster Schritt

Da der erste  
Weise die  
Farbe seines  
Huts nicht  
erschließen  
kann, kann  
die Welt

(b w w)

nicht auftre-  
ten.

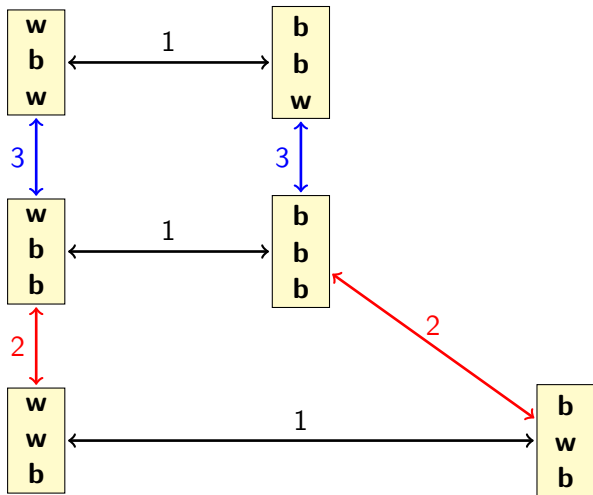


## Erster Schritt

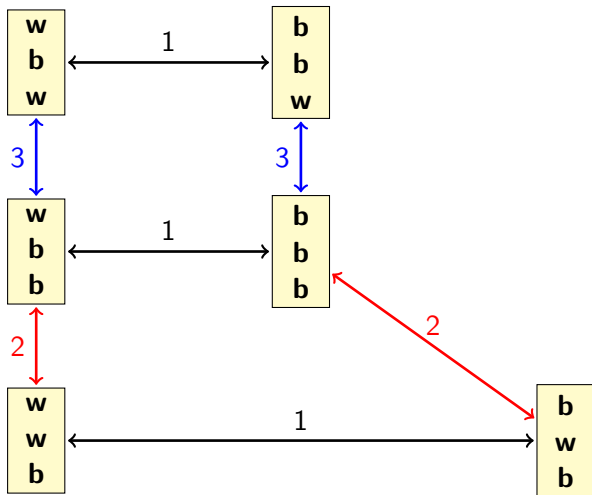
Da der erste  
Weise die  
Farbe seines  
Huts nicht  
erschließen  
kann, kann  
die Welt

(**b w w**)

nicht auftre-  
ten.



## Zweiter Schritt



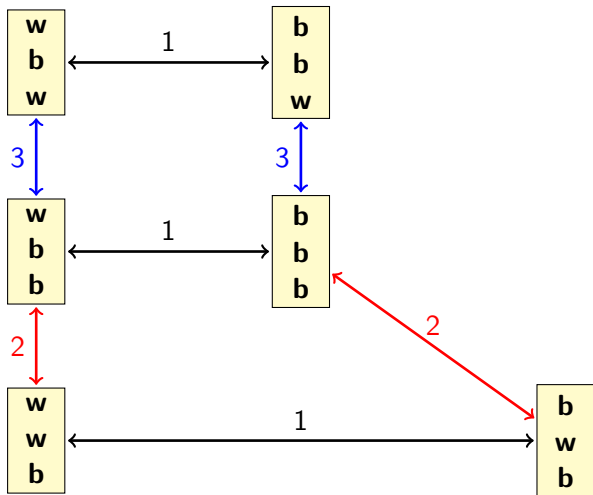


## Zweiter Schritt

Da der zweite Weise die Farbe seines Huts nicht weiß, können die Welten

(w b w)  
(b b w)

nicht auftreten.

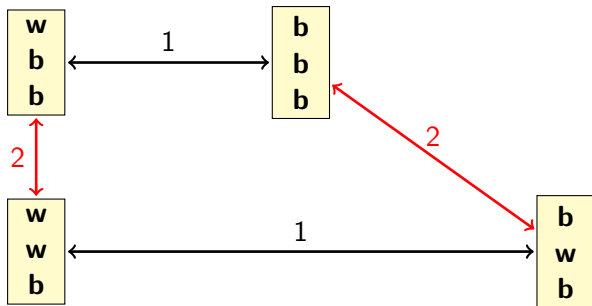


## Zweiter Schritt

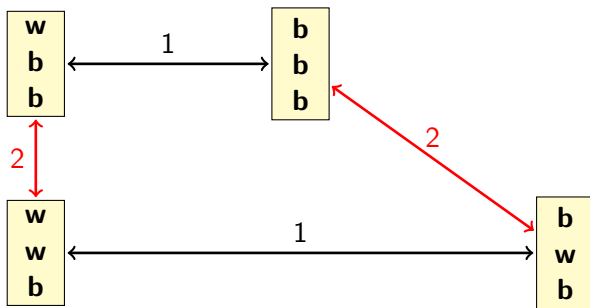
Da der zweite Weise die Farbe seines Huts nicht weiß, können die Welten

(w b w)  
(b b w)

nicht auftreten.



## Letzter Schritt



In den noch verbleibenden möglichen Welten hat der dritte Weise stets einen schwarzen Hut auf.



# *Modallogische Grundbegriffe*

in der Welt  $s$  weiß der  $i$ -te Weise die Aussage  $A$



## *Modallogische Grundbegriffe*

in der Welt  $s$  weiß der  $i$ -te Weise die Aussage  $A$

genauer

in jeder für den  $i$ -ten Weisen von  $s$  aus gesehen möglichen Welt gilt  $A$ .



## Modallogische Grundbegriffe

in der Welt  $s$  weiß der  $i$ -te Weise die Aussage  $A$

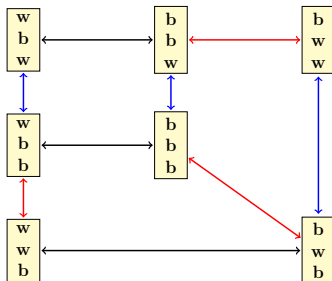
genauer

in jeder für den  $i$ -ten Weisen von  $s$  aus gesehen möglichen Welt gilt  $A$ .

$$s \models \Box_i A$$



# Beispiele



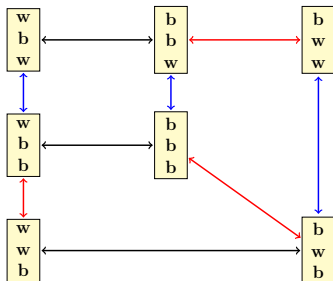
Die Boolesche Variable

$B_i$

ist wahr in der Welt  $s$ , wenn in  $s$  der  $i$ -te Weise einen schwarzen Hut aufhat. Entsprechend für  $W_j$ .



## Beispiele



Die Boolesche Variable

$B_i$

ist wahr in der Welt  $s$ , wenn in  $s$  der  $i$ -te Weise einen schwarzen Hut aufhat. Entsprechend für  $W_j$ .

$$(w, b, w) \models \Box_1 B_2 \quad (w, b, w) \models \Box_1 W_3$$

$$\text{nicht } (w, b, w) \models \Box_1 B_1 \quad (b, w, w) \models \Box_1 B_1$$





## *Zweites Einführungsbeispiel*

### *Konfliktfreie Zugriffskontrolle*

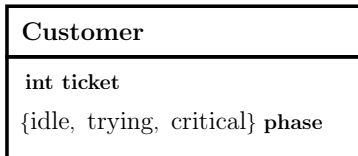
Der *Bakery*-Algorithmus ist benannt nach der in manchen amerikanischen Bäckereien (und manchen deutschen Behörden, Arztpraxen etc.) üblichen Methode, daß der Kunde beim Eintritt eine Nummer zieht und dann an die Reihe kommt, wenn seine Nummer die kleinste unter den noch Wartenden ist.

So ist sichergestellt, daß jeder schließlich an die Reihe kommt und kein Streit darüber entsteht, wer als nächster drankommt.



## Prozesse

Die Prozesse, die am *Bakery*-Algorithmus teilnehmen, können wir uns als Instanzen der Klasse *Customer* vorstellen.



## Zustandsübergangsregeln

---

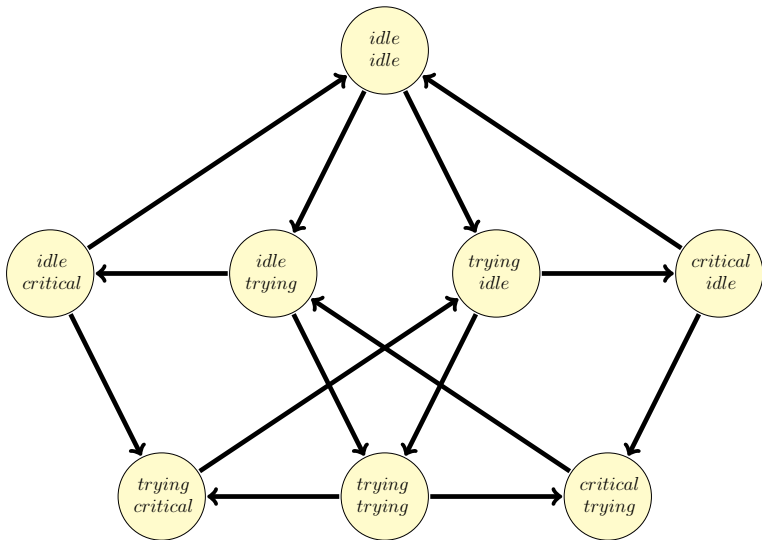
try:	if phase = idle	then
		phase := trying
		ticket := max of all other tickets + 1
enter:	if phase = trying and ticket less than all other tickets	then
		phase := critical
leave	phase = critical	then
		phase := idle
		ticket := 0

---

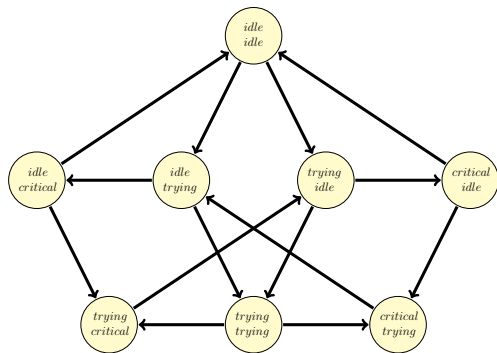


# Endlicher Automat

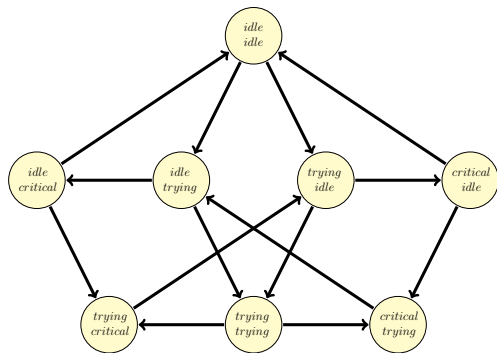
Zwei Prozesse, keine Nummern



# Eigenschaften



# Eigenschaften

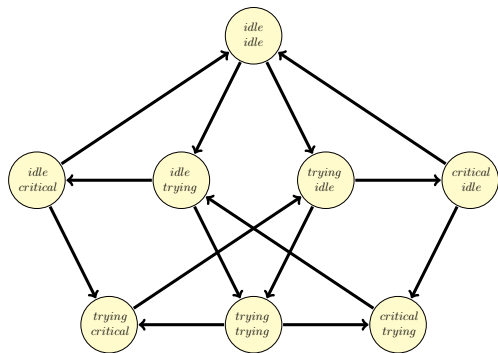


## Notation

Die Booleschen Variablen  $i.idle$ ,  $i.trying$ ,  $i.critical$  seien wahr in einem Zustand  $s$ , wenn in  $s$  der  $i$ -te Prozess in der angegebenen Phase ist.



## Eigenschaften



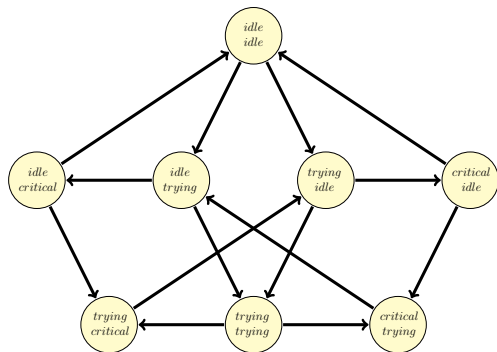
### Notation

Die Booleschen Variablen  $i.idle$ ,  $i.trying$ ,  $i.critical$  seien wahr in einem Zustand  $s$ , wenn in  $s$  der  $i$ -te Prozess in der angegebenen Phase ist.

Ist der 1. Prozess in der *trying* Phase, dann kann er in höchstens zwei Schritt in die kritische Phase gelangen.



## Eigenschaften



### Notation

Die Booleschen Variablen  $i.idle$ ,  $i.trying$ ,  $i.critical$  seien wahr in einem Zustand  $s$ , wenn in  $s$  der  $i$ -te Prozess in der angegebenen Phase ist.

Ist der 1. Prozess in der *trying* Phase, dann kann er in höchstens zwei Schritt in die kritische Phase gelangen.

$$1.trying \rightarrow (\diamond 1.critical \vee \diamond\diamond 1.critical)$$





# Formeln der Modalen Aussagenlogik

## Definition

1.  $\mathbf{1}, \mathbf{0} \in mFor0_{\Sigma}$



# Formeln der Modalen Aussagenlogik

## Definition

1.  $\mathbf{1}, \mathbf{0} \in mFor0_{\Sigma}$
2. Jede aussagenlogische Variable  $P \in \Sigma$  ist in  $mFor0_{\Sigma}$ .



# Formeln der Modalen Aussagenlogik

## Definition

1.  $\mathbf{1}, \mathbf{0} \in mFor0_{\Sigma}$
2. Jede aussagenlogische Variable  $P \in \Sigma$  ist in  $mFor0_{\Sigma}$ .
3. Mit  $A, B \in mFor0_{\Sigma}$  liegen ebenfalls in  $mFor0_{\Sigma}$ :  
 $\neg A, A \wedge B, A \vee B, A \rightarrow B$ .



# Formeln der Modalen Aussagenlogik

## Definition

1.  $\mathbf{1}, \mathbf{0} \in mFor0_{\Sigma}$
2. Jede aussagenlogische Variable  $P \in \Sigma$  ist in  $mFor0_{\Sigma}$ .
3. Mit  $A, B \in mFor0_{\Sigma}$  liegen ebenfalls in  $mFor0_{\Sigma}$ :  
 $\neg A, A \wedge B, A \vee B, A \rightarrow B$ .
4. Mit  $A \in mFor0_{\Sigma}$  liegen ebenfalls in  $mFor0_{\Sigma}$ :  
 $\square A$  (gelesen als „Box A“, „notwendig A“)  
 $\diamond B$  (gelesen als „Diamond A“, „möglich A“)



# Kripke-Strukturen

## Definition

Sei  $\Sigma$  eine Menge aussagenlogischer Variablen.

Eine Kripke-Struktur

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

über  $\Sigma$  besteht aus:

- $S$  eine nichtleere Menge  
(die Menge von *Zuständen* oder möglichen *Welten*)



# Kripke-Strukturen

## Definition

Sei  $\Sigma$  eine Menge aussagenlogischer Variablen.

Eine Kripke-Struktur

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

über  $\Sigma$  besteht aus:

- $S$  eine nichtleere Menge  
(die Menge von *Zuständen* oder möglichen *Welten*)
- $R \subseteq S \times S$  (die Zugänglichkeitsrelation)



# Kripke-Strukturen

## Definition

Sei  $\Sigma$  eine Menge aussagenlogischer Variablen.

Eine Kripke-Struktur

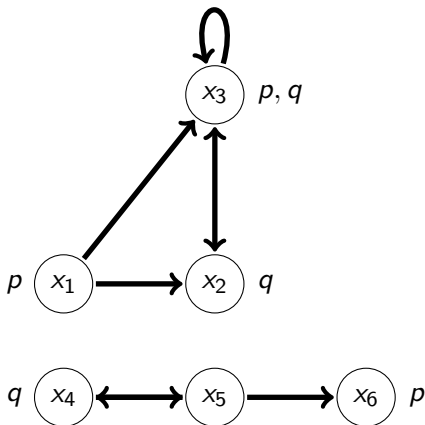
$$\mathcal{K} = (S, R, I)$$

über  $\Sigma$  besteht aus:

- $S$  eine nichtleere Menge  
(die Menge von *Zuständen* oder möglichen *Welten*)
- $R \subseteq S \times S$  (die Zugänglichkeitsrelation)
- $I: (\Sigma \times S) \rightarrow \{W, F\}$  (Interpretation der AL-Variablen)

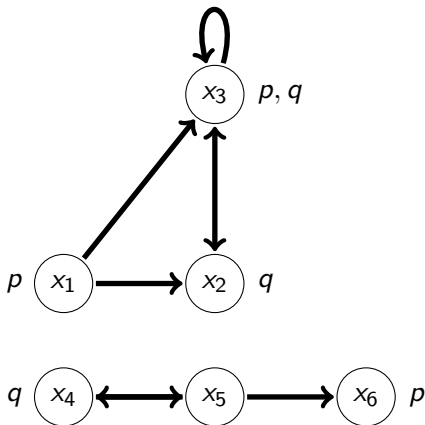


# Beispiel einer Kripke-Struktur aus Huth and Ryan





# Beispiel einer Kripke-Struktur aus Huth and Ryan

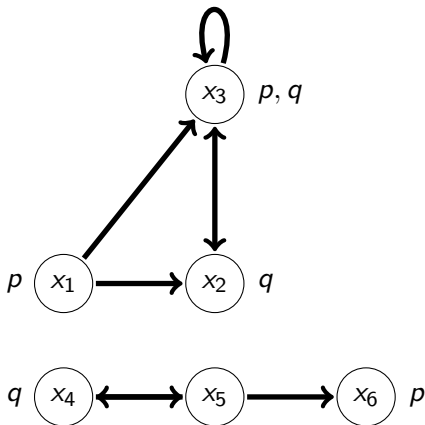


Menge der Zustände  $S = \{x_1, x_2, x_3, x_4, x_5, x_6\}$



# Beispiel einer Kripke-Struktur

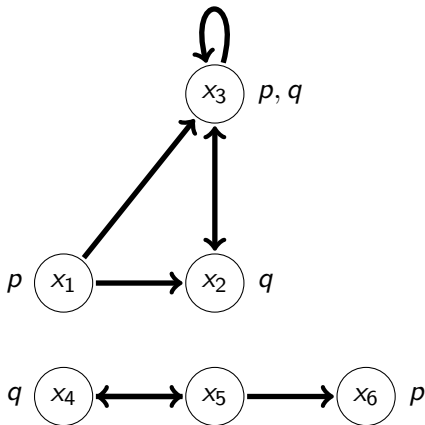
aus Huth and Ryan



$$R = \{(x_1, x_2), (x_1, x_3), (x_2, x_3), (x_3, x_2), (x_3, x_3), (x_4, x_5), (x_5, x_4), (x_5, x_6)\}$$



# Beispiel einer Kripke-Struktur aus Huth and Ryan



$$I(p, x_1) = I(p, x_3) = I(p, x_6) = 1$$

$$I(q, x_2) = I(q, x_3) = I(q, x_4) = 1, \text{ sonst } I(x, s) = 0$$



## Auswertung von Formeln

Sei  $\mathcal{K} = (S, R, I)$  eine Kripke-Struktur. Wir definieren für jeden Zustand  $s \in S$ , wann eine Formeln aus  $mFor0$  in  $s$  wahr ist.

### Definition

$$\begin{aligned} val_s(\Box A) &= \begin{cases} W & \text{falls für alle } s' \in S \text{ mit } sRs' \\ & \text{gilt } val_{s'}(A) = W \\ F & \text{sonst} \end{cases} \\ val_s(\Diamond A) &= \begin{cases} W & \text{falls ein } s' \in S \text{ existiert mit } sRs' \\ & \text{und } val_{s'}(A) = W \\ F & \text{sonst} \end{cases} \end{aligned}$$



## *Notation*

$\mathcal{K} = (S, R, I)$  eine Kripke-Struktur,

$s \in S$ ,

$F$  eine modale Formel



## Notation

$\mathcal{K} = (S, R, I)$  eine Kripke-Struktur,

$s \in S$ ,

$F$  eine modale Formel

$$(\mathcal{K}, s) \models F \Leftrightarrow \text{val}_s(F) = W$$

wenn  $\mathcal{K}$  aus dem Kontext bekannt ist auch:

$$s \models F \Leftrightarrow \text{val}_s(F) = W$$

$$\mathcal{K} \models F \Leftrightarrow \text{für alle } s \in S \text{ gilt } (\mathcal{K}, s) \models F$$

Gültigkeit in einen Kripke-Rahmen  $(S, R)$  :

$$(S, R) \models F \Leftrightarrow \text{für alle } I \text{ gilt } (S, R, I) \models F$$



## *Saul Aaron Kripke*



Geboren 1940 in Omaha (US)

1. Publikation *A Completeness Theorem in Modal Logic*  
The Journal of Symbolic Logic, 1959

Studium in Harvard, Princeton, Oxford  
und an der Rockefeller University

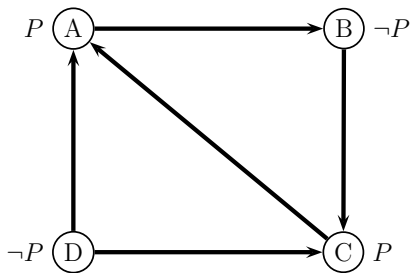
Positionen in Harvard, Rockefeller, Columbia,  
Cornell, Berkeley and UCLA, Oxford

Ab 1977 Professor an der Princeton University

Seit 1998 Emeritus der Princeton University

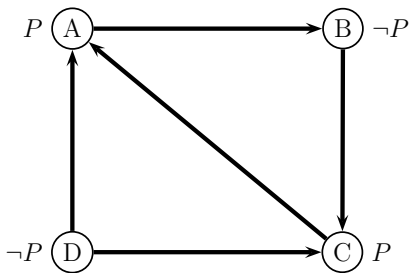


## Beispiel zur Auswertung von Formeln





## Beispiel zur Auswertung von Formeln



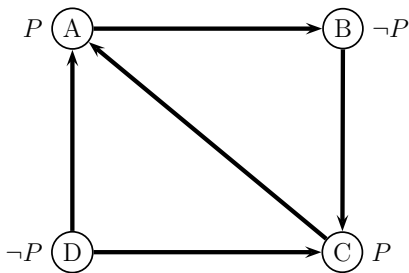
$$(\mathcal{K}, A) \models P \quad (\mathcal{K}, B) \models P \quad (\mathcal{K}, C) \models P \quad (\mathcal{K}, D) \models P$$

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

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



## Beispiel zur Auswertung von Formeln



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



## Logische Folgerung

### Definition

Sei  $A$  eine Formel und  $\Gamma$  eine Menge von Formeln der modalen Aussagenlogik.

$A$  ist eine **logische Folgerung** aus  $\Gamma$

$\Gamma \vdash A$

gdw

für alle Kripke-Strukturen  $\mathcal{K}$  und jede Welt  $s$  von  $\mathcal{K}$  gilt  
wenn  $(\mathcal{K}, s) \models \Gamma$  dann auch  $(\mathcal{K}, s) \models A$

$A$  ist **allgemeingültig** wenn

$\emptyset \vdash A$



## *Allgemeingültige Formeln*

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$



## *Allgemeingültige Formeln*

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2.  $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$



## Allgemeingültige Formeln

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2.  $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$
3.  $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$



## Allgemeingültige Formeln

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2.  $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$
3.  $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$
4.  $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$



## Allgemeingültige Formeln

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2.  $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$
3.  $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$
4.  $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$
5.  $\Box P \leftrightarrow \neg \Diamond \neg P$





## Allgemeingültige Formeln

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2.  $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$
3.  $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$
4.  $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$
5.  $\Box P \leftrightarrow \neg \Diamond \neg P$
6.  $\Diamond(P \vee Q) \leftrightarrow (\Diamond P \vee \Diamond Q)$



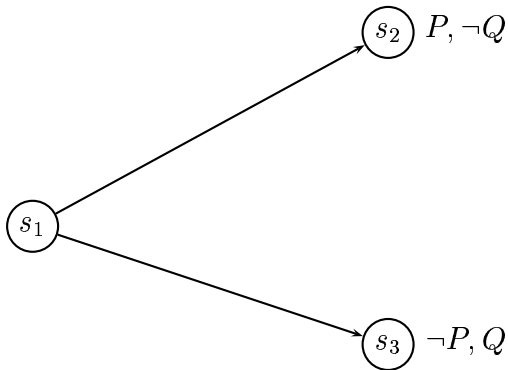
## Allgemeingültige Formeln

1.  $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2.  $(\Box P \wedge \Box(P \rightarrow Q)) \rightarrow \Box Q$
3.  $(\Box P \vee \Box Q) \rightarrow \Box(P \vee Q)$
4.  $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$
5.  $\Box P \leftrightarrow \neg \Diamond \neg P$
6.  $\Diamond(P \vee Q) \leftrightarrow (\Diamond P \vee \Diamond Q)$
7.  $\Diamond(P \wedge Q) \rightarrow (\Diamond P \wedge \Diamond Q)$



*Gegenbeispiel zur Allgemeingültigkeit von*

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



# *Relative Allgemeingültigkeit*

## *Erstes Beispiel*

Die Formel

$$\Box A \rightarrow A$$

ist nicht allgemeingültig.



# *Relative Allgemeingültigkeit*

## *Erstes Beispiel*

Die Formel

$$\Box A \rightarrow A$$

ist nicht allgemeingültig.

Aber



# Relative Allgemeingültigkeit

## Erstes Beispiel

Die Formel

$$\Box A \rightarrow A$$

ist nicht allgemeingültig.

Aber

für alle Kripke-Strukturen  $\mathcal{K} = (S, R, I)$ , so daß  $(S, R)$  eine reflexive Relation ist gilt

$$\mathcal{K} \models \Box A \rightarrow A$$



## *Relative Allgemeingültigkeit*

allgemeingültige Formel

$\Box A \rightarrow A$

Eigenschaft von  $R$

reflexiv



## *Relative Allgemeingültigkeit*

allgemeingültige Formel

Eigenschaft von  $R$

---

$\Box A \rightarrow A$

reflexiv

$\Box A \rightarrow \Box \Box A$

transitiv





## *Relative Allgemeingültigkeit*

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch



## Relative Allgemeingültigkeit

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht



## Relative Allgemeingültigkeit

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht
	für alle $t_1, t_2 \in S$ mit $R(t_1, t_2)$ existiert $t_3 \in S$ mit $R(t_1, t_3)$ und $R(t_3, t_2)$ .



## Relative Allgemeingültigkeit

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht
	für alle $t_1, t_2 \in S$ mit $R(t_1, t_2)$ existiert $t_3 \in S$ mit $R(t_1, t_3)$ und $R(t_3, t_2)$ .
$\Diamond A \rightarrow \Box A$	partiell funktional



## Relative Allgemeingültigkeit

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht für alle $t_1, t_2 \in S$ mit $R(t_1, t_2)$ existiert $t_3 \in S$ mit $R(t_1, t_3)$ und $R(t_3, t_2)$ .
$\Diamond A \rightarrow \Box A$	partiell funktional für alle $s, t_1, t_2 \in S$ mit $R(s, t_1) \wedge R(s, t_2)$ folgt $t_1 = t_2$ .



## Relative Allgemeingültigkeit

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht für alle $t_1, t_2 \in S$ mit $R(t_1, t_2)$ existiert $t_3 \in S$ mit $R(t_1, t_3)$ und $R(t_3, t_2)$ .
$\Diamond A \rightarrow \Box A$	partiell funktional für alle $s, t_1, t_2 \in S$ mit $R(s, t_1) \wedge R(s, t_2)$ folgt $t_1 = t_2$ .
$\Box A \rightarrow \Diamond A$	endlos



## Relative Allgemeingültigkeit

allgemeingültige Formel	Eigenschaft von $R$
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht für alle $t_1, t_2 \in S$ mit $R(t_1, t_2)$ existiert $t_3 \in S$ mit $R(t_1, t_3)$ und $R(t_3, t_2)$ .
$\Diamond A \rightarrow \Box A$	partiell funktional für alle $s, t_1, t_2 \in S$ mit $R(s, t_1) \wedge R(s, t_2)$ folgt $t_1 = t_2$ .
$\Box A \rightarrow \Diamond A$	endlos für jedes $s \in S$ ein $t$ existiert mit $R(s, t)$ .



# Relative Allgemeingültigkeit

## Weitere Beispiele

allgemeingültige Formel	Eigenschaft von $R$
$\Box p \rightarrow p$	reflexiv
$p \rightarrow \Diamond p$	reflexiv
$\Box \Box p \rightarrow \Box p$	reflexiv
$\Box \Diamond p \rightarrow \Diamond p$	reflexiv
$\Box p \rightarrow \Diamond \Box p$	reflexiv
$\Diamond \Diamond p \rightarrow \Diamond p$	transitiv
$\Box p \rightarrow \Box \Box p$	transitiv
$p \rightarrow \Box \Diamond p$	symmetrisch
$\Box \Box p \leftrightarrow \Box p$	reflexiv und transitiv
$\Diamond \Diamond p \leftrightarrow \Diamond p$	reflexiv und transitiv
$\Diamond \Box p \leftrightarrow \Box p$	Äquivalenzrelation
$\Box \Diamond p \leftrightarrow \Diamond p$	Äquivalenzrelation





# *Charakterisierung*

## *Erstes Beispiel*



# Charakterisierung

## Erstes Beispiel

Gilt für einen Kripke-Rahmen  $(S, R)$

für alle  $I$  gilt  $(S, R, I) \models \Box A \rightarrow A$

dann ist

$(S, R)$  reflexiv



## Definition

Sei  $\mathbf{R}$  eine Klasse von Kripke-Rahmen,  
und  $F$  eine Formel der Modallogik.



## Definition

Sei  $\mathbf{R}$  eine Klasse von Kripke-Rahmen,  
und  $F$  eine Formel der Modallogik.

$F$  charakterisiert die Klasse  $\mathbf{R}$  genau dann, wenn für alle Kripke-Rahmen  $(S, R)$  gilt

$$\begin{aligned} &\text{für alle } I \text{ gilt } (S, R, I) \models F \\ &gdw \\ &(S, R) \in \mathbf{R} \end{aligned}$$



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht





## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht
$\Diamond A \rightarrow \Box A$	partiell funktional



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht
$\Diamond A \rightarrow \Box A$	partiell funktional
$\Box A \rightarrow \Diamond A$	



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht
$\Diamond A \rightarrow \Box A$	partiell funktional
$\Box A \rightarrow \Diamond A$	



## *Einige Charakterisierungsergebnisse*

Formel	charakterisierte Eigenschaft
$\Box A \rightarrow A$	reflexiv
$\Box A \rightarrow \Box \Box A$	transitiv
$A \rightarrow \Box \Diamond A$	symmetrisch
$\Box \Box A \rightarrow \Box A$	dicht
$\Diamond A \rightarrow \Box A$	partiell funktional
$\Box A \rightarrow \Diamond A$	endlos



# Grenzen der Charakterisierungstheorie

## Konkretisierung

Sei  $\phi$  eine Formel der Prädikatenlogik in der Signatur  $\Sigma = \{R\}$  und

$$\mathcal{R}_\phi = \{(S, R) \mid (S, R) \models \phi\}$$

*Frage 1* Gibt es zu jedem  $\phi$  eine modallogische Formel  $F$ , so daß die Klasse der Rahmen  $\mathcal{R}_\phi$  charakterisiert?



# Grenzen der Charakterisierungstheorie

## Konkretisierung

Sei  $\phi$  eine Formel der Prädikatenlogik in der Signatur  $\Sigma = \{R\}$  und

$$\mathcal{R}_\phi = \{(S, R) \mid (S, R) \models \phi\}$$

*Frage 1* Gibt es zu jedem  $\phi$  eine modallogische Formel  $F$ , so daß die Klasse der Rahmen  $\mathcal{R}_\phi$  charakterisiert?

*Frage 2* Gibt es zu jeder modallogischen Formel  $F$  eine prädikatenlogische Formel  $\phi$ , so daß  $\mathcal{R}_\phi$  mit der Klasse der durch  $F$  charakterisierten Rahmen zusammenfällt?



# Grenzen der Charakterisierungstheorie

## Antworten

*Antwort 1* Nein

Z.B. für  $\phi = \forall x \neg R(x, x)$  kann die Klasse  $\mathcal{R}_\phi$  nicht durch eine modallogische Formel charakterisiert werden



# Grenzen der Charakterisierungstheorie

## Antworten

*Antwort 1* Nein

Z.B. für  $\phi = \forall x \neg R(x, x)$  kann die Klasse  $\mathcal{R}_\phi$  nicht durch eine modallogische Formel charakterisiert werden

*Antwort 2* Nein

Es gibt modallogische Formel  $F$ , so daß die durch  $F$  charakterisierten Rahmen nicht durch eine prädikatenlogische Formel  $\phi$  axiomatisiert werden kann.





# Entscheidbarkeit modaler Logiken



# *Entscheidbarkeit*

Aus dem Filtrationslemma (siehe Skriptum) folgt:

## Theorem

Jede Menge  $\Gamma$  modallogischer Formeln, die überhaupt ein Modell hat, hat auch ein Modell  $(S, R, I)$ , so dass  $S$  endlich ist, wobei eine obere Schranke für die Größe von  $S$  aus  $\Gamma$  berechnet werden kann.



# Entscheidbarkeit

Aus dem Filtrationslemma (siehe Skriptum) folgt:

## Theorem

Jede Menge  $\Gamma$  modallogischer Formeln, die überhaupt ein Modell hat, hat auch ein Modell  $(S, R, I)$ , so dass  $S$  endlich ist, wobei eine obere Schranke für die Größe von  $S$  aus  $\Gamma$  berechnet werden kann.

## Korollar

Die modale Aussagenlogik **K** ist entscheidbar,



# Entscheidbarkeit

Aus dem Filtrationslemma (siehe Skriptum) folgt:

## Theorem

Jede Menge  $\Gamma$  modallogischer Formeln, die überhaupt ein Modell hat, hat auch ein Modell  $(S, R, I)$ , so dass  $S$  endlich ist, wobei eine obere Schranke für die Größe von  $S$  aus  $\Gamma$  berechnet werden kann.

## Korollar

Die modale Aussagenlogik **K** ist entscheidbar, d.h.

es gibt einen Algorithmus, der für jede Formel  $A$  entscheidet, ob  $A$  eine **K**-Tautologie ist oder nicht.



# Andere Modalitäten



## Informale Interpretationen von $\Box$

$\Box F$
$F$ ist notwendigerweise wahr
$F$ ist zu jedem zukünftigen Zeitpunkt wahr
Ein Agent $a$ glaubt $F$
Ein Agent $a$ weiß $F$
Nach jeder Ausführung des Programms $p$ gilt $F$

Falls erforderlich schreibt man

$$\Box_a F, \quad \Box_p F, \quad [a]F \quad \text{oder} \quad [p]F$$

anstelle von  $\Box F$ .



## Informale Interpretationen von $\diamond$

$\diamond F \equiv \neg \square \neg F$	
$F$ ist notwendigerweise wahr	$F$ ist möglicherweise wahr
$F$ ist zu jedem zukünftigen Zeitpunkt wahr	es gibt einen zukünftigen Zeitpunkt, zu dem $F$ wahr ist.
Ein Agent $a$ glaubt $F$	$F$ ist konsistent mit den Aussagen, die $a$ für wahr hält.
Ein Agent $a$ weiß $F$	$a$ weiß nicht, daß $F$ falsch ist.
Nach jeder Ausführung des Programms $p$ gilt $F$	Es gibt eine Ausführung des Programms $p$ , nach der $F$ wahr ist.



$\Box F$	$\Box F \rightarrow F$ $\Box F \rightarrow \Box \Box F$ $\Box F \rightarrow \Diamond F$ $(\Box(F \rightarrow G) \wedge \Box F) \rightarrow \Box G$ $\Diamond true$
$F$ ist notwendigerweise wahr	
$F$ ist immer wahr	
Ein Agent $a$ glaubt $F$	
Ein Agent $a$ weiß $F$	
Nach jeder Ausführung des Programms $p$ gilt $F$	





$\Box F$	$\Box F \rightarrow F$	$\Box F \rightarrow \Box \Box F$	$\Box F \rightarrow \Diamond F$	$(\Box(F \rightarrow G) \wedge \Box F) \rightarrow \Box G$	$\Diamond true$
$F$ ist notwendigerweise wahr	yes	yes	yes	yes	yes
$F$ ist immer wahr	no	yes	no	yes	no
Ein Agent $a$ glaubt $F$	no	yes	yes	yes	yes
Ein Agent $a$ weiß $F$	yes	yes	yes	yes	yes
Nach jeder Ausführung des Programms $p$ gilt $F$	no	no	no	yes	no

