Kapitel 8

Ausblick auf weitere Logiken

Kontext und Ziele

In diesem Kapitel führen kurz zwei weitere Logiken ein:

- Die Logik der zweiten Stufe ist eine sehr mächtige Erweiterung der Logik der 1. Stufe. Sie ist deutlich ausdrucksstärker als die Logik der 1. Stufe. Viele der wichtigen Eigenschaften der Logik der 1. Stufe lassen sich aber nicht erweitern.
- Die Modallogik liegt zwischen Aussagenlogik und Logik der 1. Stufe. Sie ist ausdrucksschwächer als die Logik der 1. Stufe, hat aber dafür deutlich bessere algorithmische Eigenschaften, etwa eine entscheidbares Erfüllbarkeitsproblem.

8.1 Die Logik der 2. Stufe

Symbole und Variablen

- Wie üblich bezeichnet σ eine Symbolmenge.
- Neben den Variablen der Logik der 1. Stufe, die wir in diesem Kontext als Individuenvariablen bezeichnen, verwenden wir in der Logik der 2. Stufe auch noch Relationsvariablen.
- Jede Relationsvariable X hat eine Stelligkeit $\text{stell}(X) \in \mathbb{N}$.
- Neben der Menge Var von Individuenvariablen halten wir auch noch eine abzählbare Menge Var_R von Relationsvariablen fest, die für jedes $k \in \mathbb{N}$ unendliche viele k-stellige Relationsvariablen enthält.
- Wir bezeichnen Relationsvariablen mit lateinischen Großbuchstaben X, Y, Z, und verwenden die Schreibweise X/k um anzuzeigen, dass $\text{stell}(X) = k$ ist.
- Das Alphabet der Logik der 2. Stufe über σ ist

$$\Sigma_{\text{SO}(\sigma)} := \Sigma_{\text{L}(\sigma)} \cup \text{Var}_\text{R} .$$

Definition 8.1

Die Menge $\mathrm{SO}(\sigma) \subseteq \Sigma^*_{\mathrm{SO}(\sigma)}$ aller σ-Formeln der Logik der 2. Stufe ist rekursiv wie folgt definiert.

(i) Für alle $\theta_1, \theta_2 \in \mathrm{T}(\sigma)$ ist $\theta_1 \doteq \theta_2 \in \mathrm{SO}(\sigma)$.

(ii) Für alle $k \in \mathbb{N}$, alle k-stelligen Relationssymbole $R \in \sigma$ und alle $\theta_1, \dots, \theta_k \in \mathrm{T}(\sigma)$ ist $R(\theta_1, \dots, \theta_k) \in \mathrm{SO}(\sigma)$.

(iii) Für alle $k \in \mathbb{N}$, alle k-stelligen Relationsvariablen $X \in \mathrm{Var}_\mathrm{R}$ und alle $\theta_1, \dots, \theta_k \in \mathrm{T}(\sigma)$ ist $X(\theta_1, \dots, \theta_k) \in \mathrm{SO}(\sigma)$.

(iv) $\bot, \top \in \mathrm{SO}(\sigma)$.

(v) Wenn $\varphi, \psi \in \mathrm{SO}(\sigma)$, dann $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi) \in \mathrm{SO}(\sigma)$.

(vi) Für alle $x \in \mathrm{Var}$, wenn $\varphi \in \mathrm{SO}(\sigma)$, dann $\exists x\varphi, \forall x\varphi \in \mathrm{SO}(\sigma)$.

(vii) Für alle $X \in \mathrm{Var}_\mathrm{R}$, wenn $\varphi \in \mathrm{SO}(\sigma)$, dann $\exists X\varphi, \forall X\varphi \in \mathrm{SO}(\sigma)$.

Ergänzungen zu Seite 8.5

SO steht für <u>S</u>econd-<u>O</u>rder Logic. Eine andere übliche Bezeichnung für die Logik ist L^{II}.

Die Logik der 1. Stufe wird häufig auch mit FO für <u>F</u>irst-<u>O</u>rder Logic bezeichnet.

Zweitstufige Belegungen und Interpretationen

Definition 8.2

(1) Eine zweitstufige Belegung in einer Menge A ist eine Abbildung $\mathfrak{b}$, die jeder Individuenvariablen $x \in \mathrm{Var}$ ein Element $\mathfrak{b}(x) \in A$ zuordnet und für jedes $k \in \mathbb{N}$ jeder k-stelligen Relationsvariablen $X \in \mathrm{Var}_{\mathrm{R}}$ eine k-stellige Relation $\mathfrak{b}(X) \subseteq A^k$.

(2) Eine zweitstufige σ-Interpretation ist ein Paar $\mathfrak{I} = (\mathfrak{A}, \mathfrak{b})$ bestehend aus einer σ-Struktur $\mathfrak{A}$ und einer zweitstufigen Belegung $\mathfrak{b}$ in A.

Die Semantik der Terme ist in der Logik der 2. Stufe im Vergleich zur Logik der 1. Stufe unverändert.

Definition 8.3

Sei $\theta \in \mathrm{T}(\sigma)$, und sei $\mathfrak{I} = (\mathfrak{A}, \mathfrak{b})$ eine zweitstufige σ-Interpretation.

Dann ist der Wert $[\![\theta]\!]^{\mathfrak{I}}$ von θ in der zweitstufigen Interpretation $\mathfrak{I}$ ist gleich dem Wert von θ in der (erststufigen) Interpretation $(A, \mathfrak{b}{\restriction}_{\mathrm{Var}})$, das heißt,

$$[\![\theta]\!]^{\mathfrak{I}} := [\![\theta]\!]^{(A, \mathfrak{b}{\restriction}_{\mathrm{Var}})} .$$

Definition 8.4

Den Wert $[\![\varphi]\!]^{\mathfrak{I}} \in \{0,1\}$ einer Formel $\varphi \in \mathrm{SO}(\sigma)$ in einer zweitstufigen σ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \mathfrak{b})$ definieren wir rekursiv über den Aufbau von φ.

- Für Formeln φ der Gestalt $\theta_1 \doteq \theta_2$, $R(\theta_1, \dots, \theta_k)$, $\bot$, $\top$, $\neg\psi$, $\psi_1 * \psi_2$ für $\in \{\wedge, \vee, \rightarrow\}$, $Qx\psi$ für $Q \in \{\exists, \forall\}$, $x \in \mathrm{Var}$ übernehmen wir die Definition der Logik der 1. Stufe.
- Für $\varphi = X(\theta_1, \dots, \theta_k)$, wobei $X/k \in \mathrm{Var_R}$, setzen wir

$$[\![X(\theta_1, \dots, \theta_k)]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{falls } \left([\![\theta_1]\!]^{\mathfrak{I}}, \dots, [\![\theta_k]\!]^{\mathfrak{I}}\right) \in \mathfrak{b}(X), \\ 0 & \text{sonst.} \end{cases}$$

- Für $\varphi = \exists X\psi$, wobei $X/k \in \mathrm{Var_R}$, setzen wir

$$[\![\exists X\psi]\!]^{\mathfrak{I}} := 1 \quad :\Longleftrightarrow \quad \text{es existiert eine } R \subseteq A^k, \text{ so dass } [\![\psi]\!]^{\mathfrak{I}\frac{R}{X}} = 1.$$

- Für $\varphi = \forall X\psi$, wobei $X/k \in \mathrm{Var_R}$, setzen wir

$$[\![\forall X\psi]\!]^{\mathfrak{I}} := 1 \quad :\Longleftrightarrow \quad \text{für alle } R \subseteq A^k \text{ gilt } [\![\psi]\!]^{\mathfrak{I}\frac{R}{X}} = 1.$$

Bemerkungen

- Wir können die Menge frei(φ) aller freien Variablen einer Formel $\varphi \in \mathrm{SO}(\sigma)$ ähnlich wie für die Logik der 1. Stufe definieren. Man beachte, dass frei(φ) sowohl Individuen- als auch Relationsvariablen enthalten kann.

  Sätze der Logik der 2. Stufe sind Formeln ohne freie Variablen.
- Für die Logik der 2. Stufe gilt dann das Koinzidenzlemma und das Isomorphielemma.
- Weiterhin gilt auch das Substitutionslemma. Zudem gibt es noch ein andere Art von Substitution, bei der man freie Relationsvariablen durch Formeln ersetzt.
- Auch für die Logik der 2. Stufe gibt es eine Negationsnormalform und folgende pränexe Normalform: *Jede Formel der $\varphi \in \mathrm{SO}(\sigma)$ ist äquivalent zu einer Formel der Gestalt*

$$Q_1 X_1 \cdots Q_k X_k Q_{k+1} x_1 \dots Q_{k+\ell} x_\ell \psi,$$

  wobei $Q_1, \dots, Q_{k+\ell} \in \{\exists, \forall\}$, $X_1, \dots, X_k \in \mathrm{Var}_{\mathrm{R}}$, $x_1, \dots, x_\ell \in \mathrm{Var}$ und ψ quantorenfrei.

Wir bezeichnen die Menge aller Formeln der Logik der zweiten Stufe mit SO, also

$$\mathsf{SO} := \bigcup_{\sigma \text{ Symbolmenge}} \mathsf{SO}(\sigma).$$

Definition 8.5

Sei $\mathsf{S} \subseteq \mathsf{SO}$. Ein Klasse $\mathscr{K}$ von σ-Strukturen ist S-definierbar, wenn es einen Satz $\varphi \in \mathsf{S}(\sigma) := \mathsf{S} \cap \mathsf{SO}(\sigma)$ gibt, so dass für alle σ-Strukturen $\mathfrak{A}$ gilt:

$$\mathfrak{A} \in \mathscr{K} \iff \mathfrak{A} \models \varphi.$$

Bemerkungen

- Entsprechend der erststufigen Definierbarkeit im Endlichen können wir auch S-Definierbarkeit im Endlichen definieren. Diesen Begriff benötigen wir allerdings in dieser Vorlesung nicht.
- Statt "erststufiger Definierbarkeit (im Endlichen)" können wir jetzt auch L-Definierbarkeit (im Endlichen) sagen, wobei $\mathsf{L} := \bigcup_\sigma \mathsf{L}(\sigma)$ die Menge aller Formeln der Logik der 1. Stufe bezeichnet.
- Teilmengen $\mathsf{S} \subseteq \mathsf{SO}$ bezeichnet man oft als Fragmente der Logik der 2. Stufe. In diesem Sinne ist die Logik der 1. Stufe ein Fragment der Logik der 2. Stufe.

  Wir werden zwei weitere wichtige Fragmente kennenlernen: $\exists$SO und MSO.
- S-Definierbarkeit können wir auch für beliebige Mengen von Formeln anderer Logiken betrachten. Später werden wir noch Definierbarkeit in der Modallogik ML untersuchen.

Beispiel 8.6

Die Klasse der zusammenhängenden Graphen ist SO-definierbar.

Beispiel 8.7

Für jede Symbolmenge σ ist die Klasse der endlichen σ-Strukturen SO-definierbar.

Zu Beispiel 8.6:

$\varphi_{\text{Graph}} \in \mathrm{L}(\sigma)$ sei eine Formel, die die Klasse aller Graphen definiert.

Beobachtung.

Ein Graph $\mathfrak{G} = (G, E^{\mathfrak{G}})$ ist genau dann zusammenhängend, wenn für jede Menge $W \subseteq G$ gilt: $W = \emptyset$ oder $W = G$ oder es gibt ein $w \in W$, $v \in G \setminus W$, so dass $(w, v) \in E^{\mathfrak{G}}$.

Wir setzen

$$\varphi_{\text{zshg}} := \varphi_{\text{Graph}} \wedge \forall X \Big(\forall x \neg X(x) \vee \forall x\, X(x) \vee \exists x \exists y \big(X(x) \wedge \neg X(y) \wedge E(x, y) \big) \Big).$$

Zu Beispiel 8.7:

Beobachtung.

Eine Menge A ist genau dann unendlich, wenn es eine totale Ordnung $\leq$ auf A gibt, so dass für alle $a \in A$ ein $b \in A \setminus \{a\}$ mit $a \leq b$ existiert.

Wir setzen

$$\begin{aligned}\psi_{\text{ord}} := {} & \forall x\, X(x,x) \\ & \wedge \forall x \forall y \big(X(x,y) \wedge X(y,x) \to x \doteq y \big) \\ & \wedge \forall x \forall y \forall z \big(X(x,y) \wedge X(y,z) \to X(x,z) \big) \\ & \wedge \forall x \forall y \big(X(x,y) \vee X(y,x) \big).\end{aligned}$$

Dann gilt für alle zweitstufigen σ-Interpretationen $\mathfrak{I} = (\mathfrak{A}, \mathfrak{b})$:

$$\mathfrak{I} \models \psi_{\text{ord}} \iff \mathfrak{b}(X) \text{ ist eine totale Ordnung auf } A.$$

Jetzt setzen wir

$$\varphi_{\text{endl}} := \neg \exists X \Big(\psi_{\text{ord}} \wedge \forall x \exists y \big(x \not\doteq y \wedge X(x,y) \big) \Big).$$

Endlichkeitssatz und Vollständigkeitssatz

Satz 8.8

Es gibt eine Formelmenge $\Phi \subseteq \mathrm{SO}(\emptyset)$, so dass gilt:

(i) *Jede endliche Teilmenge von Φ ist erfüllbar.*

(ii) *Φ ist unerfüllbar*

Der Endlichkeitssatz gilt also für die Logik der 2. Stufe nicht.

Bemerkung 8.9

Aus dem Satz folgt auch sofort, dass es keinen vollständigen Beweiskalkül für die Logik der 2. Stufe gibt, dass also auch kein Vollständigkeitssatz gilt.

Beweis von Satz 8.8.

Sei $\varphi_{\text{endl}} \in \text{SO}(\emptyset)$ ein Satz, der Klasse der endlichen $\emptyset$-Strukturen definiert. Für alle $n \in \mathbb{N}_{>0}$ sei

$$\varphi_n := \exists x_1 \ldots \exists x_n \bigwedge_{\substack{i,j \in [n] \\ i \neq j}} x_i \dot{\neq} x_j .$$

Wir setzen $\Phi := \{\varphi_{\text{endl}}\} \cup \{\varphi_n \mid n \in \mathbb{N}_{>0}\}$. Dann ist Φ unerfüllbar, aber es ist leicht zu sehen, dass jede endliche Teilmenge erfüllbar ist. □

Um die Aussage aus Bemerkung 8.9 zu präzisieren, müssten wir zunächst definieren, was ein "vollständiger Beweiskalkül" für eine Logik ist. Wir verzichten hier auf diese formale Definition und belassen es bei der intuitiven Bemerkung. Entscheidend ist, dass jeder formale Beweis in einem Beweiskalkül endlich ist und damit nur endlich viele Formeln verwendet.

Satz 8.10

Es gibt einen Satz $\varphi_{\mathsf{PA}} \in \mathsf{SO}(\sigma_{\mathsf{Ar}})$, *so dass für alle* σ_{Ar}*-Strukturen* $\mathfrak{A}$ *gilt:*

$$\mathfrak{A} \models \varphi_{\mathsf{PA}} \quad \Longleftrightarrow \quad \mathfrak{A} \cong \mathfrak{N}.$$

Wir sagen auch, dass $\mathfrak{N}$, *das Standardmodell der Arithmetik,* SO-*axiomatisierbar ist.*

Bemerkung 8.11

Der Satz φ_{PA} formalisiert die sogenannten Peano-Axiome für die Arithmetik.

Beweis.
Wir setzen

$$
\begin{aligned}
\varphi_{\mathrm{PA}} :=\ & \dot{0} \dot{+} \dot{1} \doteq \dot{1} && \text{Nachfolgeraxiome}\\
& \wedge \forall x\, \neg x \dot{+} \dot{1} \doteq \dot{0} \\
& \wedge \forall x \forall y (x \dot{+} \dot{1} \doteq y \dot{+} \dot{1} \to x \doteq y) \\
& \wedge \forall X \Big(X(\dot{0}) \wedge \forall x (X(x) \to X(x \dot{+} \dot{1})) \to \forall x X(x) \Big) && \text{Induktionsaxiom}\\
& \wedge \forall x\, x \dot{+} \dot{0} \doteq x && \text{Axiomatisierung der Addition}\\
& \wedge \forall x \forall y\, x \dot{+} (y \dot{+} \dot{1}) \doteq (x \dot{+} y) \dot{+} \dot{1} \\
& \wedge \forall x\, x \dot{*} \dot{0} \doteq \dot{0} && \text{Axiomatisierung der Multiplikation}\\
& \wedge \forall x \forall y\, x \dot{*} (y \dot{+} \dot{1}) \doteq (x \dot{*} y) \dot{+} x.
\end{aligned}
$$

„$\Longleftarrow$“: Es ist leicht zu sehen, dass $\mathfrak{N} \models \varphi_{\mathrm{PA}}$. Nach dem Isomorphielemma gilt dann auch $\mathfrak{A} \models \varphi_{\mathrm{PA}}$ für alle $\mathfrak{A} \cong \mathfrak{N}$.

„$\Longrightarrow$“: Nehmen wir an, $\mathfrak{A} \models \varphi_{\text{PA}}$. Wir müssen zeigen, dass $\mathfrak{A} \cong \mathfrak{N}$.

Wir definieren rekursiv für alle $n \in \mathbb{N}$ einen Term η_n: wir setzen $\eta_0 := \dot{0}$ und $\eta_{n+1} := \eta_n \dot{+} \dot{1}$. Dann gilt für alle $n \in \mathbb{N}$:

$$[\![\eta_n]\!]^{\mathfrak{N}} = n.$$

Für alle $n \in \mathbb{N}$ sei

$$a_n := [\![\eta_n]\!]^{\mathfrak{A}}.$$

Wir definieren $\pi : \mathbb{N} \to A$ durch $\pi(n) := a_n$. Wir werden zeigen, dass π ein Isomorphismus ist.

Behauptung 1

Es gilt

$$a_0 = \dot{0}^{\mathfrak{A}} \qquad \text{und} \qquad a_1 = \dot{1}^{\mathfrak{A}}.$$

Also $\pi(\dot{0}^{\mathfrak{N}}) = \dot{0}^{\mathfrak{A}}$ und $\pi(\dot{1}^{\mathfrak{N}}) = \dot{1}^{\mathfrak{A}}$.

Beweis.

Weil $\eta_0 = \dot{0}$ gilt $a_0 = [\![\eta_0]\!]^{\mathfrak{A}} = \dot{0}^{\mathfrak{A}}$.

Weil $\eta_1 = \dot{0} \dot{+} \dot{1}$ gilt

$$a_1 = [\![\dot{0} \dot{+} \dot{1}]\!]^{\mathfrak{A}} = \dot{0}^{\mathfrak{A}} \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} = \dot{1}^{\mathfrak{A}}.$$

Die letzte Gleichung gilt, weil $\mathfrak{A} \models \dot{0} \dotplus \dot{1} \doteq \dot{1}$. ⌟

Behauptung 2

Für alle $m, n \in \mathbb{N}$ gilt:

$$a_{m+n} = a_m \dotplus^{\mathfrak{A}} a_n.$$

Also $\pi(m \dotplus^{\mathfrak{N}} n) = \pi(m) \dotplus^{\mathfrak{A}} \pi(n)$.

Beweis.

Sei $m \in \mathbb{N}$. Wir zeigen die Behauptung per Induktion über n.

$n = 0$:

Es gilt

$$a_{m+0} = a_m = a_m \dotplus^{\mathfrak{A}} \dot{0}^{\mathfrak{A}} = a_m \dotplus^{\mathfrak{A}} a_0.$$

Die zweite Gleichung gilt, weil $\mathfrak{A} \models \forall x\; x \dotplus \dot{0} \doteq x$, und die dritte Gleichung folgt aus Behauptung 1.

$n \to n+1$:

Nach der Definition der Terme η_k gilt für alle $k \in \mathbb{N}$

$$a_{k+1} = [\![\eta_{k+1}]\!]^{\mathfrak{A}} = [\![\eta_k \dotplus \dot{1}]\!]^{\mathfrak{A}} = [\![\eta_k]\!]^{\mathfrak{A}} \dotplus^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} = a_k \dotplus^{\mathfrak{A}} \dot{1}^{\mathfrak{A}}. \qquad (\star)$$

Also

$$
\begin{aligned}
a_{m+(n+1)} &= a_{(n+m)+1} \\
&= a_{n+m} \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} && (\star) \text{ mit } k = m+n \\
&= (a_m \dot{+}^{\mathfrak{A}} a_n) \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} && \text{Induktionsannahme} \\
&= a_m \dot{+}^{\mathfrak{A}} (a_n \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}}) && \text{weil } \mathfrak{A} \models \forall x \forall y\ x \dot{+} (y \dot{+} \dot{1}) \doteq (x \dot{+} y) \dot{+} \dot{1} \\
&= a_m \dot{+}^{\mathfrak{A}} a_{n+1} && (\star) \text{ mit } k = n.
\end{aligned}
$$

Das beweist Behauptung 2. ⌟

Behauptung 3

Für alle $m, n \in \mathbb{N}$ gilt:

$$a_{m \cdot n} = a_m \dot{*}^{\mathfrak{A}} a_n.$$

Also $\pi(m \dot{*}^{\mathfrak{N}} n) = \pi(m) \dot{*}^{\mathfrak{A}} \pi(n)$.

Beweis.

Sei $m \in \mathbb{N}$. Wir zeigen die Behauptung per Induktion über n.

$n = 0$:
Es gilt

$$a_{m\cdot 0} = a_0 = a_m \dot{*}^{\mathfrak{A}} \dot{0}^{\mathfrak{A}} = a_m \dot{*}^{\mathfrak{A}} a_0 .$$

Die zweite Gleichung gilt, weil $\mathfrak{A} \models \forall x\, x \dot{*} \dot{0} \doteq \dot{0}$.

$n \to n+1$:
Es gilt

$$\begin{aligned} a_{m\cdot(n+1)} &= a_{(n\cdot m)+m} \\ &= a_{n\cdot m} \dot{+}^{\mathfrak{A}} a_m && \text{Behauptung 2} \\ &= (a_m \dot{*}^{\mathfrak{A}} a_n) \dot{+}^{\mathfrak{A}} a_m && \text{Induktionsannahme} \\ &= a_m \dot{*}^{\mathfrak{A}} (a_n \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}}) && \text{weil } \mathfrak{A} \models \forall x \forall y\; x \dot{*} (y \dot{+} \dot{1}) \doteq (x \dot{*} y) \dot{+} x \\ &= a_m \dot{*}^{\mathfrak{A}} a_{n+1} && (\star) \text{ mit } k = n. \end{aligned}$$

Das beweist Behauptung 3. ⌟

Behauptung 4

π ist injektiv.

Beweis.

Wenn π ist nicht injektiv ist, gibt es $m, n \in \mathbb{N}$, so dass $m < n$ und $a_m = a_n$. Wir zeigen per Induktion über m, dass $a_m \neq a_n$ für alle $n > m$.

$m = 0$:

Angenommen, $a_0 = a_n$ für ein $n \geq 1$. Dann gilt

$$\dot{0}^{\mathfrak{A}} = a_0 = a_{(n-1)+1} = a_{n-1} \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} .$$

Das kann aber nicht sein, weil $\mathfrak{A} \models \forall x \, \neg x \dot{+} \dot{1} \doteq \dot{0}$. *Widerspruch*.

$m \to m + 1$:

Angenommen, $a_{m+1} = a_{n+1}$ für ein $n \geq m + 1$. Dann gilt

$$\mathfrak{A} \models \eta_m \dot{+} \dot{1} \doteq \eta_n \dot{+} \dot{1} .$$

Weil $\mathfrak{A} \models \forall x \forall y (x \dot{+} \dot{1} \doteq y \dot{+} \dot{1} \to x \doteq y)$ folgt

$$\mathfrak{A} \models \eta_m \doteq \eta_n .$$

Also gilt $a_m = a_n$, was der Induktionsannahme *widerspricht*. ⌟

Behauptung 5

π ist surjektiv.

Beweis.

Sei $B := \text{bild}(\pi) = \{a_i \mid i \in \mathbb{N}\}$. Es gilt $\dot{0}^{\mathfrak{B}} = a_0 \in B$, und für alle $b \in B$ gilt $b \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} \in B$, denn wenn $b = a_n$ ist $b \dot{+}^{\mathfrak{A}} \dot{1}^{\mathfrak{A}} = a_{n+1}$. Weil $\mathfrak{A}$ das Induktionsaxiom erfüllt gilt dann $B = A$, also ist π surjektiv. ⌟

Behauptungen 1–5 zeigen, dass π ein Isomorphismus ist. □

Die monadische Logik der 2. Stufe

Definition 8.12

(1) Eine Formel $\varphi \in \mathrm{SO}(\sigma)$ ist monadisch, wenn alle Relationsvariablen in $X \in \mathrm{Var}_{\mathrm{R}}$, die in φ vorkommen, einstellig sind.

(2) Die Menge aller monadischen Formeln in $\mathrm{SO}(\sigma)$ bezeichnen wir mit $\mathrm{MSO}(\sigma)$.

Bemerkung 8.13

Einstellige Relationsvariablen bezeichnen wir auch als Mengenvariablen.

Definierbarkeit der endlichen linearen Ordnungen

Satz 8.14

Die Klasse der endlichen $\emptyset$-Strukturen ist nicht MSO*-definierbar.*

(Ohne Beweis.)

Satz 8.15

Es gibt einen Satz $\varphi \in \mathrm{MSO}(\{\dot{\leq}\})$, der die Klasse aller endlichen total geordneten Mengen definiert.

Korollar 8.16

Der Endlichkeitssatz gilt für die monadische Logik der 2. Stufe nicht.

Beweis von Satz 8.15.

Sei $\psi_{\mathrm{ord}} \in \mathrm{L}(\sigma)$ ein Satz der Logik der 1. Stufe, der die Klasse der total geordneten Mengen definiert.

Beobachtung.

Eine total geordnete Menge $(A, \leq)$ ist genau dann endlich, wenn es keine unendliche aufsteigende und keine unendliche absteigende Folge gibt, wenn also jede Teilmenge $B \subseteq A$ bezüglich $\leq$ ein kleinstes und ein größtes Element hat.

Also definiert folgender Satz die Klasse der endlichen total geordneten Mengen

$$\varphi := \psi_{\mathrm{ord}} \wedge \underbrace{\forall X \exists x \Big(X(x) \wedge \forall y \big(X(y) \to x \dot{\leq} y \big) \Big)}_{\text{Jede Teilmenge hat ein Minimum}} \wedge \underbrace{\forall X \exists x \Big(X(x) \wedge \forall y \big(X(y) \to y \dot{\leq} x \big) \Big)}_{\text{Jede Teilmenge hat ein Maximum}} .$$

□

Wörter und Sprachen

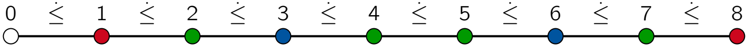
Sei Σ ein endliches Alphabet.

Zur Erinnerung

Wir können Wörter $w \in \Sigma^*$ durch Strukturen $\mathfrak{A}_w$ über dem Alphabet $\sigma_\Sigma = \{\dot{\leq}\} \cup \{P_a \mid a \in \Sigma\}$ beschreiben.

Beispiel 8.17

Für das Wort $w = abcbbcba$ über dem Alphabet $\Sigma = \{a, b, c\}$ sieht die Struktur $\mathfrak{A}_w$ folgendermaßen aus:



Für eine Sprache $L \subseteq \Sigma^*$ sei

$$\mathscr{K}_L := \{\mathfrak{A} \mid \text{es gibt ein } w \in L, \text{ so dass } \mathfrak{A} \cong \mathfrak{A}_w\}.$$

Der Satz von Büchi und Trachtenbrot

Beobachtung 8.18

Die Klasse $\mathscr{K}_{\Sigma^*}$ aller Wortstrukturen ist MSO*-definierbar.*

Satz 8.19

Für alle $L \subseteq \Sigma^*$ gilt:

$$L \text{ ist regulär} \quad \Longleftrightarrow \quad \mathscr{K}_L \text{ ist } \mathrm{MSO}\text{-definierbar}.$$

(Ohne Beweis.)

Ergänzungen zu Seite 8.18

Für die Beobachtung verwenden wir, dass die Klasse der endlichen total geordneten Strukturen MSO-definierbar ist. Wortstrukturen über Σ^* sind endliche σ_Σ-Strukturen $\mathfrak{A}$, in denen $\dot{\leq}^{\mathfrak{A}}$ eine totale Ordnung ist, das kleinste Element in keiner einstelligen Relation ist, und alle anderen Elemente in genau einer einstelligen Relation sind.

Die existentielle Logik der 2. Stufe

Definition 8.20

(1) Eine Formel $\varphi \in \mathrm{SO}(\sigma)$ ist erststufig, wenn sie keine Quantifikation über Relationsvariablen enthält.

(2) Eine Formel $\varphi \in \mathrm{SO}(\sigma)$ ist existentiell, wenn sie die Gestalt $\exists X_1 \ldots \exists X_k \psi$ hat, wobei ψ erststufig ist.

(3) Die Menge aller existentiellen Formeln in $\mathrm{SO}(\sigma)$ bezeichnen wir mit $\exists\mathrm{SO}(\sigma)$.

Beispiel 8.21

Die Klasse der 3-färbbaren Graphen ist $\exists$SO-definierbar (sogar durch einen Satz in $\exists\mathrm{SO} \cap \mathrm{MSO}$).

Beispiel 8.22

Die Klasse der hamiltonischen Graphen (also Graphen mit einem Kreis, der durch alle Knoten geht) ist $\exists$SO-definierbar, aber nicht MSO-definierbar. (Ohne Beweis.)

Eine erststufige SO-Formel darf Relationsvariablen enthalten, diese dürfen nur nicht quantifiziert sein. Man kann eine erststufige Formel $\varphi \in \mathrm{SO}(\sigma)$ als Formel in

$$\mathrm{L}\big(\sigma \cup \mathrm{Var}_{\mathrm{R}}\big)$$

auffassen.

Zu Beispiel 8.21.

Folgender Satz definiert die Klasse der 3-färbbaren Graphen:

$$\begin{aligned}\varphi_{3\mathrm{col}} := \exists X \exists Y \exists Z \Bigg(& \forall x \Big(\big(X(x) \vee Y(x) \vee Z(x) \big) \wedge \neg \big(X(x) \wedge Y(x) \big) \wedge \neg \big(X(x) \wedge Z(x) \big) \wedge \neg \big(Y(x) \wedge Z(x) \big) \Big) \\ & \wedge \forall x \forall y \Big(E(x, y) \to \neg \big(X(x) \wedge X(y) \big) \wedge \neg \big(Y(x) \wedge Y(y) \big) \wedge \neg \big(Z(x) \wedge Z(y) \big) \Big) \Bigg)\end{aligned}$$

Entscheidungsprobleme als Strukturklassen

Wir können Entscheidungsprobleme als Klassen endlicher Strukturen auffassen.

Beispiel 8.23

Das 3-Färbbarkeitsproblem entspricht der Klasse aller endlichen 3-färbbaren Graphen.

Beispiel 8.24

Das Entscheidungsproblem für eine Sprache $L \subseteq \Sigma^*$ entspricht der Klasse $\mathscr{K}_L$ von Wortstrukturen.

Umgekehrt entspricht jede Klasse $\mathscr{K}$ von σ-Strukturen dem Entscheidungsproblem:

$\mathscr{K}$

Eingabe:	Endliche σ-Struktur $\mathfrak{A}$.
Frage:	Gilt $\mathfrak{A} \in \mathscr{K}$?

Ergänzungen zu Seite 8.20

Die Modellierung von Entscheidungsproblemen durch Strukturklassen ist oft einfacher und direkter als die Modellierung durch Sprachen über einem endlichen Alphabet, weil wir uns „künstliche“ Kodierungsschritte wie die Kodierung von Graphen durch Adjazenzmatrizen ersparen.

Beispiel 8.24 zeigt, dass die Modellierung von Entscheidungsproblemen als Sprachen ein Spezialfall der Modellierung durch Strukturklassen ist.

Satz 8.25

Für alle Klasse $\mathscr{K}$ von endlichen Strukturen sind folgende Aussagen äquivalent:

(i) $\mathscr{K}$ *(aufgefasst als Entscheidungsproblem) ist in der Komplexitätsklasse* NP.

(ii) $\mathscr{K}$ *ist* $\exists$SO*-definierbar.*

(Ohne Beweis.)

8.2 Die Modallogik

Symbolmenge und Alphabet

Die Modallogik verwendet *aussagenlogische* Symbolmengen.

Das Alphabet der Modallogik über σ ist

$$\Sigma_{\mathrm{ML}(\sigma)} := \sigma \cup \{\bot, \top, \neg, \vee, \wedge, \to, (,), \Box, \Diamond\}.$$

Definition 8.26

Sei σ eine aussagenlogische Symbolmenge. Die Menge $\mathrm{ML}(\sigma) \subseteq \Sigma^*_{\mathrm{ML}(\sigma)}$ der modallogischen Formeln über σ ist die wie folgt rekursiv definiert:

(i) $P \in \mathrm{ML}(\sigma)$ für alle $P \in \sigma$.

(ii) $\bot, \top \in \mathrm{ML}(\sigma)$.

(iii) Wenn $\varphi, \psi \in \mathrm{ML}(\sigma)$, dann $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi) \in \mathrm{ML}(\sigma)$.

(iv) Wenn $\varphi \in \mathrm{ML}(\sigma)$, dann $\Box\varphi, \Diamond\varphi \in \mathrm{ML}(\sigma)$.

Bemerkungen

- $\Box\varphi$ lesen wir als „Box φ“ und $\Diamond\varphi$ als „Diamond φ“.
- Wir verwenden die üblichen Klammerkonventionen. Die Modaloperatoren $\Box$ und $\Diamond$ binden stärker als alle Junktoren.
- Für den Rest des Kapitels halten wie eine abzählbar unendliche aussagenlogische Symbolmenge σ fest und schreiben ML statt ML(σ).

Beobachtung 8.27

Die Menge AL *der aussagenlogischen Formeln ist die Teilmenge von* ML, *die aus allen Formeln besteht, in denen* $\Box$ *und* $\Diamond$ *nicht vorkommen.*

Definition 8.28

Eine Kripkestruktur ist ein Tupel $\mathfrak{A} = \left(A, E^{\mathfrak{A}}, \mathrm{al}^{\mathfrak{A}}\right)$, wobei

- $A \neq \emptyset$ eine Menge,
- $E^{\mathfrak{A}} \subseteq A^2$,
- $\mathrm{al}^{\mathfrak{A}} : A \times \sigma \to \{0, 1\}$.

Bemerkungen 8.29

Sei $\mathfrak{A}$ eine Kripkestruktur.

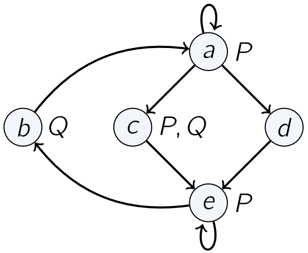
- Wir bezeichnen A als das Universum von $\mathfrak{A}$ und die Elemente $a \in A$ als Welten.
- $E^{\mathfrak{A}}$ ist die Erreichbarkeitsrelation zwischen den Welten. Eine Welt $b \in A$ ist von einer Welt $a \in A$ erreichbar, wenn $(a, b) \in E^{\mathfrak{A}}$. Die Menge aller von a aus erreichbaren Welten bezeichnen wir mit $N^{\mathfrak{A}}(a)$.
- $\mathrm{al}^{\mathfrak{A}}$ ordnet jeder Welt $a \in A$ ein aussagenlogische Interpretation $\mathrm{al}^{\mathfrak{A}}(a, \cdot) : \sigma \to \{0, 1\}$ zu, die wir als eine (aussagenlogische) Beschreibung der Welt a auffassen.

Ergänzungen zu Seite 8.26

Man nennt den Digraphen $(A, E^{\mathfrak{A}})$ auch den Rahmen der Kripkestruktur $\mathfrak{A}$.

Alternativ können wir eine Kripkestruktur als ein Transitionssystem auffassen. Welten sind dann Zustände, die Erreichbarkeitsrelation ist die Übergangsrelation (oder Transitionsrelation) zwischen den Zuständen. Die Funktion $\mathrm{al}^{\mathfrak{A}}(v, \cdot)$ gibt die (beobachtbaren) Eigenschaften der Zustände.

Beispiel 8.30



Kripkestruktur $\mathfrak{A}$ mit

- Universum $A = \{a, b, c, d, e\}$;
- Erreichbarkeitsrelation

$$E^{\mathfrak{A}} = \big\{(a,a),(a,c),(a,d),(c,e),(d,e),\\ (e,e),(e,b),(b,a)\big\}$$

- $\mathrm{al}^{\mathfrak{A}}$ ist gegeben durch folgende Tabelle

$\mathrm{al}^{\mathfrak{A}}$	a	b	c	d	e
P	1	0	1	0	1
Q	0	1	1	0	0

Definition 8.31

Wir definieren rekursiv für jede modallogische Formel $\varphi \in \mathrm{ML}$, jede Kripkestruktur $\mathfrak{A}$, und jede Welt $a \in A$ einen Wahrheitswert $[\![\varphi]\!]^{\mathfrak{A},a} \in \{0,1\}$:

(i) Für $P \in \sigma$ setzen wir $[\![P]\!]^{\mathfrak{A},a} := \mathrm{al}^{\mathfrak{A}}(a, P)$.

(ii)–(iii) Für Formeln φ der Gestalt $\bot$, $\top$, $\neg\psi$, $\psi_1 * \psi_2$ für $\in \{\wedge, \vee, \rightarrow\}$ übernehmen wir die Definition der Aussagenlogik.

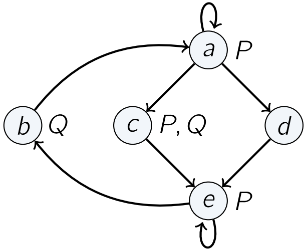
(iv) $$[\![\Box\varphi]\!]^{\mathfrak{A},a} := \begin{cases} 1 & \text{wenn } [\![\varphi]\!]^{\mathfrak{A},b} = 1 \text{ für alle } b \in N^{\mathfrak{A}}(a), \\ 0 & \text{sonst,} \end{cases}$$

$$[\![\Diamond\varphi]\!]^{\mathfrak{A},a} := \begin{cases} 1 & \text{wenn } [\![\varphi]\!]^{\mathfrak{A},b} = 1 \text{ für mindestens ein } b \in N^{\mathfrak{A}}(a), \\ 0 & \text{sonst.} \end{cases}$$

Notation

Statt $[\![\varphi]\!]^{\mathfrak{A},a} = 1$ schreiben wir $\mathfrak{A}, a \models \varphi$.

Beispiel 8.32



In der abgebildeten Kripkestruktur $\mathfrak{A}$ gilt in der Welt a:

$$\mathfrak{A}, a \overset{?}{\models}\models \Diamond P$$

$$\mathfrak{A}, a \overset{?}{\models}\not\models \Box P$$

$$\mathfrak{A}, a \overset{?}{\models}\not\models \Box(Q \vee \neg P)$$

$$\mathfrak{A}, a \overset{?}{\models}\models \Diamond\Box P$$

$$\mathfrak{A}, a \overset{?}{\models}\models \Diamond\Box\Diamond P.$$

Klassische Interpretation der Semantik: Modallogik als Wissenslogik

- Der $\Box$-Operator trifft Aussagen über Wissen: Wir interpretieren die Formel $\Box\varphi$ als:
  Ich (bzw. ein Agent) weiß, dass φ gilt.
- Unser Wissen über die Welt ist unvollständig, deswegen sind mehrere Welten mit unserem Wissen verträglich.
  Die Erreichbarkeitsrelation verbindet die tatsächliche Welt (also die Welt, in der wir uns befinden) mit allen möglichen Welten (also Welten, die mit unserem Wissen verträglich sind.
- Unter dieser Interpretation bedeutet $\Diamond\varphi$:
  Es ist möglich (d.h., mit meinem Wissen verträglich), dass φ gilt.
- Es gibt eine Reihe von Varianten dieser Interpretation, in denen $\Box\varphi$ etwa gelesen wird als:
  - *Ich glaube φ.*
  - *φ ist beweisbar.*

Ergänzungen zu Seite 8.30

Je nach intendierter Interpretation kann man den Rahmen der Kripkestrukturen $\mathfrak{A}$ einschränken. Für die Wissensinterpretation bietet es sich zum Beispiel an, zu verlangen, dass $E^{\mathfrak{A}}$ reflexiv ist. Intuitiv bedeutet das: „Wenn ich etwas weiß, dann gilt es in meiner Welt.“ Formal gilt in allen Kripkestrukturen $\mathfrak{A}$ mit reflexivem Rahmen für alle $\varphi \in \mathrm{ML}$:

$$\Box\varphi \to \varphi.$$

Eine alternative Interpretation: Modallogik als Programmlogik

- Wir interpretieren Kripkestrukturen als Transitionssysteme, Welten sind also Zustände eines Systems oder Programms.
- Man interpretiert dann $\Box\varphi$ als:
  In allen Nachfolgezuständen des aktuellen Zustands gilt φ.
- Jetzt können wir Korrektheitseigenschaften formalisieren, etwa $\varphi \to \Box\psi$:
  Wenn im aktuellen Zustand φ gilt, dann gilt in allen Nachfolgezuständen ψ.

Semantische Begriffe

Grundlegende semantische Begriffe wie Erfüllbarkeit einer modallogischen Formel oder Formelmenge, Allgemeingültigkeit einer Formel, Äquivalenz zweier Formeln ((wir schreiben: $\varphi \equiv \psi$), Folgerung einer Formel aus einer Formelmenge ($\Phi \models \varphi$) sind wie üblich definiert.

Zum Beispiel ist $\varphi \in \text{ML}$ allgemeingültig, wenn für alle Kripkestrukturen $\mathfrak{A}$ und alle $a \in A$ gilt: $\mathfrak{A}, a \models \varphi$.

Beispiel 8.33

Für alle Formeln $\varphi, \psi \in \text{ML}$ ist folgende Formel allgemeingültig:

$$\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$$

Zu Beispiel 8.33.

Sei $\mathfrak{A}$ eine Kripkestruktur und $a \in A$. Wir wollen zeigen, dass

$$\mathfrak{A}, a \models \Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi).$$

Nehmen wir an, $\mathfrak{A}, a \models \Box(\varphi \to \psi)$, sonst ist nichts zu zeigen. Jetzt müssen wir zeigen, dass $\mathfrak{A}, a \models \Box\varphi \to \Box\psi$. Nehmen weiter an, dass $\mathfrak{A}, a \models \Box\varphi$. Dann müssen wir zeigen, dass $\mathfrak{A}, a \models \Box\psi$.

Sei $b \in N^{\mathfrak{A}}(a)$. Dann gilt $\mathfrak{A}, b \models \varphi$, weil $\mathfrak{A}, a \models \Box\varphi$, und $\mathfrak{A}, b \models \varphi \to \psi$, weil $\mathfrak{A}, a \models \Box(\varphi \to \psi)$. Also gilt $\mathfrak{A}, b \models \psi$. Weil b eine beliebige von a erreichbare Welt ist, folgt $\mathfrak{A}, a \models \Box\psi$.

Für die Modallogik gelten die üblichen aussagenlogischen Äquivalenzen. Außerdem gelten folgende Äquivalenzen für die Modaloperatoren.

Lemma 8.34

Für alle Formeln $\varphi, \psi \in \mathrm{ML}$ gelten folgende Äquivalenzen:

(1) $\neg\Box\varphi \equiv \Diamond\neg\varphi$.

(2) $\Box(\varphi \wedge \psi) \equiv (\Box\varphi \wedge \Box\psi)$.

(3) $\Diamond(\varphi \vee \psi) \equiv (\Diamond\varphi \vee \Diamond\psi)$.

Korollar 8.35

Jede modallogische Formel ist äquivalent zu einer Formel in Negationsnormalform.

Korollar 8.36

Jede modallogische Formel ist äquivalent zu einer Formel, in der nur Aussagensymbole, die Junktoren $\neg$, $\wedge$, und der Operator $\Box$ vorkommen.

Beweis von Lemma 8.34.

Sei $\mathfrak{A}$ eine Kripkestruktur und $a \in A$. Dann gilt:

$$\begin{aligned}
\mathfrak{A}, a \models \neg\Box\varphi &\iff \text{es gilt nicht für alle } b \in N^{\mathfrak{A}}(a), \text{ dass } \mathfrak{A}, b \models \varphi \\
&\iff \text{es gibt ein } b \in N^{\mathfrak{A}}(a), \text{ so dass } \mathfrak{A}, b \not\models \varphi \\
&\iff \text{es gibt ein } b \in N^{\mathfrak{A}}(a), \text{ so dass } \mathfrak{A}, b \models \neg\varphi \\
&\iff \mathfrak{A}, a \models \Diamond\neg\varphi
\end{aligned}$$

Das zeigt (1). Aussagen (2) und (3) lassen sich ähnlich einfach beweisen. $\square$

Einbettung in die Logik der 1. Stufe

Definition 8.37

(1) Für alle $P \in \sigma$ sei $\widetilde{P}$ ein 1-stelliges Relationssymbol, und es sei

$$\widetilde{\sigma} := \{E\} \cup \{\widetilde{P} \mid P \in \sigma\}.$$

Wie üblich ist hier E ein 2-stelliges Relationssymbol.

(2) Für jede Kripkestruktur $\mathfrak{A}$ sei $\widetilde{\mathfrak{A}}$ folgende $\widetilde{\sigma}$-Struktur:

- $\widetilde{A} := A$;
- $E^{\widetilde{\mathfrak{A}}} := E^{\mathfrak{A}}$;
- $\widetilde{P}^{\widetilde{\mathfrak{A}}} := \{a \in A \mid \mathrm{al}^{\mathfrak{A}}(a, P) = 1\}$ für alle $P \in \sigma$.

Lemma 8.38

Die durch $\mathfrak{A} \mapsto \widetilde{\mathfrak{A}}$ definierte Abbildung ist eine bijektive Abbildung zwischen der Klasse aller Kripkestrukturen (über der Symbolmenge σ) und der Klasse aller $\widetilde{\sigma}$-Strukturen.

Beweis.

Wir definieren die Umkehrabbildung: für jede $\widetilde{\sigma}$-Struktur $\mathfrak{B}$ sei $\overline{\mathfrak{B}}$ die Kripkestruktur mit

- $\overline{B} := B$;
- $E^{\overline{\mathfrak{B}}} := E^{\mathfrak{B}}$;
- $\overline{\mathrm{al}^{\mathfrak{B}}} : \overline{B} \times \sigma$ definiert durch

$$\overline{\mathrm{al}^{\mathfrak{B}}}(b, P) := \begin{cases} 1 & \text{falls } b \in \widetilde{P}^{\mathfrak{B}}, \\ 0 & \text{sonst.} \end{cases}$$

Es ist leicht zu sehen, dass

- $\widetilde{\overline{\mathfrak{B}}} = \mathfrak{B}$ für alle $\widetilde{\sigma}$-Strukturen $\mathfrak{B}$;
- $\overline{\widetilde{\mathfrak{A}}} = \mathfrak{A}$ für alle Kripkestrukturen $\mathfrak{A}$.

Es folgt, dass die Abbildung $\mathfrak{A} \mapsto \widetilde{\mathfrak{A}}$ bijektiv ist. $\square$

Einbettung in die Logik der 1. Stufe (Forts.)

Im Folgenden halten wir zwei Variablen $x, x' \in \mathrm{Var}$ mit $x \neq x'$ fest.

Definition 8.39

Für jede Formel $\varphi \in \mathrm{ML}$ definieren wir rekursiv eine Formel $\widetilde{\varphi}(x) \in \mathrm{L}(\widetilde{\sigma})$.

(i) $\widetilde{P} := \widetilde{P}(x)$;

(ii) $\widetilde{\bot} := \bot$ und $\widetilde{\top} := \top$;

(iii) $\widetilde{\neg\varphi} := \neg\widetilde{\varphi}$ und $\widetilde{\varphi * \psi} := \widetilde{\varphi} * \widetilde{\psi}$ für $* \in \{\wedge, \vee, \to\}$;

(iv) $\widetilde{\Box\varphi} := \forall x'\Big(E(x, x') \to \widetilde{\varphi}\frac{x'}{x}\Big)$ und $\widetilde{\Diamond\varphi} := \exists x'\Big(E(x, x') \wedge \widetilde{\varphi}\frac{x'}{x}\Big)$.

Beispiel 8.40

$$\Diamond\Box(\widetilde{\neg P \to} \Box Q) = \exists x'\Bigg(E(x, x') \wedge \forall x''\Big(E(x', x'') \to \Big(\neg\tilde{P}(x'') \to \forall x'''\big(E(x'', x''') \to \tilde{Q}(x''')\big)\Big)\Big)\Bigg).$$

Satz 8.41

Für alle $\varphi \in \mathrm{ML}$, alle Kripkestrukturen $\mathfrak{A}$, und alle Welten $a \in A$ gilt

$$\mathfrak{A}, a \models \varphi \quad \iff \quad \widetilde{\mathfrak{A}} \models \widetilde{\varphi}(a).$$

Beweis.

Einfache Induktion über den Aufbau von $\varphi \in \mathrm{ML}$. $\square$

Korollar 8.42

(1) *Seien* $\Phi \subseteq \mathrm{ML}$ *und* $\psi \in \mathrm{ML}$. *Dann gilt genau dann* $\Phi \models \psi$, *wenn es eine endliche Teilmenge* $\Gamma \subseteq \Phi$ *gibt, so dass* $\Gamma \models \psi$.

(2) *Sei* $\Phi \subseteq \mathrm{ML}$. *Dann ist* Φ *genau dann erfüllbar, wenn jede endliche Teilmenge von* Φ *erfüllbar ist.*

Bemerkung 8.43

Es gibt auch einen vollständigen Beweiskalkül für die Modallogik.

Ergänzungen zu Seite 8.37

Der Endlichkeitssatz folgt sofort aus dem Äquivalenzsatz und dem Endlichkeitssatz für die Logik der 1. Stufe.

Einen vollständigen Sequenzenkalkül für die Modallogik kann man sich aus dem Sequenzenkalkül für die Logik der 1. Stufe konstruieren. Es gibt aber auch andere Arten von vollständigen Beweiskalkülen für die Modallogik.

Endliche Erfüllbarkeit

Satz 8.44

Jede erfüllbare Formel der Modallogik hat ein endliches Modell.

(Ohne Beweis.)

Korollar 8.45

Erfüllbarkeitsproblem und Allgemeingültigkeitsproblem der Modallogik sind entscheidbar.

Ergänzungen zu Seite 8.38

Beweis des Korollars.

Weil es einen vollständigen Beweiskalkül gibt, sind Allgemeingültigkeit und damit Unerfüllbarkeit semi-entscheidbar. Satz 8.44 impliziert, dass Erfüllbarkeit semi-entscheidbar ist. Also ist Erfüllbarkeit entscheidbar. Damit ist auch Allgemeingültigkeit entscheidbar. $\square$

Definition 8.46

Seien $\mathfrak{A}, \mathfrak{B}$ Kripkestrukturen und $a_0 \in A, b_0 \in B$. Das Bisimilationsspiel $\mathrm{BS}(\mathfrak{A}, a_0, \mathfrak{B}, b_0)$ wird von zwei Spielern, genannt Herausforderer (H) und Duplikatorin (D), gespielt.

- Positionen des Spiels sind Paare $(a, b) \in A \times B$. Die Anfangsposition ist (a_0, b_0) und für $i \in \mathbb{N}_{>0}$ sei (a_i, b_i) die Position nach Runde i.

  Falls die Partie nach i Runden endet, so sind die Positionen (a_j, b_j) für $j > i$ undefiniert.
- In Runde $i \in \mathbb{N}$ wählt (H)
  - entweder ein $a_i \in N^{\mathfrak{A}}(a_{i-1})$ und (D) antwortet mit einem $b_i \in N^{\mathfrak{B}}(b_{i-1})$,
  - oder ein $b_i \in N^{\mathfrak{B}}(b_{i-1})$ und (D) antwortet mit einem $a_i \in N^{\mathfrak{A}}(a_{i-1})$.
- Die Partie endet nach Runde $i \in \mathbb{N}$, wenn einer der folgenden Fälle eintritt:

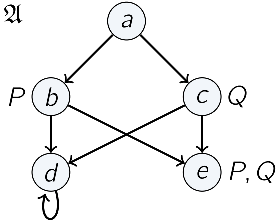
  (i) Es gibt ein $P \in \sigma$, so dass $\mathrm{al}^{\mathfrak{A}}(a_i, P) \neq \mathrm{al}^{\mathfrak{B}}(b_i, P)$. In diesem Fall gewinnt (H).

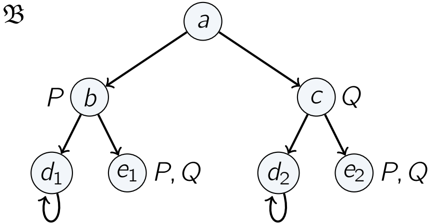
  (ii) Nicht (i), und $N^{\mathfrak{A}}(a_i) \cup N^{\mathfrak{B}}(b_i) = \emptyset$. In diesem Fall gewinnt (D).

  (iii) Nicht (i), (ii), und $N^{\mathfrak{A}}(a_i) = \emptyset$ oder $N^{\mathfrak{B}}(b_i) = \emptyset$. In diesem Fall gewinnt (H).

  Falls das Spiel niemals endet, gewinnt (D).

Beispiel 8.47





(D) hat eine Gewinnstrategie für das Spiel $\mathrm{BS}(\mathfrak{A}, a, \mathfrak{B}, a)$.

Beispiel 8.48

(H) hat eine Gewinnstrategie für das Spiel $\mathrm{BS}(\mathfrak{A}, a, \mathfrak{B}, a)$.

Definition 8.49

Seien $\mathfrak{A}, \mathfrak{B}$ Kripkestrukturen und $a \in A, b \in B$.

(1) $\mathfrak{A}, a$ und $\mathfrak{B}, b$ sind bisimilar (wir schreiben $\mathfrak{A}, a \sim \mathfrak{B}, b$), wenn (D) eine Gewinnstrategie für das Spiel $\mathrm{BS}(\mathfrak{A}, a, \mathfrak{B}, a)$ hat.

(2) $\mathfrak{A}, a$ und $\mathfrak{B}, b$ sind modallogisch äquivalent, wenn für alle $\varphi \in \mathrm{ML}$ gilt:

$$\mathfrak{A}, a \models \varphi \quad \Longleftrightarrow \quad \mathfrak{B}, b \models \varphi.$$

Satz 8.50

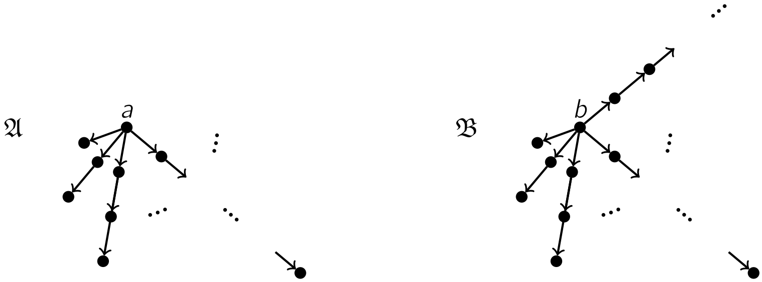
Seien $\mathfrak{A}, \mathfrak{B}$ Kripkestrukturen und $a \in A, b \in B$, so dass $\mathfrak{A}, a \sim \mathfrak{B}, b$. Dann $\mathfrak{A}, a$ und $\mathfrak{B}, b$ modallogisch äquivalent.

Die Umkehrung gilt im Allgemeinen nicht.

(Ohne Beweis.)

Beispiel 8.51

Folgende Kripkestrukturen sind modallogisch äquivalent, aber nicht bisimilar.



Der Satz von Hennessy und Milner

Definition 8.52

Eine Kripkestruktur $\mathfrak{A}$ ist endlich verzweigt, wenn für alle $a \in A$ die Menge $N^{\mathfrak{A}}(a)$ endlich ist.

Satz 8.53

Seien $\mathfrak{A}, \mathfrak{B}$ endlich verzweigte Kripkestrukturen und $a \in A, b \in B$. Dann gilt

$$\mathfrak{A}, a \text{ und } \mathfrak{B}, b \text{ sind modallogisch äquivalent} \iff \mathfrak{A}, a \sim \mathfrak{B}, b.$$

(Ohne Beweis.)

Der Charakterisierungssatz von van Benthem

Definition 8.54

Eine Formel $\varphi(x) \in \mathrm{L}(\tilde{\sigma})$ ist bisimulationsinvariant, wenn für alle Kripkestrukturen $\mathfrak{A}, \mathfrak{B}$ und alle Welten $a \in A, b \in B$ gilt:

$$\mathfrak{A}, a \sim \mathfrak{B}, b \implies \big(\mathfrak{A} \models \varphi(a) \iff \mathfrak{B} \models \varphi(b)\big).$$

Satz 8.55

Eine Formel $\varphi(x) \in \mathrm{L}(\tilde{\sigma})$ ist genau dann bisimulationsinvariant, wenn sie äquivalent zu einer modallogischen Formel ist.

(Ohne Beweis.)