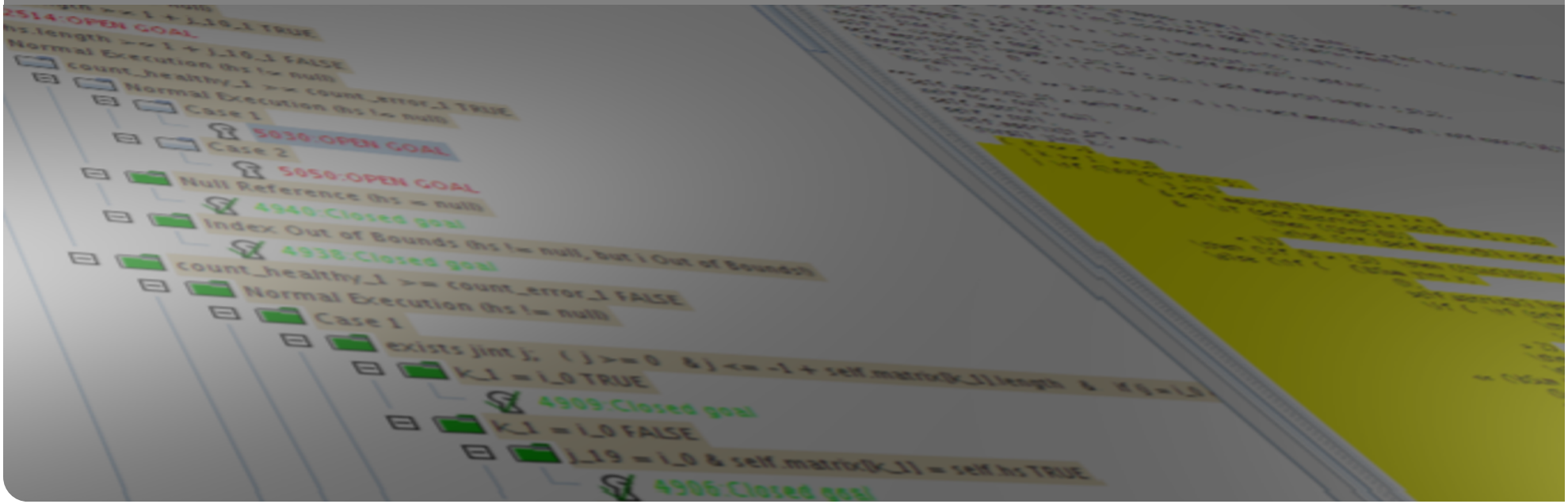
# Formale Systeme

## Prof. Dr. Bernhard Beckert, WS 2017/2018

Modallogik

KIT – Institut für Theoretische Informatik



# 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.**

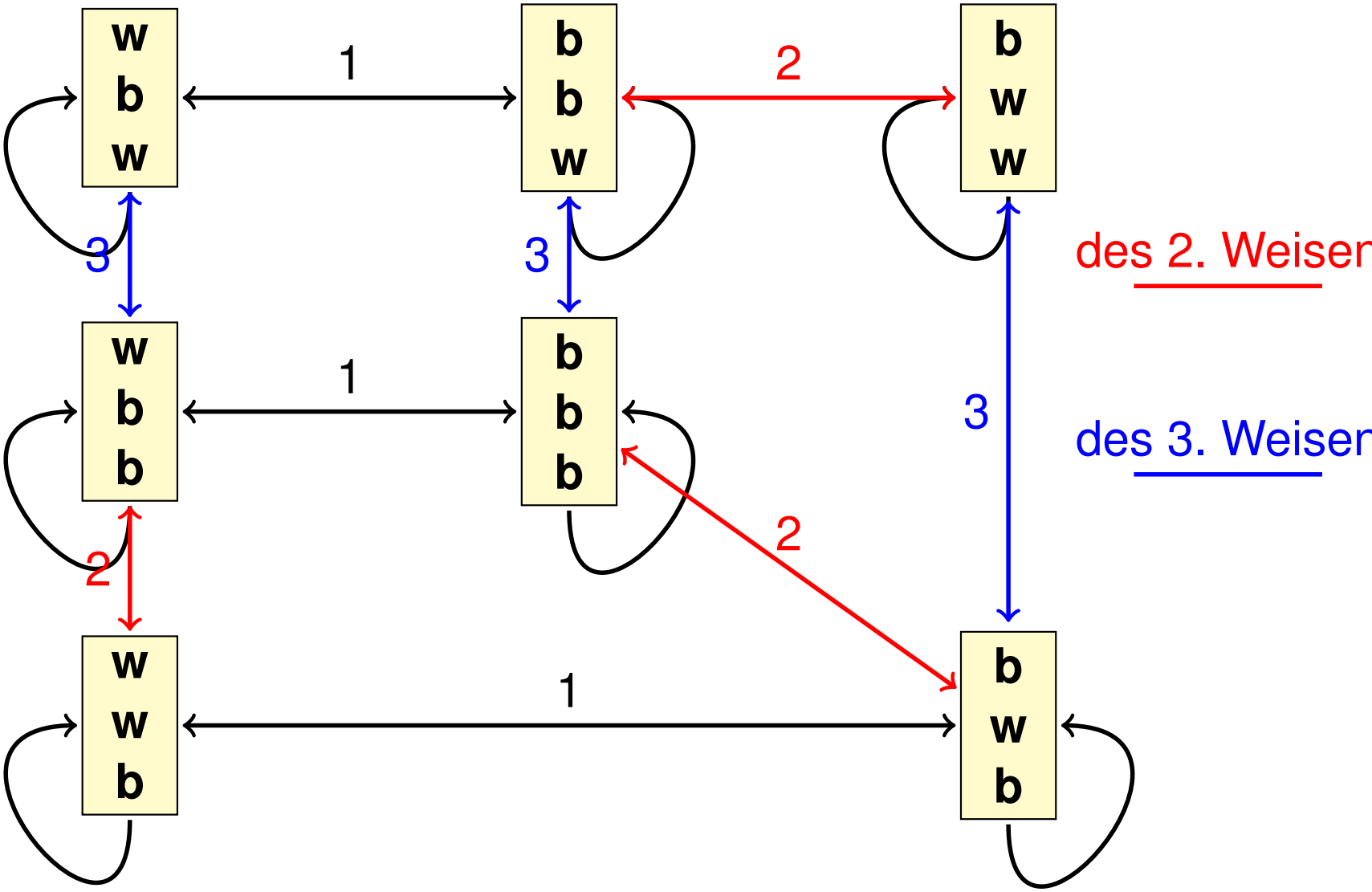
Eine Aussage ist

- 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

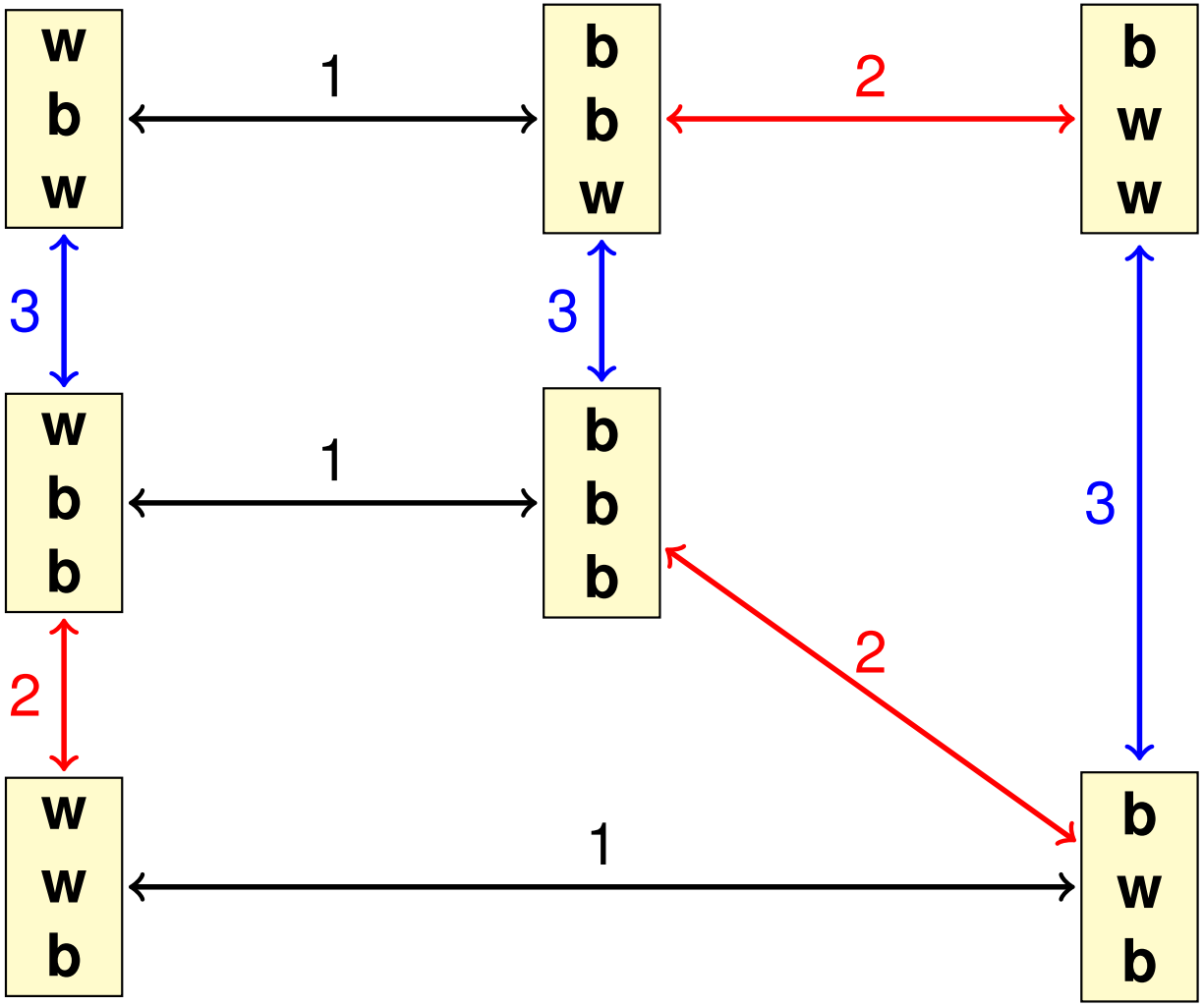


# Erster Schritt

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

(**b** **w** **w**)

nicht auftreten.

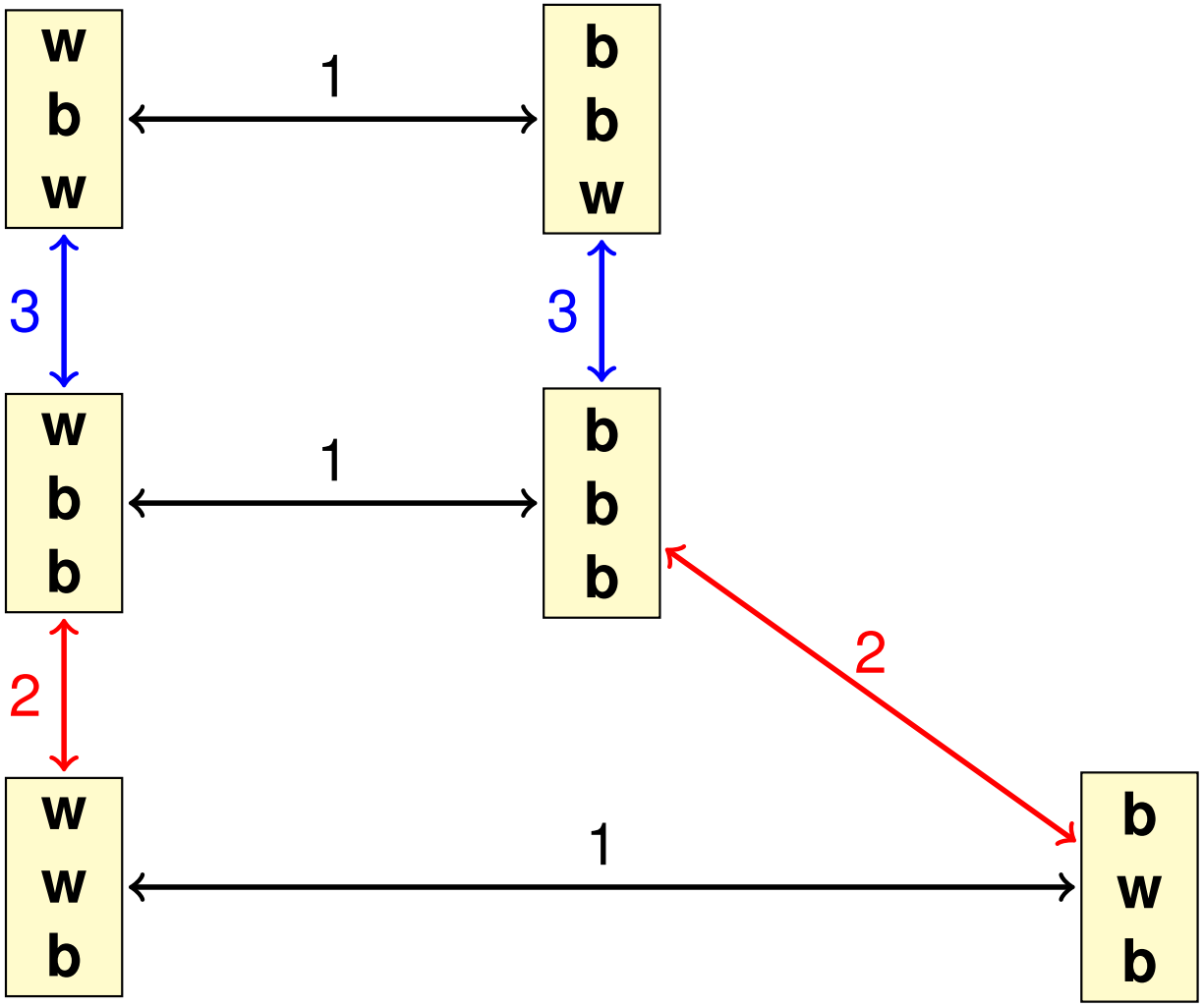


# Zweiter Schritt

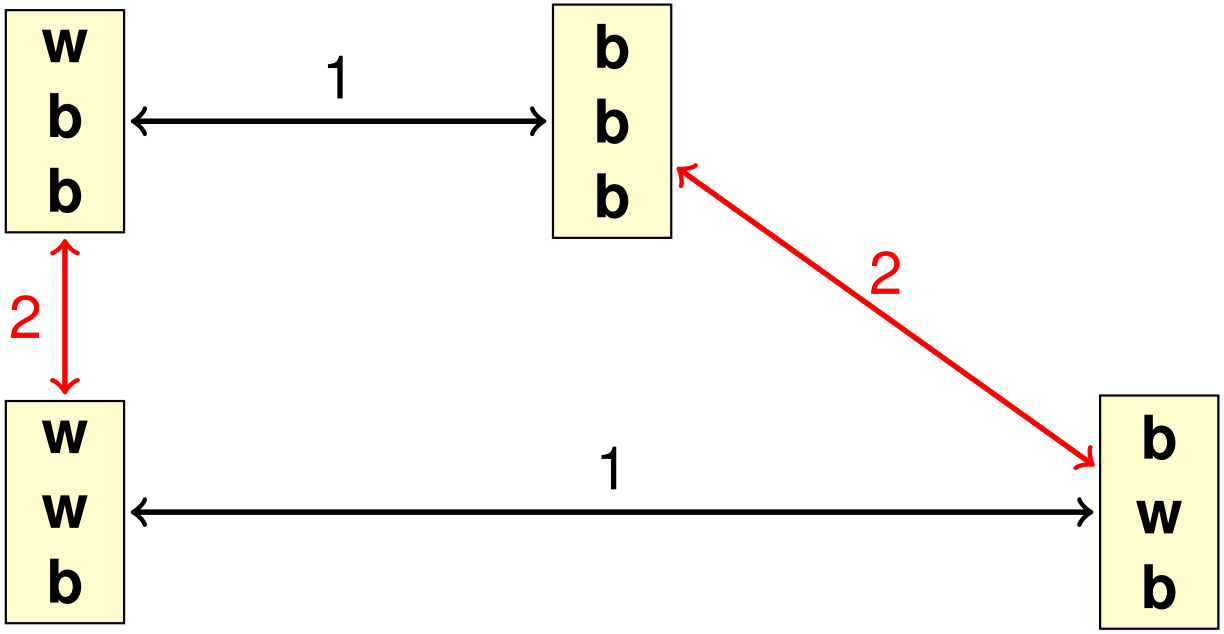
Da der zweite Weise die Farbe seines Huts nicht weiß, können die Welten

(**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

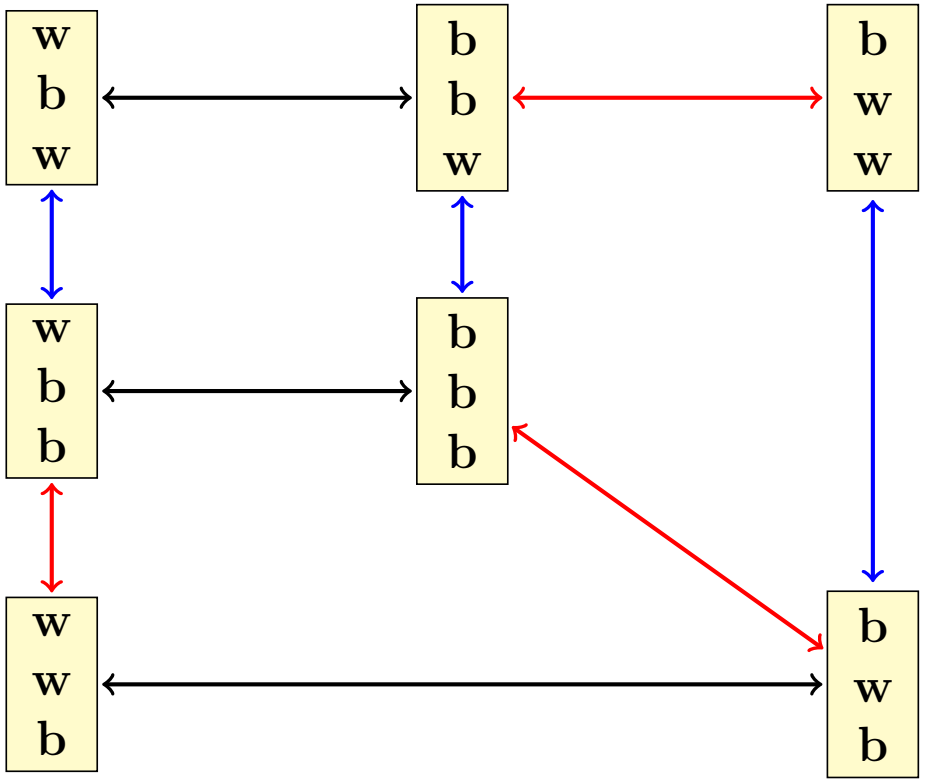
in der Welt $s$ weiß der $i$-te Weise die Aussage $A$

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 $W_j$.

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

nicht $(w, b, w) \models \Box_1 W_1$ $\quad$ $(b, w, w) \models \Box_1 B_1$

# 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 Numnmer 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.

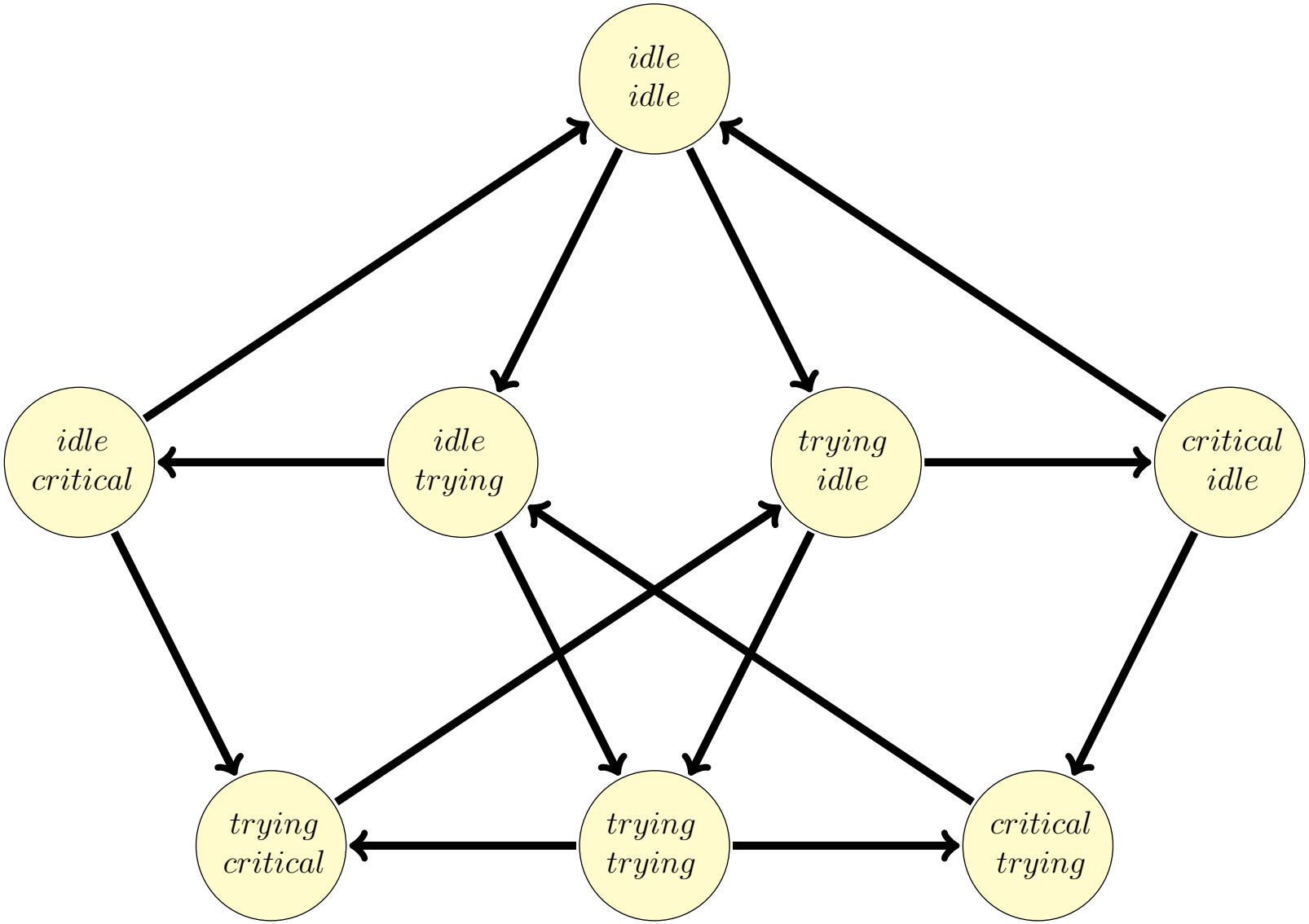
| **Customer** |
| --- |
| **int ticket**<br>$\{\text{idle}, \text{trying}, \text{critical}\}$ **phase** |

# Zustandsübergangsregeln

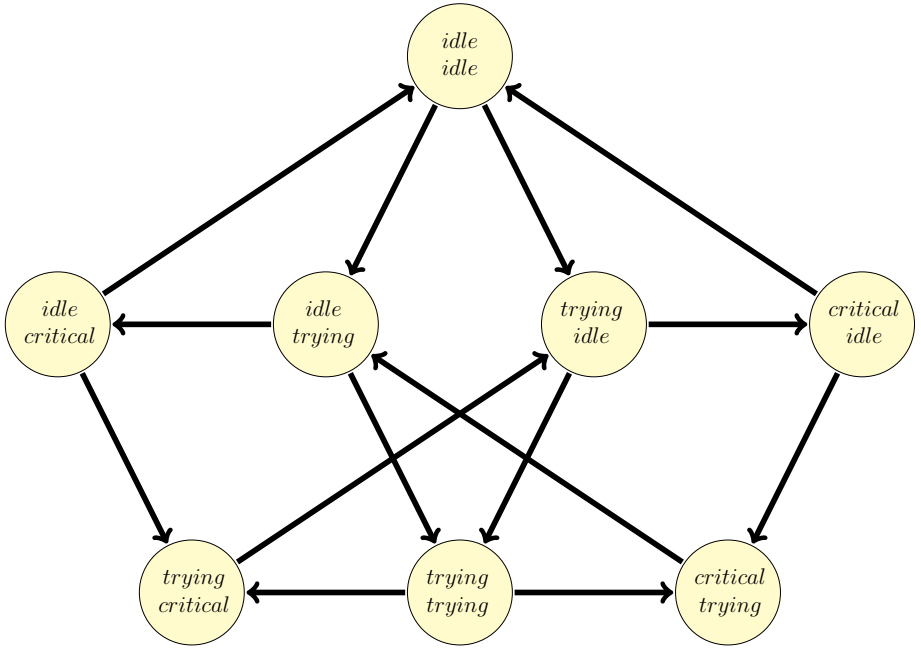
| | | |
|---|---|---|
| try: | if phase = idle | then<br>phase := trying<br>ticket := max of all other tickets + 1 |
| enter: | if phase = trying and<br>ticket less than<br>all other tickets | <br><br>then<br>phase := critical |
| leave | phase = critical | then<br>phase := idle<br>ticket := 0 |

# Endlicher Automat

Zwei Prozesse, keine Nummern



# 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.

$$1.\mathit{trying} \rightarrow (\Diamond 1.\mathit{critical} \vee \Diamond\Diamond 1.\mathit{critical})$$

$$\text{nicht } 1.\mathit{trying} \rightarrow \Diamond 1.\mathit{idle}$$

# 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 $mFor0_\Sigma$:
   $\Box A$ (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

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

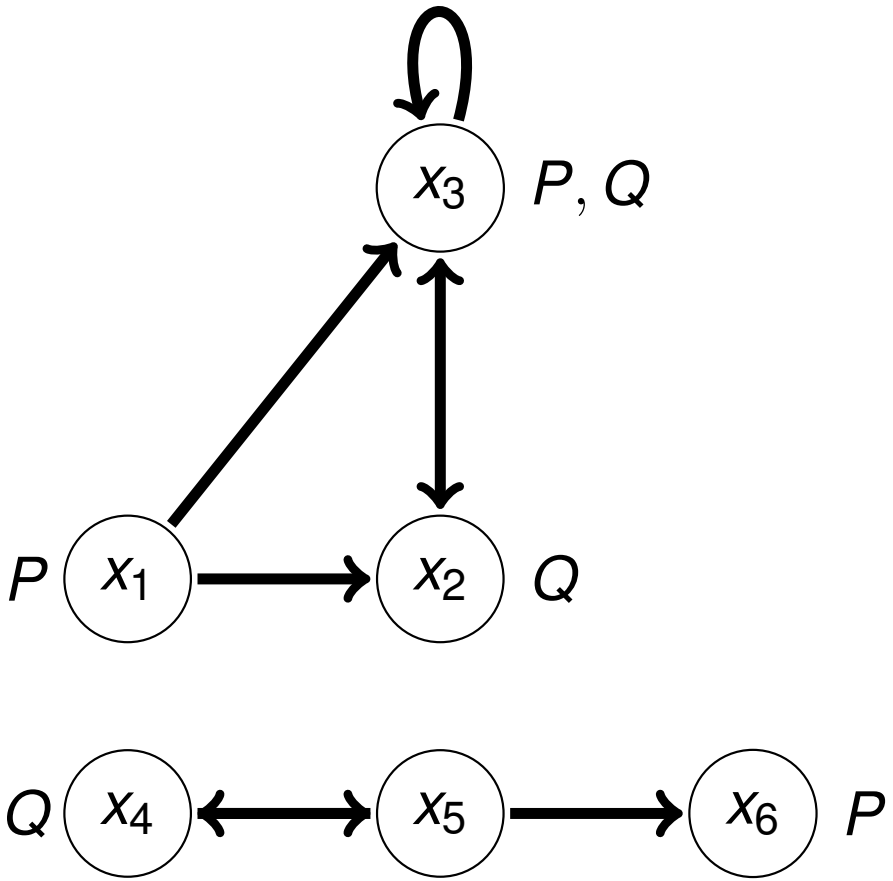
über $\Sigma$ besteht aus:

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

$(S, R)$ heißt der *Kripke Rahmen* von $\mathcal{K}$.

# Beispiel einer Kripke-Struktur

aus Huth and Ryan




Menge der Zustände $S = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ $R = \{(x_1, x_2), (x_1, x_3), (x_2, x_3), (x_3, x_2), (x_3, x_3), (x_4, x_5), (x_5, x_4), (x_5, x_6)\}$
$I(P, x_1) = I(P, x_3) = I(P, x_6) = 1$

# 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**

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

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

# Notation

$\mathcal{K} = (S, R, I)$ eine Kripke-Struktur,
$s \in S$,
$F$ eine modale Formel

$$(\mathcal{K}, s) \models F \Leftrightarrow val_s(F) = W$$

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

$$s \models F \Leftrightarrow val_s(F) = W$$

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

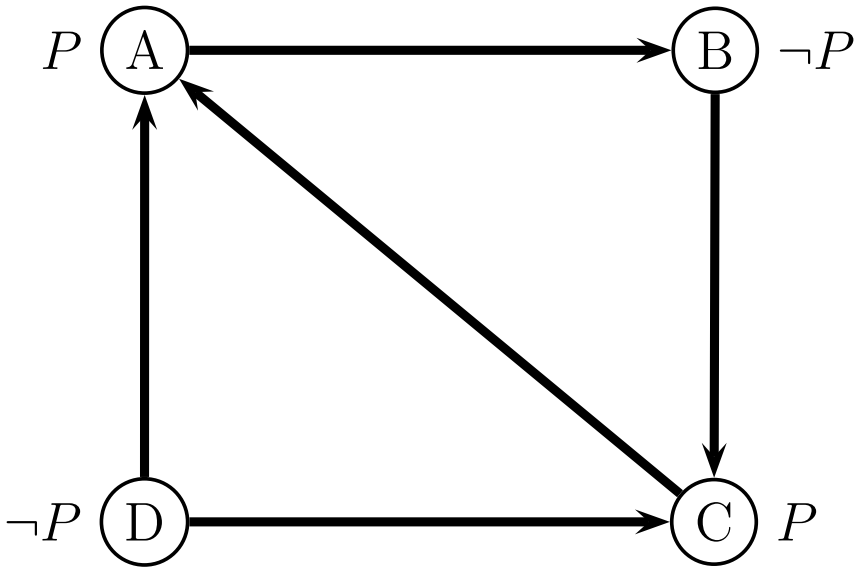
Gültigkeit in einen Kripke-Rahmen $(S, R)$ :

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

# 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




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

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

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

true false

# Logische Folgerung

## Definition

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

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

$$\Gamma \models A$$

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

$$\emptyset \models A$$

# Allgemeingültige Formeln

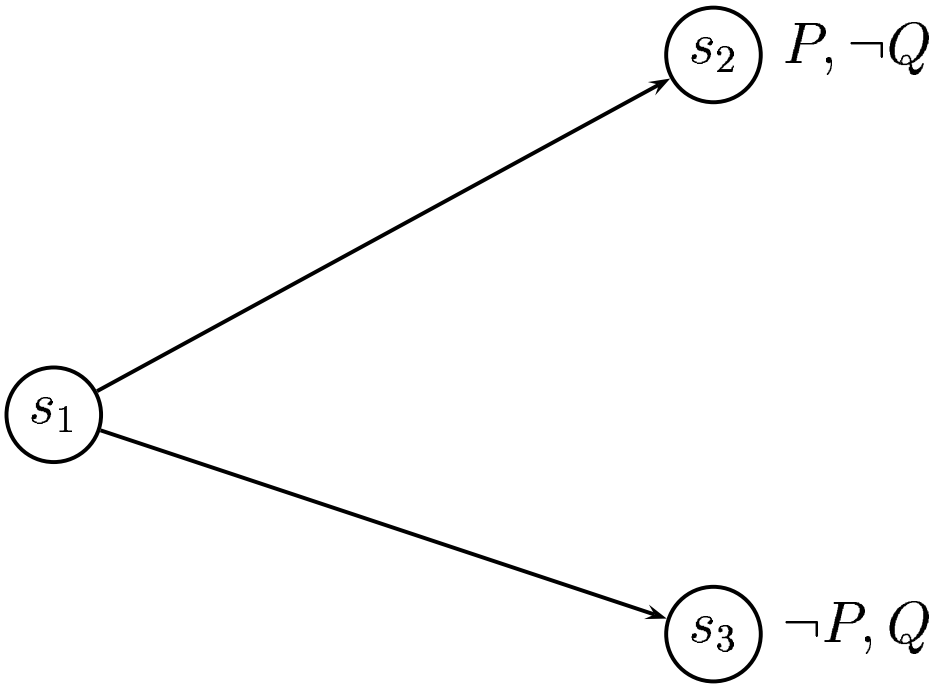
1. $\Box(P \to Q) \to (\Box P \to \Box Q)$
2. $(\Box P \wedge \Box(P \to Q)) \to \Box Q$
3. $(\Box P \vee \Box Q) \to \Box(P \vee Q)$
4. $(\Box P \wedge \Box Q) \leftrightarrow \Box(P \wedge Q)$
5. $\Box P \leftrightarrow \neg\Diamond\neg P$
6. $\Diamond(P \vee Q) \leftrightarrow (\Diamond P \vee \Diamond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

# Äquivalenzen zwischen den beiden Modalitäten

Varianten

| Modale Logik | | | Analogie aus Prädikatenlogik | | |
|---|---|---|---|---|---|
| $\Box P$ | $\leftrightarrow$ | $\neg\Diamond\neg P$ | $\forall x A$ | $\leftrightarrow$ | $\neg\exists x \neg A$ |
| $\neg\Box P$ | $\leftrightarrow$ | $\Diamond\neg P$ | $\neg\forall x A$ | $\leftrightarrow$ | $\exists x \neg A$ |
| $\Diamond P$ | $\leftrightarrow$ | $\neg\Box\neg P$ | $\exists x A$ | $\leftrightarrow$ | $\neg\forall x \neg A$ |
| $\neg\Diamond P$ | $\leftrightarrow$ | $\Box\neg P$ | $\neg\exists x A$ | $\leftrightarrow$ | $\forall x \neg A$ |

# Gegenbeispiel zur Allgemeingültigkeit von $\Box(P \vee Q) \rightarrow (\Box P \vee \Box Q)$



# Relative Allgemeingültigkeit

Erstes Beispiel

Die Formel

$$\Box A \to A$$

ist nicht allgemeingültig.

Aber

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

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

# Relative Allgemeingültigkeit

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

$P$ eine aussagenlogische Variable.

# Relative Allgemeingültigkeit

Weitere Beispiele

| allgemeingültige Formel | Eigenschaft von $R$ |
|---|---|
| $\Box P \to P$ | reflexiv |
| $P \to \Diamond P$ | reflexiv |
| $\Box\Box P \to \Box P$ | reflexiv |
| $\Box\Diamond P \to \Diamond P$ | reflexiv |
| $\Box P \to \Diamond\Box P$ | reflexiv |
| $\Diamond\Diamond P \to \Diamond P$ | transitiv |
| $\Box P \to \Box\Box P$ | transitiv |
| $P \to \Box\Diamond P$ | 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 |

$P$ eine aussagenlogische Variable.

# Charakterisierung

## Erstes Beispiel

Gilt für einen Kripke-Rahmen $(S, R)$

$$\text{für alle } I \text{ gilt } (S, R, I) \models \Box P \to P$$

dann ist

$$(S, R) \text{ reflexiv}$$

# Charakterisierungstheorie

## Definition

Sei **R** eine Klasse von Kripke-Rahmen,
und $F$ eine Formel der Modallogik.

$F$ charakterisiert die Klasse **R** genau dann, wenn für alle Kripke-Rahmen $(S, R)$ gilt

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

# Einige Charakterisierungsresultate

| Formel | charakterisierte Eigenschaft |
|---|---|
| $\Box P \to P$ | reflexiv |
| $\Box P \to \Box\Box P$ | transitiv |
| $P \to \Box\Diamond P$ | symmetrisch |
| $\Box\Box P \to \Box P$ | dicht |
| $\Diamond P \to \Box P$ | partiell funktional |
| $\Box P \to \Diamond P$ | endlos |

$P$ eine aussagenlogische Variable.

# Grenzen der Charaktersierungstheorie

## 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 Charaktersierungstheorie

## 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.

**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 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 $\Diamond$

| $\Diamond F \equiv \neg\Box\neg F$ | |
|---|---|
| $\Box F$ | $\Diamond F$ |
| $F$ 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 immer wahr (in der Zukunft) | ?no | yes | yes | yes | yes |
| Ein Agent $a$ weiß $F$ | yes | ?yes | yes | yes | yes |
| Ein Agent $a$ glaubt $F$ | no | ?yes | yes | yes | yes |
| Nach jeder Ausführung des Programms $p$ gilt $F$ | no | no | no | yes | no |