

Nicht-Standard-Logiken

- ▶ **Intuitionistische Aussagenlogik**
- ▶ **Prädikatenlogik 2. Stufe**
- ▶ **Modallogik**

Modelltheorie und Beweistheorie

Grundlegende Frage in der Philosophie: Was ist wahr / Wahrheit?

Hier haben wir 2 Ansätze gesehen, mathematisch Wahrheit zu definieren.

- ① Modell-Theorie: Semantik einer Logik ist gegeben durch Abbildung

$$\models: \text{Struktur} \times \text{Variablenbelegung} \times \text{Formel} \rightarrow \{ \text{wahr, falsch} \}$$

- ② Beweistheorie: Formel ist **beweisbar**, wenn es einen Beweis in einem formalen System (z.B. Sequenzenkalkül) gibt.

Verbindung zwischen diesen Ansätzen gegeben durch Sätze über **Korrektheit** und **Vollständigkeit** des Beweissystems: $\vdash \varphi$ gdw. $\models \varphi$

Intuitionismus

Dies führt dazu, dass in einem korrekten und vollständigen System der Satz

$$\neg \forall x. \neg P(x) \rightarrow \exists x. P(x)$$

beweisbar sein muss.

Hier wird die Existenz eines x , auf das P zutrifft, bloß aus der Annahme bewiesen, dass das **Gegenteil nicht** der Fall ist.

Ein **Intuitionist** würde so etwas ablehnen. Im Intuitionismus ist die **Existenz** eines Objekts mit einer bestimmten Eigenschaft gleichzusetzen mit der Möglichkeit, solch ein Objekt zu **konstruieren**.

In einer **intuitionistischen Logik** darf es also z.B. das Gesetz vom **ausgeschlossenen Dritten** nicht geben: $A \vee \neg A$ sollte nur beweisbar sein, wenn entweder A oder $\neg A$ beweisbar ist.

Beispiel für Intuitionismus

Bsp.: Es gibt zwei irrationale Zahlen a und b mit a^b rational.

Beweis durch Fallunterscheidung.

Fall $\sqrt{2}^{\sqrt{2}}$ ist rational. Wähle $a = b = \sqrt{2}$.

Fall $\sqrt{2}^{\sqrt{2}}$ ist irrational. Wähle $a = \sqrt{2}^{\sqrt{2}}$ und $b = \sqrt{2}$. Denn:

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$$



Dieser Beweis verwendet das Gesetz vom ausgeschlossenen Dritten und liefert keine Zeugen für a und b .

Negation in intuitionistischer Logik

Bem.: **klassische Logik** = ist Logik in dem Sinne, wie wir sie als Aussagenlogik und FO kennengelernt haben

- In klassischer Logik ist $\neg A$ zu lesen als “A ist falsch”.
- In intuitionistischer Logik ist $\neg A$ zu lesen als “A ist widerlegbar” im Sinne, dass es einen Beweis dafür gibt, dass A nicht gilt.

Somit:

- In klassischer Logik ist $A \leftrightarrow \neg\neg A$ gültig.
- In intuitionistischer Logik ist $A \rightarrow \neg\neg A$ gültig, aber $\neg\neg A \rightarrow A$ nicht: Wenn A beweisbar ist, so ist es nicht der Fall, dass A widerlegbar ist. Aus der Nicht-Existenz eines Beweises für $\neg A$ folgt jedoch nicht die Existenz eines Beweises für A.

Semantik der intuitionistischen Aussagenlogik

Offensichtlich bietet es sich mit obiger Argumentation an, intuitionistische Logik **beweistheoretisch** anzugehen. Statt also erst eine modelltheoretische Semantik zu formulieren und dann einen korrekten und vollständigen Beweiskalkül zu konstruieren, kann man gleich einen Beweiskalkül nehmen und alle darin beweisbaren Aussagen als wahr **definieren**.

Beachte: Begriffe wie Korrektheit und Vollständigkeit machen nur Sinn in Bezug auf etwas, z.B. eine gegebene modelltheoretische Semantik.

Man kann intuitionistischer Aussagenlogik auch eine modelltheoretische Semantik geben, z.B. über sogenannte **Kripke-Strukturen**.

Intuitionistischer Sequenzenkalkül

Der intuitionistische Sequenzenkalkül entsteht aus dem klassischen dadurch, dass Sukzedentien nur **genau eine Formel** enthalten dürfen, z.B.:

$$\frac{\Gamma \Rightarrow \varphi \quad \Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \wedge \psi} (\wedge_R) \quad \frac{\Gamma, \varphi, \psi \Rightarrow \chi}{\Gamma, \varphi \wedge \psi \Rightarrow \chi} (\wedge_L) \quad \frac{\Gamma \Rightarrow \varphi}{\Gamma \Rightarrow \varphi \vee \psi} (\vee_R^1)$$

$$\frac{\Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \vee \psi} (\vee_R^2) \quad \frac{\Gamma, \varphi \Rightarrow \chi \quad \Gamma, \psi \Rightarrow \chi}{\Gamma, \varphi \vee \psi \Rightarrow \chi} (\vee_L)$$

$$\frac{\Gamma \Rightarrow \perp}{\Gamma \Rightarrow \varphi} (\text{Efq}) \quad \frac{\Gamma \Rightarrow \varphi}{\Gamma, \neg \varphi \Rightarrow \perp} (\neg_L) \quad \frac{\Gamma, \varphi \Rightarrow \perp}{\Gamma \Rightarrow \neg \varphi} (\neg_R)$$

$$\frac{\Gamma \Rightarrow \varphi \quad \Gamma, \psi \Rightarrow \chi}{\Gamma, \varphi \rightarrow \psi \Rightarrow \chi} (\rightarrow_L) \quad \frac{\Gamma, \varphi \Rightarrow \psi}{\Gamma \Rightarrow \varphi \rightarrow \psi} (\rightarrow_R)$$

Beweise im intuitionistischen Sequenzenkalkül

Beachte:

- Ist φ **intuitionistisch** beweisbar, dann auch **klassisch**.
- Es gibt Formeln φ , die **klassisch** beweisbar sind, aber **nicht intuitionistisch**.

Bsp.: Man versuche, jeweils auf klassischem und intuitionistischem Weg **Pierce's Gesetz** zu beweisen:

$$((P \rightarrow Q) \rightarrow P) \rightarrow P$$

Von klassischer zu intuitionistischer Logik

Definiere **Abbildung** f , die Formeln der Aussagenlogik wiederum Formeln zuordnet, die keine Disjunktion enthalten, induktiv wie folgt:

$$f(A) := \neg\neg A$$

$$f(\varphi \wedge \psi) := f(\varphi) \wedge f(\psi)$$

$$f(\neg\varphi) := \neg f(\varphi)$$

$$f(\varphi \rightarrow \psi) := f(\varphi) \rightarrow f(\psi)$$

$$f(\varphi \vee \psi) := \neg(\neg f(\varphi) \wedge \neg f(\psi))$$

Thm.: φ ist klassisch beweisbar gdw. $f(\varphi)$ intuitionistisch beweisbar ist.

Bsp.: Man versuche, $f(((P \rightarrow Q) \rightarrow P) \rightarrow P)$ intuitionistisch zu beweisen.

Motivation der Prädikatenlogik 2. Stufe

Zur Erinnerung: “1. Stufe” bedeutet, dass nur über **Elemente** des Universums **quantifiziert** werden kann.

Betrachte das Partnersuche-Problem: Gegeben sind n Männer und n Frauen, die alle auf Partnersuche sind. Nach einer Kennenlernphase hat jede(r) Präferenzen entwickelt, die jeweils einige Vertreter des anderen Geschlechts als mögliche Partner in Frage kommen lassen, andere aber ausschließen. Jetzt soll eine 1-1-Zuordnung zwischen den Männern und Frauen gefunden werden, die alle Präferenzen berücksichtigt.

Abstrakt betrachtet: Geg. gerichteter, bipartiter Graph $G = (V_0, V_1, E)$, gibt es eine symmetrische Kantenmenge $M \subseteq E$, die eine Bijektion von V_0 nach V_1 darstellt?

Prädikatenlogik 2. Stufe

Prädikatenlogik 2. Stufe (SO) erweitert FO um **Variablen** $X, Y, \dots$ für **Relationen** und **Quantoren** darüber. Einer zweitstufigen Variable X ist immer eine **Stelligkeit** $st(X)$ zugeordnet.

Syntax wie bei FO mit zusätzlich:

- Sind $t_1, \dots, t_n$ Terme und X zweitstufige Variable mit $st(X) = n$, so ist $X(t_1, \dots, t_n)$ eine SO-Formel.
- Ist φ eine SO-Formel, so sind $\exists X.\varphi$ und $\forall X.\varphi$ SO-Formeln.

Semantik wie bei FO, wobei die Variablenbelegung ϑ zusätzlich die zweitstufigen Variablen durch Relationen auf dem Universum interpretiert, z.B.

$$\mathcal{A}, \vartheta \models X(t_1, \dots, t_n) \quad \text{gdw.} \quad ([t_1]_{\vartheta}^{\mathcal{A}}, \dots, [t_n]_{\vartheta}^{\mathcal{A}}) \in \vartheta(X)$$

$$\mathcal{A}, \vartheta \models \exists X.\varphi \quad \text{gdw.} \quad \text{es gibt } R \subseteq A^{st(X)} \text{ mit } \mathcal{A}, \vartheta[X \mapsto R] \models \varphi$$

Das Partnersucheproblem in SO

Das oben genannte Partnersucheproblem lässt sich in SO definieren.

Signatur $\tau = (V_0, V_1, E)$, wobei V_0, V_1 einstellig, E zweistellig.

$$\begin{aligned} \exists M. & \left(\forall x. \forall y. M(x, y) \rightarrow E(x, y) \right. \\ & \wedge \forall x. \forall y. M(x, y) \rightarrow M(y, x) \\ & \wedge \forall x. \forall y. \forall z. \left((M(x, y) \wedge M(x, z) \rightarrow y \doteq z) \right. \\ & \quad \left. \wedge (M(y, x) \wedge M(z, x) \rightarrow y \doteq z) \right) \\ & \left. \wedge \forall x. (\exists y. M(x, y)) \wedge \exists y. M(y, x) \right) \end{aligned}$$

Resultate über SO

- Es gibt **keine vollständige Axiomatisierung** von SO.
- **EF-Spiele** können leicht auf SO erweitert werden. (Aber Beweise, dass **D** ein Spiel $\mathcal{G}$ gewinnt, werden typischerweise aufgrund der exponentiell vielen Zugmöglichkeiten sehr kompliziert.)
- Es gibt **nicht-triviale, entscheidbare Fragmente** von SO (z.B. **Monadisches SO** auf Listen oder Bäumen).
- ...

Modallogik

Modallogik ist im Grunde eine **Familie** von Logiken mit ähnlichen Eigenschaften, die wir im Folgenden kennenlernen werden.

In Modallogik gibt es zwei zusätzliche einstellige Operatoren $\Diamond$ und $\Box$, die je nach Sichtweise verschiedene Bedeutungen haben. Dabei bedeutet $\Box A$ z.B.

- “A ist notwendig” (ursprüngliche Modallogik)
- “A wird geglaubt” (epistemische Logik)
- “A ist beweisbar” (provability logic)
- “A gilt immer” (Temporallogik)
- ...

Man kann Modallogik jedoch eine Semantik geben, die (zuerst einmal) unabhängig von der jeweiligen Intention ist.

Syntax der Modallogik

Def.: Seien $\mathcal{P} = \{p, q, \dots\}$ und $\Sigma = \{a, b, \dots\}$ eine nicht-leere Menge. **Formel** der Modallogik (ML) sind wie folgt aufgebaut.

- Ist $p \in \mathcal{P}$, so ist p eine Formel.
- Sind φ, ψ Formeln, so auch $\neg\varphi$, $\varphi \vee \psi$, $\varphi \wedge \psi$, $\varphi \rightarrow \psi$.
- Ist φ eine Formel und $a \in \Sigma$, so sind auch $\langle a \rangle \varphi$ und $[a] \varphi$ Formeln. (Sprich: “diamond-a-fi”, “box-a-fi”)

Ist $|\Sigma| = 1$ so schreiben wir auch einfach $\Diamond\varphi$ und $\Box\varphi$.

Kripke-Strukturen

Modallogik wird über speziellen relationalen Strukturen interpretiert. Mit $\mathcal{V}$ und Σ assoziieren wir eine Signatur τ , in der für

- jedes $q \in \mathcal{P}$ eine 1-stellige Relation R_q und
- jedes $a \in \Sigma$ eine 2-stellige Relation R_a existiert.

Beachte: τ -Strukturen sind somit gerichtete Graphen, deren Kanten mit Elementen aus Σ und deren Knoten mit Elementen aus $2^{\mathcal{P}}$ beschriftet sind. Diese nennt man **Kripke-Strukturen**.

Semantik der Modallogik

Formeln der Modallogik werden interpretiert in **Elementen** einer Kripke-Struktur.

Def.: Sei $\mathcal{A} = (A, \tau)$ eine Kripke-Struktur, $v \in A$.

$$\mathcal{A}, v \models q \quad \text{gdw.} \quad v \in R_q^{\mathcal{A}}$$

$$\mathcal{A}, v \models \varphi \wedge \psi \quad \text{gdw.} \quad \mathcal{A}, v \models \varphi \text{ und } \mathcal{A}, v \models \psi$$

$$\mathcal{A}, v \models \varphi \vee \psi \quad \text{gdw.} \quad \mathcal{A}, v \models \varphi \text{ oder } \mathcal{A}, v \models \psi$$

$$\mathcal{A}, v \models \neg \varphi \quad \text{gdw.} \quad \mathcal{A}, v \not\models \varphi$$

$$\mathcal{A}, v \models \langle a \rangle \varphi \quad \text{gdw.} \quad \text{es gibt } w \in A \text{ mit } (v, w) \in R_a^{\mathcal{A}} \text{ und } \mathcal{A}, w \models \varphi$$

$$\mathcal{A}, v \models [a] \varphi \quad \text{gdw.} \quad \text{für alle } w \in A \text{ gilt: falls } (v, w) \in R_a^{\mathcal{A}} \\ \text{dann } \mathcal{A}, w \models \varphi$$

Die so erhaltene Modallogik nennt man auch **K**.

Beispiele

Sind die folgenden Formeln erfüllbar? Was drücken sie aus?

- $q \wedge \Diamond(\neg q)$
- $\Diamond q \wedge \Box \neg q$
- $[a](\langle b \rangle q \vee \langle c \rangle \neg q) \wedge \langle a \rangle [b] \neg q \wedge \langle a \rangle [c] q$

Modallogik als Fragment von FO

Beachte: Interpretationen für **K**-Formeln sind **Paare** aus Kripke-Strukturen und Elementen.

Thm.: Für jede **K**-Formel φ ex. eine FO-Formel $\psi(x)$, so dass $|\psi| = \mathcal{O}(|\varphi|)$ und für alle Kripke-Strukturen $\mathcal{A} = (A, \tau)$ und $v \in A$ gilt:

$$\mathcal{A}, v \models \varphi \quad \text{gdw.} \quad \mathcal{A}, v \models \psi(x)$$

BEWEIS: Übung. (Man formuliere einfach nur die Semantik von **K** in FO.)

Beachte: Trotz der speziellen **K**-Interpretationen sind Begriffe wie **Erfüllbarkeit**, **Allgemeingültigkeit** und **Äquivalenz** durch diese Übersetzung wohldefiniert.

Zykelfreie Modelle

Offensichtlich ist FO mindestens so ausdrucksstark wie **K**. Gilt auch die Umkehrung (für FO über Kripke-Strukturen)? Nein. Wie zeigt man das? Statt explizit die Nicht-**K**-Definierbarkeit einer Klasse von Kripke-Strukturen zu zeigen, beweisen wir eine Eigenschaft, die alle **K**-definierbaren Kripke-Strukturklassen haben.

Def.: Eine Kripke-Struktur $\mathcal{A} = (A, \tau)$ heisst **zykel-frei**, wenn es keine $v_0, \dots, v_n \in A$ gibt, so dass

- $v_0 = v_n$ und
- für alle $i = 1, \dots, n$ gibt es a so dass $(v_{i-1}, v_i) \in R_a^{\mathcal{A}}$.

Thm.: Sei φ eine erfüllbare **K**-Formel. Dann hat φ ein zykel-freies Modell.

Beweis der Existenz von zykel-freien Modellen

BEWEIS: Sei $\mathcal{A} = (A, \tau)$ und $v \in A$, so dass $\mathcal{A}, v \models \varphi$. Wir definieren die **Abwicklung** von $\mathcal{A}$ als $\mathcal{U}_{\mathcal{A}} = (A^+, \tau)$ über dem Universum A^+ der Menge aller nicht-leeren Folgen von Elementen in A wie folgt. Für alle $(v_0, \dots, v_n) \in A^+$, alle q und alle a gilt:

- $(v_0, \dots, v_n) \in R_q^{\mathcal{U}_{\mathcal{A}}}$ gdw. $v_n \in R_q^{\mathcal{A}}$
- $((v_0, \dots, v_n), (v_0, \dots, v_n, v_{n+1})) \in R_a^{\mathcal{U}_{\mathcal{A}}}$ gdw. $(v_n, v_{n+1}) \in R_a^{\mathcal{A}}$

Man vergewissert sich leicht, dass $\mathcal{U}_{\mathcal{A}}$ zykel-frei ist.

Man kann außerdem leicht durch Induktion über den Aufbau von **K**-Formeln zeigen, dass für alle ψ und alle $(v_0, \dots, v_n) \in A^+$ gilt:

$$\mathcal{U}_{\mathcal{A}}, (v_0, \dots, v_n) \models \psi \quad \text{gdw.} \quad \mathcal{A}, v_n \models \psi$$

Insbesondere gilt also $\mathcal{U}_{\mathcal{A}}, v \models \varphi$ aufgrund der Annahme. □

Relative Ausdrucksschwäche von $\mathbf{K}$

Beachte: Man kann mit einer leichten Modifikation der obigen Konstruktion auch zeigen, dass jede erfüllbare $\mathbf{K}$ -Formel ein Modell hat, welches ein **Baum** ist.

Thm.: Es gibt FO-Formeln $\psi(x)$, für die es keine äquivalenten $\mathbf{K}$ -Formeln gibt.

BEWEIS: Betrachte $R_a(x, x)$ für ein beliebiges a . Dies ist offensichtlich erfüllbar, jedoch nur in einem nicht-zykel-freien Modell. Somit kann es mit obigem Thm. keine dazu äquivalente $\mathbf{K}$ -Formel geben. □

Diese relative Ausdrucksschwäche hat jedoch auch Vorteile. So gibt es einen (sogar recht einfachen) Algorithmus, der Erfüllbarkeit in $\mathbf{K}$ (und damit dann auch Allgemeingültigkeit und Äquivalenz) entscheidet.

Positive Normalform

Def.: Eine **K**-Formel ist in **positiver Normalform**, wenn Negation höchstens unmittelbar vor atomaren Propositionen in ihr auftritt.

Lemma: Für jede **K**-Formel φ ex. ψ in positiver Normalform, so dass $|\psi| = \mathcal{O}(|\varphi|)$ und $\psi \iff \varphi$.

BEWEIS: Mit deMorgen, Doppel-Negationselimination und $\neg\langle a \rangle \varphi \iff [a]\neg\varphi$.



Unterformeln

Def.: Die Menge aller **Unterformeln** einer **K**-Formel φ ist induktiv definiert wie folgt.

$$Sub(q) := \{q\}$$

$$Sub(\varphi \wedge \psi) := \{\varphi \wedge \psi\} \cup Sub(\varphi) \cup Sub(\psi)$$

$$Sub(\varphi \vee \psi) := \{\varphi \vee \psi\} \cup Sub(\varphi) \cup Sub(\psi)$$

$$Sub(\neg\varphi) := \{\neg\varphi\} \cup Sub(\varphi)$$

$$Sub(\langle a \rangle \varphi) := \{\langle a \rangle \varphi\} \cup Sub(\varphi)$$

$$Sub([a]\varphi) := \{[a]\varphi\} \cup Sub(\varphi)$$

Vorbereitung auf einen Tableau-Kalkül

Def.: Ein **Literal** ist eine atomare Proposition oder deren Negation. Eine Menge $\ell_1, \dots, \ell_k$ heißt **konsistent**, falls es keine $1 \leq i, j \leq k$ gibt, so dass $\ell_i = q$ und $\ell_j = \neg q$ für eine Proposition q .

Def.: Eine Menge $\Phi \subseteq \text{Sub}(\varphi)$ heißt

- **geschlossen**, falls Φ nur aus Literalen und Formeln der Form $[a]\psi$ besteht und die Literale darin konsistent sind,
- **offen** sonst.

Ein Tableau-Kalkül für Modallogik

Def.: Ein **Tableau** für eine **K**-Formel φ in positiver Normalform ist ein endlicher Baum, dessen

- Knoten mit **Teilmengen** von $Sub(\varphi)$ beschriftet sind, so dass
- $\{\varphi\}$ die Beschriftung der **Wurzel** ist und
- die Beschriftungen von Vater- und Söhneknoten immer eine Instanz einer der folgenden Regeln ist

$$\frac{\psi_1 \vee \psi_2, \Phi}{\psi_i, \Phi} \quad i \in \{1, 2\} \qquad \frac{\psi_1 \wedge \psi_2, \Phi}{\psi_1, \psi_2, \Phi}$$

$$\frac{\langle a_1 \rangle \varphi_1, \dots, \langle a_n \rangle \varphi_n, [b_1] \psi_1, \dots, [b_m] \psi_m, \ell_1, \dots, \ell_k}{\varphi_1, \Psi_1 \quad \varphi_2, \Psi_2 \quad \dots \quad \varphi_n, \Psi_n} \quad \{\ell_1, \dots, \ell_k\} \text{ konsistent}$$

wobei $\Psi_i = \{\psi_j \mid b_j = a_i\}$,

- Blätter alle geschlossen sind.

Hauptsatz über Tableaux

Thm.: Für alle **K**-Formeln φ gilt: φ ist erfüllbar gdw. es ein Tableau für φ gibt.

BEWEIS: “ $\Rightarrow$ ” Angenommen, φ ist erfüllbar. Dann gibt es eine Kripke-Struktur $\mathcal{A} = (A, \tau)$ und ein $v \in A$, so dass $\mathcal{A}, v \models \varphi$. Wir konstruieren nun ein Tableau für φ durch **Annotation** von Teilmengen von $Sub(\varphi)$ mit Elementen aus A und Regelanwendungen, beginnend mit v und $\{\varphi\}$, so dass die folgende Invariante für alle Knotenbeschriftungen Φ mit Annotat w gilt: $\mathcal{A}, w \models \bigwedge \Phi$.

- Für die Wurzel ist dies nach Voraussetzung der Fall.
- Die Regel für Konjunktionen erhält diese Invariante trivialerweise.
- Ist $\mathcal{A}, w \models (\psi_1 \vee \psi_2) \wedge \Phi$, so gibt es ein $i \in \{1, 2\}$, so dass $\mathcal{A}, w \models \psi_i \wedge \Phi$. Mit diesem kann die Konstruktion fortfahren.

Beweis der Vollständigkeit der Tableaux

- Ist $\mathcal{A}, w \models \langle a_1 \rangle \varphi_1, \dots, \langle a_n \rangle \varphi_n, [b_1] \psi_1, \dots, [b_m] \psi_m, \Lambda$, so muss es $w_1, \dots, w_n$ geben mit $(w, w_i) \in R_{a_i}^A$, so dass $\mathcal{A}, w_i \models \varphi_i$ für alle $i = 1, \dots, n$. Zusätzlich muss gelten $\mathcal{A}, w_i \models \psi_j$, falls $b_j = a_i$. Somit lässt sich auch die Regel für die Modaloperatoren so anwenden, dass die Invarianten erhalten bleibt.

Invariante besagt: Konstruktion bleibt nicht in offener Formelmenge hängen. Enthaltene Dis-, Konjunktion und $\langle a \rangle$ -Formeln können mit entsprechenden Regeln eliminiert werden. Außerdem kann keine inkonsistente Formelmenge erreicht werden, denn $\mathcal{A}, w \models \psi \wedge \neg \psi \wedge \Phi$ ist unmöglich.

Noch zu zeigen: Konstruktion terminiert und führt zu endlichem Baum. Dies erkennt man leicht daran, dass jede Regelanwendung mindestens einen Operator aus der Formelmenge entfernt und somit keine unendlichen Äste konstruiert werden können.

Beweis der Korrektheit der Tableaux

($\Leftarrow$) Angenommen, T ist Tableau für φ . Definiere **Kollaps** T' durch Verschmelzen der Anwendungen der Regeln für Dis- und Konjunktionen. T' ist Baum, dessen Knoten Teilmengen von $Sub(\varphi)$ sind. (Beschriftet) Kanten sind durch Konklusion-Prämissen-Beziehung der Modalregel gegeben. Erweitere zu Kripke-Struktur durch Interpretation von Literalen in allen Zuständen, die sie enthalten.

Zeige durch Induktion über Aufbau von ψ , dass gilt: Ist ψ enthalten in Knoten v , so gilt $T', v \models \psi$. Für Literale ist dies per Konstruktion der Fall. Für Dis- und Konjunktionen folgt dies aus der Hypothese für kleinere Formeln und der Tatsache, dass die entsprechende Regel angewandt worden sein muss. Für Formeln der Form $\langle a \rangle \psi$ gilt: Es gibt w mit $(v, w) \in R_a^{T'}$, welches ψ enthält. Nach Hypothese gilt $T', w \models \psi$. Also gilt auch $T', v \models \langle a \rangle \psi$. Der Fall für $[b] \psi$ ist ähnlich.

Insbesondere: $T', v \models \varphi$, wobei v die Wurzel von T' ist. □

Endliche Baummodelleigenschaft

Thm.: Jede erfüllbare **K**-Formel hat ein Modell, welches ein endlicher Baum ist.

BEWEIS: Sei φ erfüllbar. Nach Vollständigkeit der Tableaux gibt es ein Tableaux für φ . Die Konstruktion im Beweis der Korrektheit liefert daraus ein Modell für φ welches ein endlicher Baum ist. $\square$

Dies liefert einen alternativen Beweis dafür, dass **K** nicht so ausdrucksstark wie FO über Kripke-Strukturen sein kann.

Entscheidbarkeit von Modallogik

Thm.: Es gibt einen Algorithmus, der in Zeit $\mathcal{O}(2^{|Sub(\varphi)|})$ entscheidet, ob φ erfüllbar ist.

BEWEIS: Übung. Hinweis: Durch systematischen Versuch, ein Tableau für φ zu bauen. Da es höchstens $2^{|Sub(\varphi)|}$ viele verschiedene Knoten in einem Tableau geben kann, muss man auch nicht mehr Knoten als so viele anschauen.

Liefert sogar einen Beweis dafür, dass eine keine **berechenbare**, Erfüllbarkeitsäquivalenz erhaltene Abbildung von FO nach **K** geben kann.

Beachte, es gibt jedoch **nicht berechenbare** Abbildungen, die Erfüllbarkeitsäquivalenz erhalten, z.B.

$$f(\varphi) := \begin{cases} \top & , \text{ falls } \varphi \text{ erfüllbar} \\ \perp & , \text{ sonst} \end{cases}$$

EF-Spiele für K

Durch die Übersetzung von K nach FO erhält man natürlich EF-Spiele “umsonst”. Beachte: Die Übersetzung liefert eine Formel in einer freien Variablen. Aus diesem Grund muss man generalisierte Spiele betrachten. Andererseits kommt jede quantifizierte Variable nur ein einziges Mal in der Formel vor. Daher lassen sich die Spiele auch gleich einfacher formulieren.

Gespielt wird auf zwei Kripke-Strukturen $\mathcal{A} = (A, \tau)$ und $\mathcal{B} = (B, \tau)$ mit zwei Spielsteinen. Zu Beginn liegen diese auf einem $v \in A$ und einem $w \in B$ gewählt. In der i -ten Runde schiebt **S** einen der Spielsteine entlang einer a -Kante zu einem Nachfolgerknoten. **D** tut dasselbe mit dem anderen Spielstein (ebenfalls entlang einer a -Kante). **S** gewinnt, sobald **D** nicht nachziehen kann oder die beiden Spielsteine auf zwei Knoten liegen, die sich in mindestens einer atomaren Proposition unterscheiden.

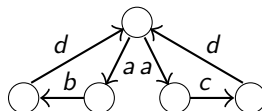
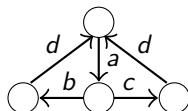
Korrektheit und Beispiel

Def.: Die **modale Tiefe** einer Formel, $md(\varphi)$ ist – analog zur Quantorentiefe – die maximale Anzahl geschachtelter $\Diamond$ - oder $\Box$ -Operatoren in φ .

Thm.: **D** gewinnt das k -Runden EF-Spiel auf $\mathcal{A}, v, \mathcal{B}, w$ gdw. für alle **K**-Formeln φ mit $md(\varphi) \leq k$ gilt: $\mathcal{A}, v \models \varphi$ gdw. $\mathcal{B}, w \models \varphi$.

BEWEIS: Übung.

Man vergewissere sich, dass **S** folgendes 2-Runden-Spiel gewinnt.



Welche **K**-Formel unterscheidet die beiden Strukturen?

Facetten

Es gibt viele verschiedenen Logiken, die einerseits im Grunde Modallogiken sind, andererseits jedoch über **K** hinausgehen, z.B. durch eine erweiterte Syntax oder eine Restriktion auf eine bestimmte Strukturklasse.

Wir wollen im folgenden noch betrachten:

- lineare Temporallogik LTL
- propositionale dynamische Logik PDL
- die Beschreibungslogik $\mathcal{ALC}$

Lineare Temporallogik

Temporallogik soll zeitliche Abläufe modellieren (z.B. den Lauf eines Programms). Lineare Temporallogik (LTL) wird über Kripke-Strukturen mit einer einzigen Erreichbarkeitsrelation, die eine lineare Ordnung auf dem Universum bildet, interpretiert. Als Universum nimmt man typischerweise $\mathbb{N}$ an.

Def.: Die Syntax von LTL erweitert Aussagenlogik (mit den Propositionssymbolen wie bei **K**) um einstellige Operatoren X (“next”), F (“finally”), G (“generally”) und einen zweistelligen Operator U (“until”). Die Interpretation dieser Operatoren ist wie folgt.

$$\mathcal{A}, i \models X\varphi \quad \text{gdw.} \quad \mathcal{A}, i + 1 \models \varphi$$

$$\mathcal{A}, i \models F\varphi \quad \text{gdw.} \quad \text{es gibt } j \geq i \text{ mit } \mathcal{A}, j \models \varphi$$

$$\mathcal{A}, i \models G\varphi \quad \text{gdw.} \quad \text{für alle } j \geq i \text{ gilt: } \mathcal{A}, j \models \varphi$$

$$\mathcal{A}, i \models \varphi U \psi \quad \text{gdw.} \quad \text{es gibt } j \geq i, \text{ so dass } \mathcal{A}, j \models \psi \text{ und für alle } h \\ \text{mit } i \leq h < j \text{ gilt } \mathcal{A}, h \models \varphi$$

Beispiele

- Lassen sich X, F, G, U jeweils irgendwie durch die anderen Konstrukte ausdrücken?
- Sind die folgenden Formeln φ_n über Propositionen $q_0, \dots, q_{n-1}$, $n \geq 1$, erfüllbar? Wenn ja, wie sehen ihre Modelle aus?

$$\varphi_n := \bigwedge_{i=0}^{n-1} \neg q_i \wedge G\left(\bigvee_{i=0}^{n-1} \neg q_i \wedge Xq_i \wedge \left(\bigwedge_{j<i} q_j \wedge \neg Xq_j\right) \wedge \left(\bigwedge_{j>i} q_j \leftrightarrow Xq_j\right)\right)$$

- Kann man ausdrücken “in jedem 2. Knoten gilt q ”?

Abwicklungen

Schwierigkeit für einen Tableau-Kalkül im Vergleich zu **K**: Die Modaloperatoren F , G und U können z.B. durch ihre **Abwicklungen** behandelt werden.

$$F\varphi \iff \varphi \vee XF\varphi$$

$$G\varphi \iff \varphi \wedge XG\varphi$$

$$\varphi U\psi \iff \psi \vee (\varphi \wedge X(\varphi U\psi))$$

- Terminierung ist nicht unbedingt gegeben, wenn man diese Äquivalenzen in Tableau-Regeln übersetzt.
- Bei F und U ist dies in jedem einzelnen Schritt korrekt, im **Limit** muss jedoch sichergestellt werden, dass irgendwann einmal der existentielle Quantor in der Semantik erfüllt wird.

Resultate

Thm.: (Kleine Modelleigenschaft) Jede erfüllbare LTL-Formel der Größe n hat ein Modell, welches sich mit höchstens 2^n vielen Elementen repräsentieren lässt.

Thm.: (Entscheidbarkeit) Es gibt einen Algorithmus, welcher Erfüllbarkeit für LTL in Zeit $2^{\mathcal{O}(n)}$ entscheidet.

Thm.: (Ausdrucksstärke) LTL und FO sind äquivalent über den hier betrachteten, linearen Strukturen.

Bem.: Die Übersetzung von LTL nach FO ist wieder sehr einfach, da die Semantik von LTL in FO formalisierbar ist. Die Umkehrung ist jedoch alles andere als trivial, und es gibt FO-Formeln der Größe n , zu denen man nur äquivalente LTL-Formeln der Größe

$$2^{2^{\dots^{2^{\mathcal{O}(1)}}}} \}^{\mathcal{O}(n)}$$

finden kann.

Beschreibungslogiken

Beschreibungslogiken werden benutzt, um **Wissen** zu modellieren und z.B. aus gegebenen Fakten notwendige Konsequenzen abzuleiten.

Die Syntax von Beschreibungslogiken baut auf auf einer Menge von **Konzeptennamen** (1-stellige Relationen) $C, \dots$ und einer Menge von **Rollennamen** (2-stellige Relationen) $R, \dots$

Def.: Die Syntax der Beschreibungslogik $\mathcal{ALUC}$ ist folgendermaßen gegeben.

- Jeder Konzeptname C ist ein (atomares) Konzept.
- Die Konstanten $\top$ und $\perp$ sind Konzepte.
- Sind φ und ψ Konzepte, so auch $\varphi \sqcap \psi$, $\varphi \sqcup \psi$ und $\neg\varphi$.
- Ist R Rollenname und φ ein Konzept, so ist $\forall R.\varphi$ ein Konzept.
- Ist R Rollenname, so ist $\exists R.\top$ ein Konzept.

Einschränkungen / Erweiterungen

Ziel bei Beschreibungslogiken ist es häufig, sehr effiziente Entscheidungsverfahren zu haben. Aus diesem Grund betrachtet man häufig nur noch Fragmente. Andererseits können diese wiederum zu schwach sein, um einen gewünschten Sachverhalt zu modellieren. Somit sind auch Erweiterungen denkbar.

Einschränkungen:

- $\mathcal{ALC}$: keine Disjunktionen von Konzepten
- $\mathcal{AL}$: keine Disjunktionen und Negationen nur auf atomaren Konzepten
- ...

Erweiterungen:

- $\mathcal{E} \dots$: existentielle Quantifizierung vor beliebigen Konzepten zulässig
- ...

Semantik und Modellierung

Beschreibungslogiken können einfach als Fragment von Modallogik aufgefasst und in Kripke-Strukturen interpretiert werden. Genauso kann man es gleich als Fragment von FO sehen und die Operatoren auf Konzepten durch Durchschnitt, Vereinigung, Komplement, etc. auf den 1-stelligen Relationen (Teilmengen des Universums) interpretieren.

Zur Modellierung von Sachverhalten verfolgt man jedoch häufig folgenden Ansatz.

- Eine **TBox** enthält Beziehungen zwischen Konzepten: $\varphi \sqsubseteq \psi$.
Sie beschreibt generelle Zusammenhänge zwischen Konzepten.
- Eine **ABox** ordnet Individuen (Konstantensymbole) in die durch die TBox gegebene Hierarchie der Konzepte ein.

Beispiel

Konzepte: *Person*, *Male*, *Female*

Rolle: *hasChild*

TBox:

$$Person \sqsubseteq Male \sqcup Female$$
$$Male \sqsubseteq Person$$
$$Female \sqsubseteq Person$$
$$Parent \sqsubseteq \exists hasChild. Person \sqcap \forall hasChild. Person$$

ABox:

$$John : Male$$
$$John hasChild Bill$$

Entscheidungsprobleme

Die wichtigsten Entscheidungsprobleme bei Beschreibungslogiken sind

- Das **Subsumptionsproblem**: Gegeben TBox $\mathcal{T}$ und zwei Konzepte φ, ψ , gilt $\varphi \sqsubseteq \psi$ in jeder Interpretation, die $\mathcal{T}$ erfüllt?
- Das **Konsistenzproblem**: Gegeben TBox $\mathcal{T}$ und ABox $\mathcal{A}$, gibt es ein Modell, welches alle Definitionen in $\mathcal{T}$ und $\mathcal{A}$ erfüllt?