Vorlesungstermine

Alt	Neu
Do.10.01.	Do.10.01.
Fr.11.01.	Fr.11.01.
Do.17.01.	Do.17.01.
Fr.18.01. keine Vorlesung	Fr.18.01.
Do.24.01.	Do.24.01.
	letztes Übungsblatt
	Praxisaufgabe zu SPIN
Fr.25.01.	Fr.25.01.
Do.31.01.	Do.31.01.
Fr.01.02. keine Vorlesung	Fr.01.02.
Do.07.02.	keine Vorlesung
Fr.08.02.	keine Vorlesung
Do.14.02. keine Vorlesung	keine Vorlesung
Fr.15.02.	Fr.15.02. Wiederholung
1.Klausur 18.02. 14:00	1.Klausur 18.02. 14:00

Inhaltsübersicht

- Aussagenlogik
- Prädikatenlogik
- Reduktionssysteme
- Logik höherer Stufe
- OCL (Object Constraint Language)
- Modale Aussagenlogik
- Endliche Automaten (Wiederholung)
- Büchi Automaten
- Temporale Logik, LTL
- SPIN/Promela
- LTL2Büchi
- Modellprüfung
- AL Modellprüfung (Zusatzstoff)

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.

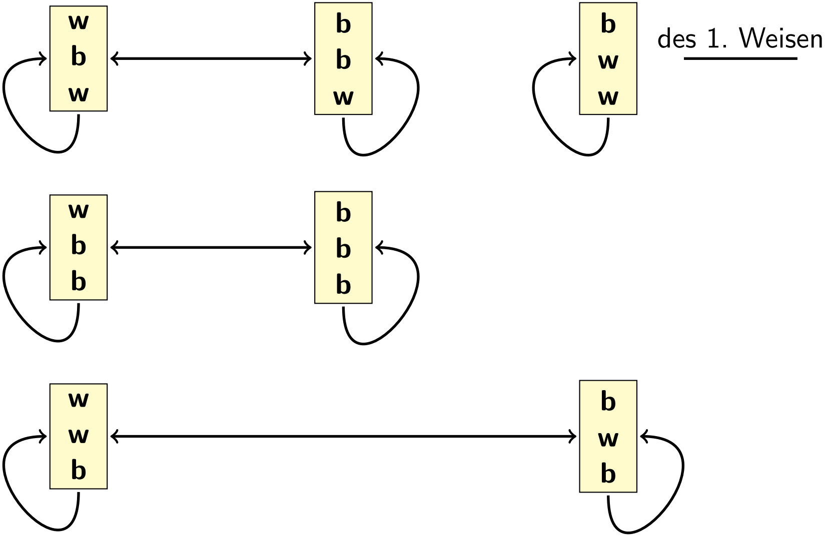
Einführungsbeispiel

Drei Weisen werden Hüte aufgesetzt, jedem genau einen. 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.“

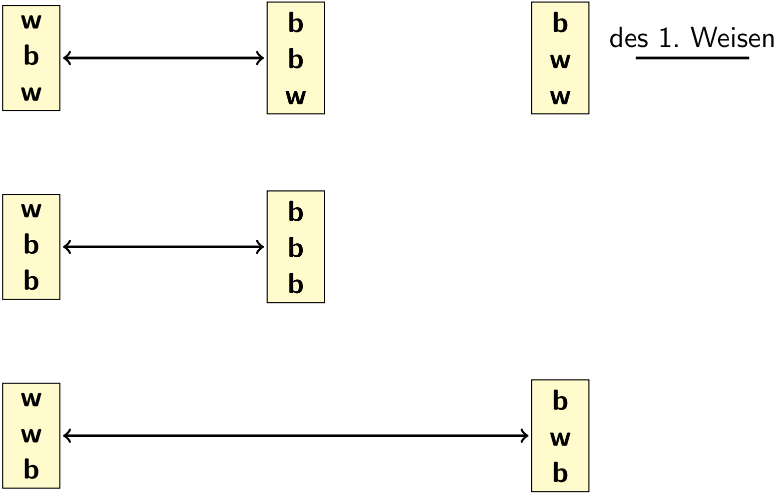
Mögliche Welten

w b w	b b w	b w w
w b b	b b b	
w w b		b w b

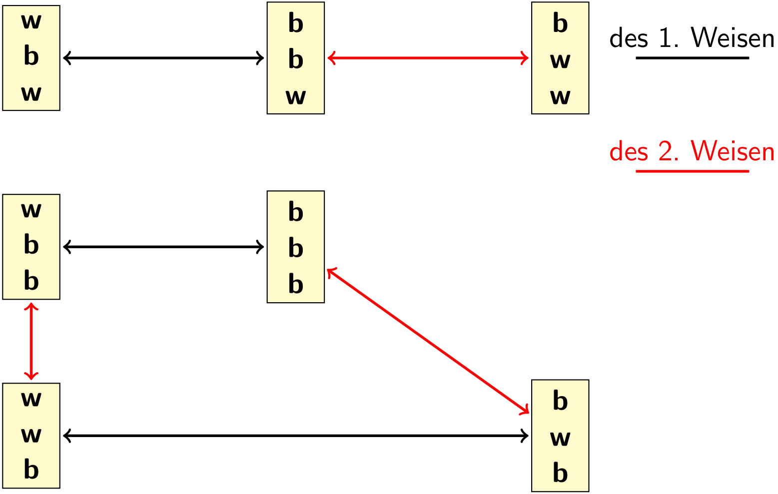
Mögliche Welten



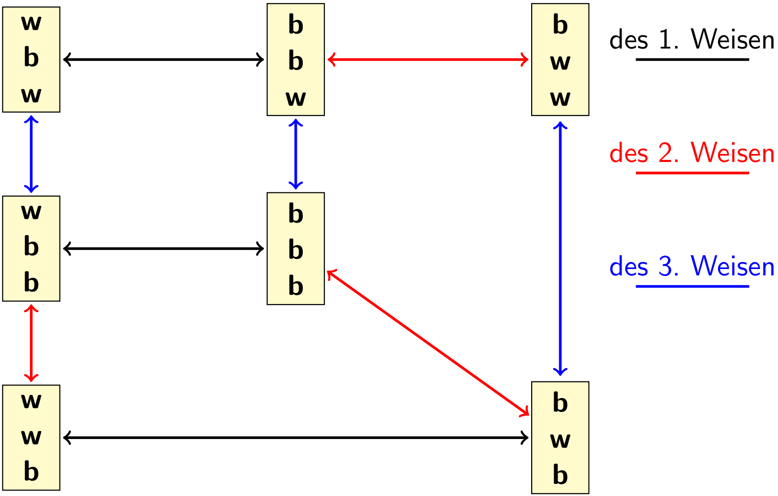
Mögliche Welten



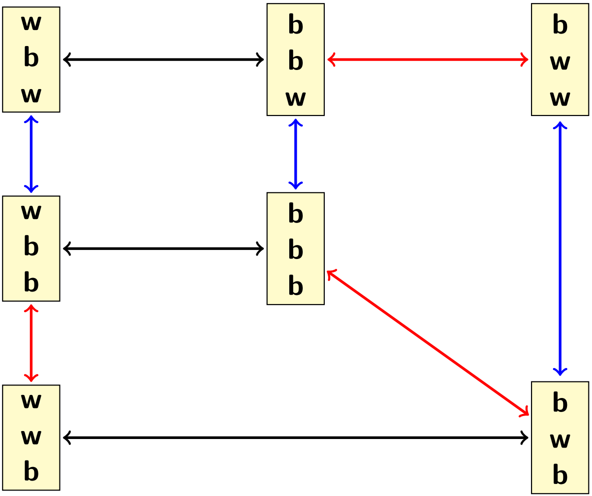
Mögliche Welten



Mögliche Welten



Erster Schritt

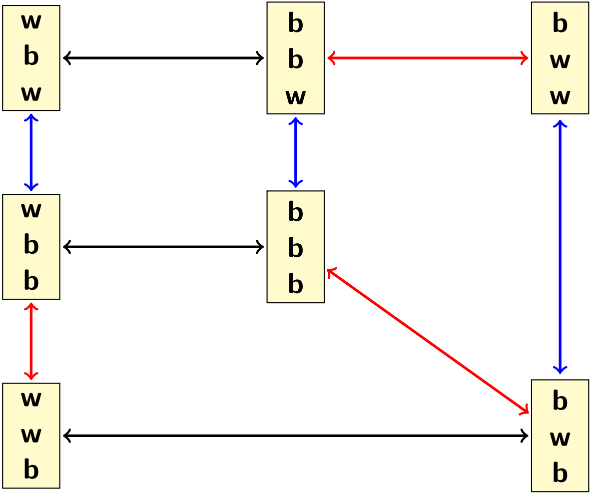


Erster Schritt

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

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

nicht auftreten.

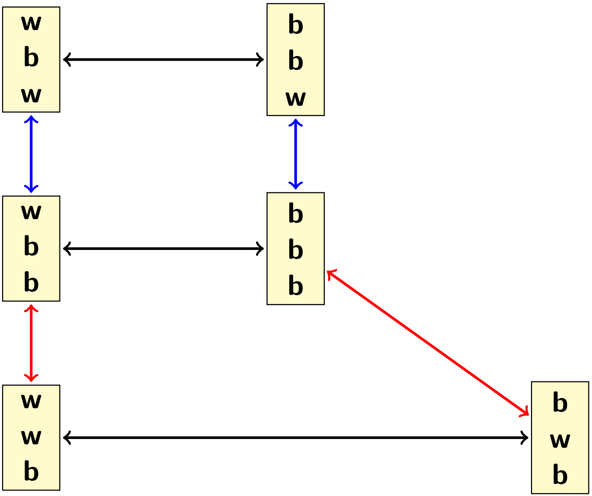


Erster Schritt

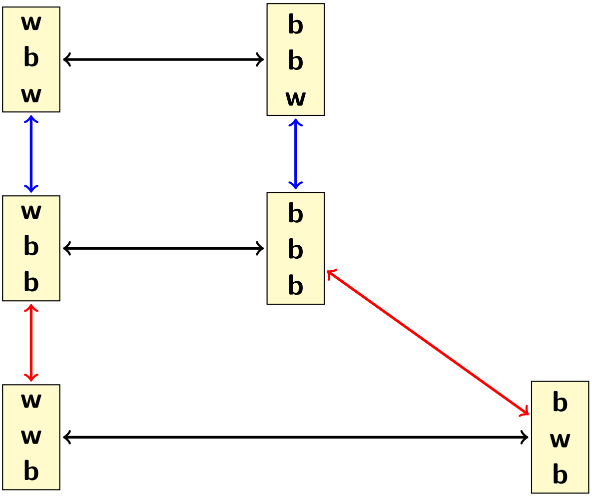
Da der erste Weise die Farbe seines Huts nicht erschließen kann, kann die Welt

(b w w)

nicht auftreten.



Zweiter Schritt

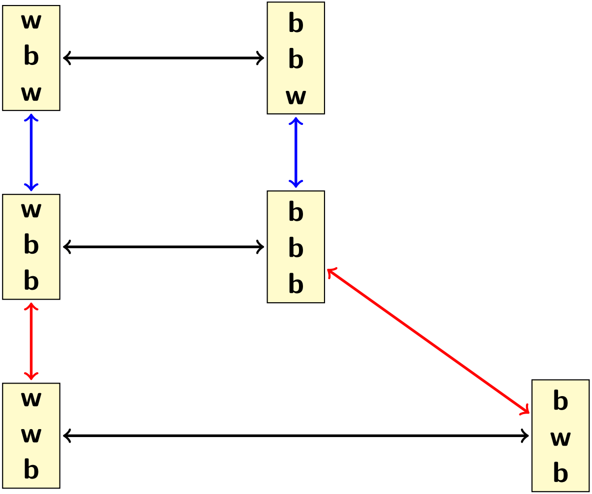


Zweiter Schritt

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

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

nicht auftreten.

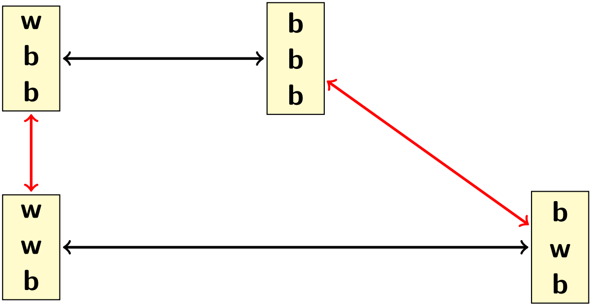


Zweiter Schritt

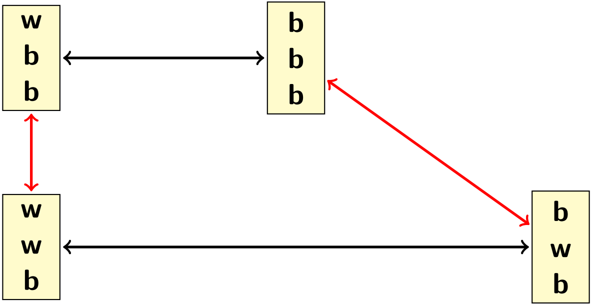
Da der zweite Weise die Farbe seines Huts nicht weiss, können die Welten

(**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-te Weisen von s ausgesehen möglichen Welt gilt A.

Modallogische Grundbegriffe

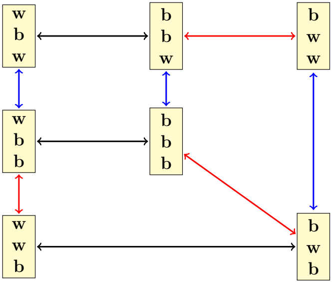
in der Welt s weiss der i-te Weise die Aussage A

genauer

in jeder für den i-te Weisen von s ausgesehen möglichen Welt gilt A.

$$s \models \Box_i A$$

Beispiele

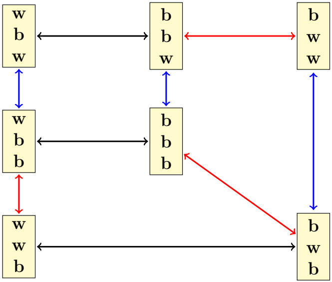


Die Boolesche Variable

$$B_i$$

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.

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

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 Arztpraxen 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 and die Reihe kommt und kein Streit darüber entsteht, wer als nächster drankommt.

Prozesse

Die Prozesse, die an dem *bakery* Algorithmus teilnehmen, können wir uns als Instanzen der Klasse *Customer* vorstellen.

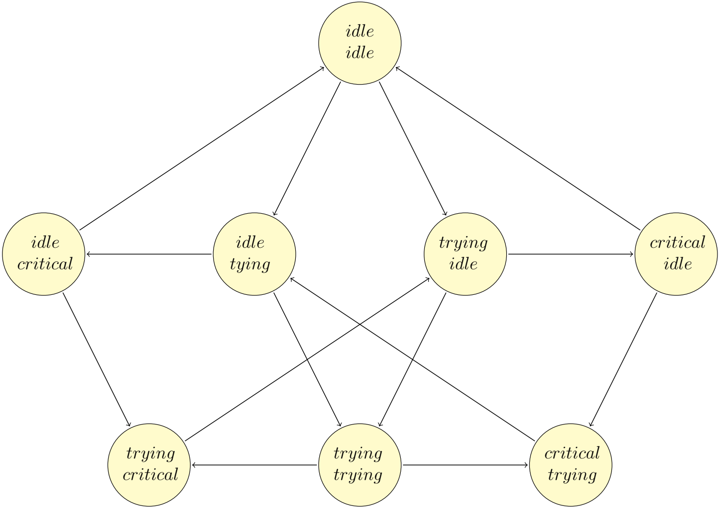
Customer
int ticket $\{\text{idle, trying, critical}\}$ **phase**

Zustandsübergangsregeln

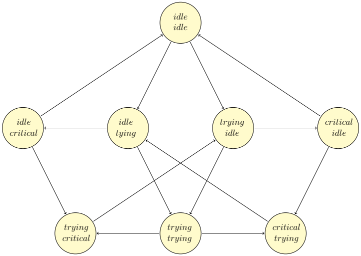
try:	if phase = idle	then phase := trying ticket := max of all other tickets + 1
enter:	if phase = trying and ticket less than all other tickets	then phase := critical
leave	phase = critical	then phase := idle ticket := 0

Endlicher Automat

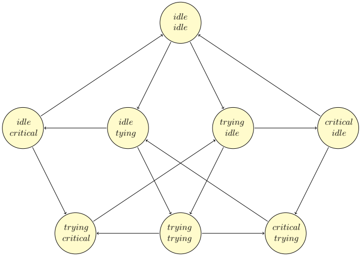
Zwei Prozesse, keine Nummern



Eigenschaften



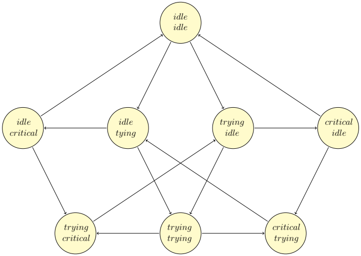
Eigenschaften



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

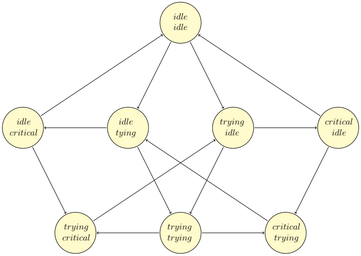


Notation

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.

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

Formeln der Modalen Aussagenlogik

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

Formeln der Modalen Aussagenlogik

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

Formeln der Modalen Aussagenlogik

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

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

Sei Σ eine Menge aussagenlogischer Variablen.
Eine Kripke Struktur

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

über Σ besteht aus

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

Kripke Strukturen

Sei Σ eine Menge aussagenlogischer Variablen.
Eine Kripke Struktur

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

über Σ besteht aus

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

Kripke Strukturen

Sei Σ eine Menge aussagenlogischer Variablen.
Eine Kripke Struktur

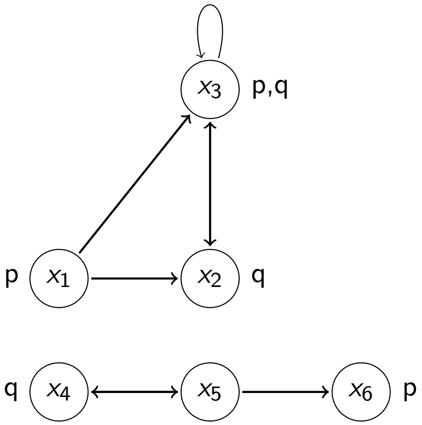
$$\mathcal{K} = (S, R, I)$$

über Σ 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)

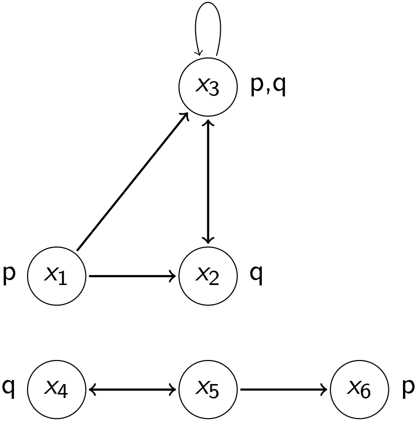
Beispiel einer Kripke Struktur

aus Huth and Ryan



Beispiel einer Kripke Struktur

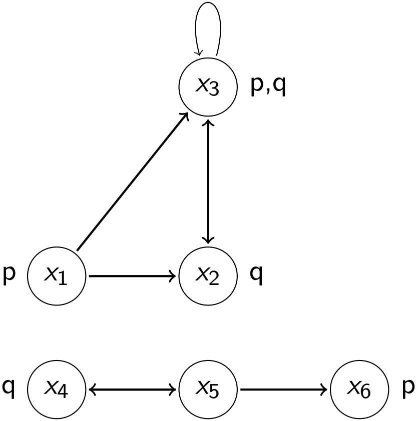
aus Huth and Ryan



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

Beispiel einer Kripke Struktur

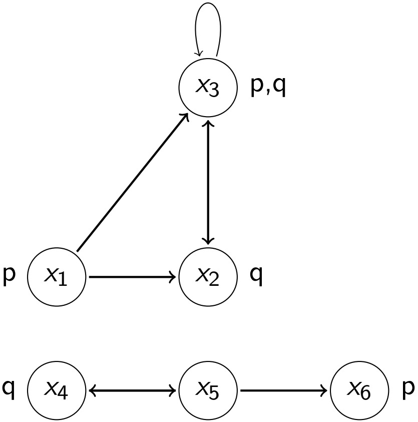
aus Huth and Ryan



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

Beispiel einer Kripke Struktur

aus Huth and Ryan



$I(p, x_1) = I(p, x_3) = I(p, x_6) = 1$
$I(q, x_2) = I(q, x_3) = I(q, x_4) = 1,$ sonst $I(x, s) = 0$

Auswertung von Formeln

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

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

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

Notation

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

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:

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

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

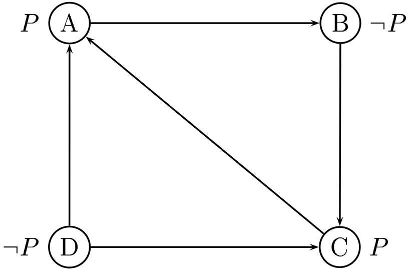
Gültigkeit in einen Kripke Rahmen (S, R) :

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

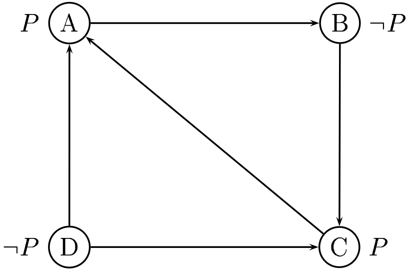
Saul Aaron Kripke

Geboren 1940 in Omaha (US)	
Erste 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

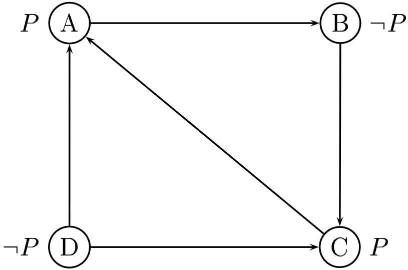


$(\mathcal{K}, A) \models P$ $\quad (\mathcal{K}, B) \models P$ $\quad (\mathcal{K}, C) \models P$ $\quad (\mathcal{K}, D) \models P$

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

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

Beispiel zur Auswertung von Formeln



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

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

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

true false

Logische Folgerung

Sei A eine Formel und Γ eine Menge von Formeln der modalen Aussagenlogik.

A ist eine logische Folgerung aus Γ
$$\Gamma \vdash A$$
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. $\Box(P \to Q) \to (\Box P \to \Box Q)$

Allgemeingültige Formeln

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

Allgemeingültige Formeln

1. $\Box(P \rightarrow Q) \rightarrow (\Box P \rightarrow \Box Q)$
2. $(\Box P \land \Box(P \rightarrow Q)) \rightarrow \Box Q$
3. $(\Box P \lor \Box Q) \rightarrow \Box(P \lor Q)$

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. $\Box P \leftrightarrow \neg\Diamond\neg P$

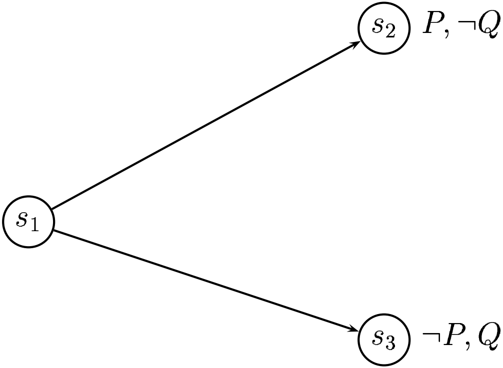
Allgemeingültige Formeln

1. $\Box(P \to Q) \to (\Box P \to \Box Q)$
2. $(\Box P \land \Box(P \to Q)) \to \Box Q$
3. $(\Box P \lor \Box Q) \to \Box(P \lor Q)$
4. $(\Box P \land \Box Q) \leftrightarrow \Box(P \land Q)$
5. $\Box P \leftrightarrow \neg\Diamond\neg P$
6. $\Diamond(P \lor Q) \leftrightarrow (\Diamond P \lor \Diamond Q)$

Allgemeingültige Formeln

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

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

$$\Box A \to A$$

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
$\Box A \rightarrow A$	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
$\Box A \to A$	reflexiv
$\Box A \to \Box\Box A$	transitiv
$A \to \Box\Diamond A$	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
$\Box A \to A$	reflexiv
$\Box A \to \Box\Box A$	transitiv
$A \to \Box\Diamond A$	symmetrisch
$\Box\Box A \to \Box A$	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 $R(t_3, t_2)$.
$\Diamond A \to \Box A$	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
$\Box A \to A$	reflexiv
$\Box A \to \Box\Box A$	transitiv
$A \to \Box\Diamond A$	symmetrisch
$\Box\Box A \to \Box A$	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 $R(t_3, t_2)$.
$\Diamond A \to \Box A$	partiell funktional
	für alle $s, t_1, t_2 \in S$ mit $R(s, t_1) \wedge R(s, t_2)$
	folgt $t_1 = t_2$.
$\Box A \to \Diamond A$	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)

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

dann ist

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

Charakterisierungstheorie

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

Charakterisierungstheorie

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
$\Box A \rightarrow A$	reflexiv

Einige Charakterisierungsresultate

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

Einige Charakterisierungsresultate

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

Einige Charakterisierungsresultate

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 Charakterisierungsresultate

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 Charakterisierungsresultate

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 Charakterisierungsresultate

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 Charakterisierungsresultate

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 Charaktersierungstheorie

Sei ϕ 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 ϕ eine modallogische Formel F, so daß die Klasse der Rahmen $\mathcal{R}_\phi$ charakterisiert?

Grenzen der Charaktersierungstheorie

Sei ϕ 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 ϕ 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 ϕ, so daß $\mathcal{R}_\phi$ mit der Klasse der durch F charakterisierten Rahmen zusammenfällt?

Grenzen der Charaktersierungstheorie

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 Charaktersierungstheorie

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 ϕ axiomatisiert werden kann.

Entscheidbarkeit

modaler Logiken

Filtration

Vorbereitende Definitionen

Sei $\mathcal{K} = (G, R, v)$ eine Kripke Struktur und
Γ eine Menge von Formeln der modalen Aussagenlogik.

Filtration

Vorbereitende Definitionen

Sei $\mathcal{K} = (G, R, v)$ eine Kripke Struktur und
Γ eine Menge von Formeln der modalen Aussagenlogik.
Die Äquivalenzrelation $\sim_\Gamma$ auf G wird definiert durch:

$$g \sim_\Gamma h \text{ gdw } (\mathcal{K}, g) \models A \Leftrightarrow (\mathcal{K}, h) \models A \text{ für alle } A \in \Gamma$$

Sei $\mathcal{K} = (G, R, v)$ eine Kripke Struktur und
Γ eine Menge von Formeln der modalen Aussagenlogik.
Die Äquivalenzrelation $\sim_\Gamma$ auf G wird definiert durch:

$$g \sim_\Gamma h \text{ gdw } (\mathcal{K}, g) \models A \Leftrightarrow (\mathcal{K}, h) \models A \text{ für alle } A \in \Gamma$$

$[g]$ bezeichnet die Äquivalenzklasse von g bezüglich $\sim_\Gamma$.

Sei $\mathcal{K} = (G, R, v)$ eine Kripke Struktur und
Γ eine Menge von Formeln der modalen Aussagenlogik.
Die Äquivalenzrelation $\sim_\Gamma$ auf G wird definiert durch:

$$g \sim_\Gamma h \text{ gdw } (\mathcal{K}, g) \models A \Leftrightarrow (\mathcal{K}, h) \models A \text{ für alle } A \in \Gamma$$

$[g]$ bezeichnet die Äquivalenzklasse von g bezüglich $\sim_\Gamma$.
Die Kripke Struktur $\mathcal{K}_\Gamma = (G_\Gamma, R_\Gamma, v_\Gamma)$ mit

$$\begin{array}{lcll}
G_\Gamma & = & \{[g] \mid g \in G\} & \\
[g]R_\Gamma[h] & \Leftrightarrow & \exists g_0 \in [g] \exists h_0 \in [h](g_0 R h_0) & \\
v_\Gamma([g], p) & = & v(g, p) & \text{für } p \in \Gamma \\
v_\Gamma([g], p) & = & \text{beliebig} & \text{sonst}
\end{array}$$

heißt eine Filtration von $\mathcal{K}$ bezüglich Γ.

Filtrationslemma

1. Sei Γ eine Menge von Formeln der modalen Aussagenlogik, abgeschlossen unter Teilformeln, dann gilt für alle $A \in \Gamma$ und alle $g \in G$

$$(\mathcal{K}, g) \models A \text{ gdw } (\mathcal{K}_\Gamma, [g]) \models A$$

Filtrationslemma

1. Sei Γ eine Menge von Formeln der modalen Aussagenlogik, abgeschlossen unter Teilformeln, dann gilt für alle $A \in \Gamma$ und alle $g \in G$

$$(\mathcal{K}, g) \models A \text{ gdw } (\mathcal{K}_\Gamma, [g]) \models A$$

2. Ist Γ endlich mit $\#\Gamma = n$, dann ist $\#G_\Gamma \leq 2^n$.

Entscheidbarkeit

Die modale Aussagenlogik **K** ist entscheidbar,

Entscheidbarkeit

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 $\Diamond$

$\Diamond F \equiv \neg\Box\neg F$	
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.

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