Mathematische Logik
WS 2000/2001

Erich Grädel

Inhaltsverzeichnis

Mathematische Logik
WS 2000/2001

Erich Grädel

Kapitel 1

Aussagenlogik

1.1 Syntax und Semantik der Aussagenlogik

Die Aussagenlogik (AL) untersucht Ausdrücke, die aus atomaren Aussagen (den Aussagenvariablen) allein mit Hilfe der aussagenlogischen Junktoren gebildet werden. Die Aussagenvariablen werden interpretiert durch die Wahrheitswerte 0 (für *falsch*) und 1 (für *wahr*).

Für mathematische Zwecke ist die Aussagenlogik relativ uninteressant, da sie zu ausdrucksschwach ist. Viele grundlegende Aspekte stärkerer Logiken lassen sich jedoch im Kontext der Aussagenlogik übersichtlich behandeln und veranschaulichen. Zudem ergeben sich in der Aussagenlogik zahlreiche interessante *algorithmische Probleme* mit fundamentaler Bedeutung für die Informatik, so etwa die Komplexität des Erfüllbarkeitsproblems, die Suche nach effizienten Beweissystemen, sowie die Spezifikation und effiziente Berechnung Boolescher Funktionen.

Syntax. Formeln sind *syntaktische Objekte*, d.h. Wörter in einer formalen Sprache. Die Menge der aussagenlogischen Formeln ist induktiv als Wortmenge über einem Alphabet definiert, welches aus folgenden Symbolen besteht

- einer festen Menge τ von *Aussagenvariablen*,
- den Booleschen Konstanten 0,1,
- den *aussagenlogischen Junktoren* $\neg, \wedge, \vee$, und $\rightarrow$,
- den Klammersymbolen (,).

Meistens wird eine feste, abzählbar unendliche Menge $\tau = \{X_0, X_1, X_2 \dots\}$ von Aussagenvariabeln zugrundegelegt. Für gewisse Anwendungen der Aussagenlogik ist ist jedoch sinnvoll, beliebige, auch überabzählbare Mengen τ zuzulassen.

Definition 1.1. Die Menge AL der *aussagenlogischen Formeln* ist induktiv definiert durch

(1) $0, 1 \in \mathrm{AL}$ (die Booleschen Konstanten sind Formeln).

(2) $\tau \subseteq \mathrm{AL}$ (jede Aussagenvariable ist eine Formel).

(3) Wenn $\psi, \varphi \in \mathrm{AL}$, dann sind auch die Wörter $\neg\psi$, $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $(\psi \rightarrow \varphi)$ Formeln aus AL.

Boolesche Konstanten und Aussagenvariabeln nennen wir auch *atomare Formeln*. Die Formel $\neg\psi$ wird gelesen "nicht ψ" und ist die *Negation* von ψ. Die Formeln $(\psi \vee \varphi)$, gelesen "ψ oder φ", und $(\psi \wedge \varphi)$, gelesen "ψ und φ", heissen die *Disjunktion* bzw. *Konjunktion* von ψ und φ. Wir nennen $(\psi \rightarrow \varphi)$ die *Implikation* von ψ nach φ und lesen sie "ψ Pfeil φ" oder "ψ impliziert φ".

Konventionen zur Notation von Formeln. Zur Vesserung der Lesbarkeit bedienen wir uns abkürzender oder vereinfachender Schreibweisen. Zum Beispiel werden wir in Formeln oft Klammern weglassen, welche für das Verständnis überflüssig sind. Wir vereinbaren, dass $\neg$ stärker bindet als alle andern Junktoren, und dass $\wedge$ und $\vee$ stärker binden als $\rightarrow$. So steht etwa $\psi \wedge \neg\varphi \rightarrow \vartheta$ für $((\psi \wedge \neg\varphi) \rightarrow \vartheta)$. Ausserdem vereinbaren wir implizite Linksklammerung bei iterierten Disjunktionen und Konjunktionen: $\psi \wedge \varphi \wedge \eta$ steht für $((\psi \wedge \varphi) \wedge \eta)$. Für iterierte Konjunktionen und Disjunktionen über Formeln $\varphi_1, \ldots, \varphi_n$ verwenden wir die Schreibweisen $\bigwedge_{i=1}^n \varphi_i$ und $\bigvee_{\imath=1}^n \varphi_i$.

Induktion über den Formelaufbau. Jede Formel $\psi \in \mathrm{AL}$ ist ein Wort über dem Alphabet $\Gamma := \tau \cup \{0, 1, \neg, \wedge, \vee, \rightarrow, (,)\}$, aber natürlich ist nicht jedes Wort aus Γ^* eine Formel. Definition 1.1 ist ein Beispiel für eine *induktive* (durch Konstruktionsregeln gegebene) Definition. Sie ist so zu verstehen, dass ausser den nach den Regeln (1), (2) und (3) festgelegten Formeln keine weiteren Zeichenketten aussagenlogische Formeln sind. Mit andern Worten: AL ist die kleinste Menge von Wörtern aus Γ^*, welche 0, 1 sowie alle Aussagenvariablen $X \in \tau$ enthält, und die unter der Regel (3) abgeschlossen ist, die also mit ψ und ψ auch die Zeichenketten $\neg\psi$, $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $(\psi \rightarrow \varphi)$ enhält.

Der induktive Aufbau von Formeln erlaubt das Prinzip der strukturellen Induktion für Definitionen und Beweise. Induktionsbeweise über den Formelaufbau folgen folgendem Muster. Um nachzuweisen, dass alle Formeln in AL eine Eigenschaft E besitzen, zeigt man:

(a) Alle atomaren Formeln haben die Eigenschaft E.

(b) Haben ψ und $\varphi \in \mathrm{AL}$ die Eigenschaft E, so auch $\neg\psi$ und $(\psi \circ \varphi)$, für $\circ \in \{\wedge, \vee, \rightarrow\}$.

Mit diesem Beweisprinzip kann man leicht die *eindeutige Lesbarkeit von Formeln* einsehen: Kein echtes Anfangsstück einer Formel ist selbst eine Formel und daher kann man jede Formel auf genau eine Weise gemäss den Regeln (1) – (3) von Definition 1.1 in ihre unmittelbaren Bestandteile zerlegen.

Daraus folgt insbesondere, dass induktive Definitionen über den Formelaufbau eindeutig sind: So können wir etwa die *Tiefe* $d(\psi)$ einer Formel $\psi \in \mathrm{AL}$ induktiv wie folgt definieren: (1) $d(\psi) := 0$ für atomare ψ, (2) $d(\neg\psi) := d(\psi) + 1$ und (3) $d((\psi \circ \varphi)) := 1 + \max(d(\psi), d(\varphi))$. Die Tiefe ist oft ein adäquateres Maß für die Komplexität einer Formel als deren Länge. Eine *Unterformel* einer Formel $\psi \in \mathrm{AL}$ ist ein Teilwort von ψ das selbst eine Formel ist. Die Unterformeln von $\psi := (X_1 \vee X_3) \wedge (X_2 \vee (X_3 \rightarrow \neg X_1))$ sind

$$\psi, (X_1 \vee X_3), (X_2 \vee (X_3 \rightarrow \neg X_1)), (X_3 \rightarrow \neg X_1), \neg X_1, X_1, X_2, X_3.$$

Die Tiefe von ψ ist 4.

Übung 1.1. Geben Sie eine *induktive* Definition für die Menge der Unterformeln einer aussagenlogischen Formel an. Zeigen Sie:

(a) Formeln der Länge n haben höchstens n Unterformeln.

(b) Formeln der Tiefe n haben höchstens $2^{n+1}-1$ Unterformeln.

(c) Es existieren für jedes $n \in \mathbb{N}$ Formeln der Tiefe n mit genau $2^{n+1}-1$ Unterformeln.

Übung 1.2. Zeigen Sie, dass das Prinzip der eindeutigen Lesbarkeit von Formeln erhalten bleibt, wenn wir die sog. *polnische Notation* verwenden, welche ganz ohne Klammern auskommt. Die Regel (3) in Definition 1.1 wird dabei ersetzt durch

(3)′ Wenn ψ und φ aussagenlogische Formeln sind, dann auch die Ausdrücke $\neg\psi$, $\wedge\psi\varphi$, $\vee\psi\varphi$ und $\rightarrow\psi\varphi$.

Man zeige andererseits, dass die eindeutige Lesbarkeit nicht mehr gewährleistet ist wenn in Definition 1.1 die Klammern einfach weggelassen werden, d.h. wenn mit ψ und φ auch die Ausdrücke $\psi \wedge \varphi$, $\psi \vee \varphi$ und $\psi \rightarrow \varphi$ als Formeln zugelassen werden.

Semantik. Für jede Formel $\psi \in \mathrm{AL}$ sei $\tau(\psi) \subseteq \tau$ die Menge der in ψ tatsächlich vorkommenden Aussagenvariablen. Für Formelmengen $\Phi \in \mathrm{AL}$ ist $\tau(\Phi) = \bigcup_{\varphi\in\Phi} \tau(\varphi)$.

Definition 1.2. Eine *(aussagenlogische) Interpretation* ist eine Abbildung $\mathfrak{I} : \sigma \rightarrow \{0,1\}$ für ein $\sigma \subseteq \tau$. Sie ist *passend* für eine Formel $\psi \in \mathrm{AL}$, wenn $\tau(\psi) \subseteq \sigma$. Jede zu ψ passende Interpretation $\mathfrak{I}$ definiert einen Wahrheitswert $[\![\psi]\!]^{\mathfrak{I}} \in \{0,1\}$, durch die folgenden Festlegungen:

(1) $[\![0]\!]^{\mathfrak{I}} := 0,\ [\![1]\!]^{\mathfrak{I}} := 1.$

(2) $[\![X]\!]^{\mathfrak{I}} := \mathfrak{I}(X)$ für $X \in \sigma$.

(3) $[\![\neg\psi]\!]^{\mathfrak{I}} := 1 - [\![\psi]\!]^{\mathfrak{I}}.$

(4) $[\![\psi \wedge \varphi]\!]^{\mathfrak{I}} := \min([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}}).$

(5) $[\![\psi \vee \varphi]\!]^{\mathfrak{I}} := \max([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}}).$

(6) $[\![\psi \rightarrow \varphi]\!]^{\mathfrak{I}} := [\![\neg\psi \vee \varphi]\!]^{\mathfrak{I}}.$

Ein *Modell* einer Formel $\psi \in \mathrm{AL}$ ist eine Interpretation $\mathfrak{I}$ mit $[\![\psi]\!]^{\mathfrak{I}} = 1$. Statt $[\![\psi]\!]^{\mathfrak{I}} = 1$ schreibt man auch $\mathfrak{I} \models \psi$ und sagt $\mathfrak{I}$ *erfüllt* ψ.

Nicht alle Aussagenvariablen im Definitionsbereich einer zu ψ passenden Interpretation $\mathfrak{I}$ müssen in ψ auch tatsächlich vorkommen. Offensichtlich ist aber für die Definition von $[\![\psi]\!]^{\mathfrak{I}}$ die Interpretation der in ψ gar nicht vorkommenden Ausagenvariablen unerheblich. Dieser Sachverhalt, den man durch eine einfache Induktion über den Formelaufbau nachweisen kann, wird durch das Koinzidenzlemma ausgedrückt.

Lemma 1.3 (Koinzidenzlemma). *Sei $\psi \in \mathrm{AL}$ eine Formel und seien $\mathfrak{I}$ und $\mathfrak{I}'$ zwei zu ψ passende Interpretationen, so dass $\mathfrak{I}(X) = \mathfrak{I}'(X)$ für alle $X \in \tau(\psi)$. Dann ist $[\![\psi]\!]^{\mathfrak{I}} = [\![\psi]\!]^{\mathfrak{I}'}$.*

Übung 1.3. (Auswerten aussagenlogischer Formeln) Geben Sie einen (möglichst effizienten) Algorithmus an, welcher zu einer gegebenen Formel $\psi \in \mathrm{AL}$ und einer gegebenen Interpretation $\mathfrak{I}$ den Wahrheitswert $[\![\psi]\!]^{\mathfrak{I}}$ berechnet. Beurteilen Sie die Laufzeit und den Bedarf an Speicherplatz des Algorithmus.

Übung 1.4. Geben Sie eine Formel ψ an, welche die Aussagenvariablen X_1, X_2, X_3 enthält, so dass für jede Interpretation $\mathfrak{I} : \{X_1, X_2, X_3\} \to \{0, 1\}$ gilt, dass das Ändern jedes Wahrheitswerts $\mathfrak{I}(X_i)$ auch den Wahrheitswert $[\![\psi]\!]^{\mathfrak{I}}$ ändert.

Notation: In diesem Kapitel stehen kleine griechische Buchstaben $\psi, \varphi, \vartheta, \dots$ immer für aussagenlogische Formeln, grosse griechische Buchstaben Φ, Γ für Mengen aussagenlogischer Formeln. Wir verwenden die Schreibweise $\psi(X_1, \dots, X_n)$ um anzudeuten, dass $\tau(\psi) \subseteq \{X_1, \dots, X_n\}$. Sei $\mathfrak{I}(X_1) = w_1, \dots, \mathfrak{I}(X_n) = w_n$. Dann schreiben wir auch $[\![\psi(w_1, \dots, w_n)]\!]$ oder $[\![\psi(\boldsymbol{w})]\!]$ für $[\![\psi]\!]^{\mathfrak{I}}$.

Definition 1.4. Zwei Formeln ψ und φ heissen *logisch äquivalent* (kurz: $\psi \equiv \varphi$), wenn für jede zu beiden Formeln passende Interpretation $\mathfrak{I}$ gilt, dass $[\![\psi]\!]^{\mathfrak{I}} = [\![\varphi]\!]^{\mathfrak{I}}$.

Hier sind ein paar einfache logische Äquivalenzen. Der Nachweis ergibt sich unmittelbar aus der Definition der Modellbeziehung. Für beliebige Formeln $\psi, \varphi, \vartheta \in \mathrm{AL}$ gilt:

(1) $\neg\neg\psi \equiv \psi$ (Elimination der doppelten Negation)

(2) $\neg(\psi \wedge \varphi) \equiv \neg\psi \vee \neg\varphi$
$\neg(\psi \vee \varphi) \equiv \neg\psi \wedge \neg\varphi$ (de Morgan'sche Gesetze)

(3) $\psi \wedge (\varphi \vee \vartheta) \equiv (\psi \wedge \varphi) \vee (\psi \wedge \vartheta)$
$\psi \vee (\varphi \wedge \vartheta) \equiv (\psi \vee \varphi) \wedge (\psi \vee \vartheta)$ (Distributivgesetze)

(4) $\psi \to \varphi \equiv \neg\varphi \to \neg\psi$ (Kontraposition)

(5) $\psi \wedge (\psi \vee \varphi) \equiv \psi \vee (\psi \wedge \varphi) \equiv \psi$ (Absorption)

(6) $\psi \wedge \psi \equiv \psi$
$\psi \vee \psi \equiv \psi$ (Idempotenz von $\wedge$ und $\vee$)

(7) $\psi \wedge \varphi \equiv \varphi \wedge \psi$
$\psi \vee \varphi \equiv \varphi \vee \psi$ (Kommutativität von $\wedge$ und $\vee$)

(8) $\psi \wedge (\varphi \wedge \vartheta) \equiv (\psi \wedge \varphi) \wedge \vartheta$
$\psi \vee (\varphi \vee \vartheta) \equiv (\psi \vee \varphi) \vee \vartheta$ (Assoziativität von $\wedge$ und $\vee$)

Die Assoziativität, Kommutativität und Idempotenz von $\wedge$ und $\vee$ impliziert, dass es bei der Bildung der Konjunktion bzw. Disjunktion über eine endliche Folge $\varphi_1, \dots, \varphi_n$ von Formeln nicht auf die Reihenfolge und Multiplizität der Formeln ankommt. Dies rechtfertigt, dass wir Konjunktionen und Disjunktion über endliche Formelmengen $\Phi = \{\varphi 1, \dots, \varphi_n\}$ bilden; anstelle von $\varphi_1 \wedge \dots \wedge \varphi_n$ verwenden wir auch die Schreibeweisen $\bigwedge_{\varphi \in \Phi} \varphi$ oder $\bigwedge \Phi$, und analog $\bigvee_{\varphi \in \Phi} \varphi$ oder $\bigvee \Phi$ für die Disjunktion. (Dabei ist natürlich immer vorauszusetzen, dass Φ endlich ist!) Wenn Φ die leere Menge ist, identifizieren wir $\bigwedge \Phi$ mit 1 und $\bigvee \Phi$ mit 0.

Übung 1.5. Beweisen oder widerlegen Sie folgende Aussagen:

(a) $\psi \wedge (\varphi \to \vartheta) \equiv (\psi \wedge \varphi) \to \vartheta \equiv (\varphi \wedge (\psi \to \vartheta)$

(b) $\neg\varphi_1 \vee \neg\varphi_1 \vee \dots \vee \neg\varphi_n \vee \psi \equiv \varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n \to \psi$
$\neg\varphi_1 \vee \neg\varphi_1 \vee \dots \vee \neg\varphi_n \equiv \varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n \to 0$

(c) $\psi \to (\varphi \wedge \vartheta) \equiv (\psi \to \varphi) \wedge (\psi \to \vartheta)$
$\psi \wedge \varphi \to \vartheta \equiv (\psi \to \vartheta) \vee (\varphi \to \vartheta)$
$(\psi \vee \varphi) \to \vartheta \equiv (\psi \to \vartheta) \wedge (\varphi \to \vartheta)$

Definition 1.5. Hat eine Formel ein Modell, dann heisst sie *erfüllbar*, andernfalls *unerfüllbar*. Eine Formel ψ heisst *allgemeingültig* oder eine *Tautologie*, wenn jede zu ψ passende Interpretation ein Modell von ψ ist. Man schreibt $\models \psi$ um anzudeuten, dass ψ eine Tautologie ist.

Lemma 1.6. *Eine Formel ψ ist erfüllbar genau dann, wenn $\neg\psi$ keine Tautologie ist.*

Es gibt ein offensichtliches Verfahren um festzustellen, ob eine aussagenlogische Formel $\psi(X_1, \dots, X_n)$ erfüllbar (oder allgemeingültig) ist: Man prüft für alle Interpretationen $\mathfrak{I} : \{X_1, \dots, X_n\} \to \{0, 1\}$ mittels des in Übung 1.3 entwickelten Auswertungsalgorithmus nach, ob $\mathfrak{I} \models \psi$. Obwohl für jede einzelne Interpretation $\mathfrak{I}$ dies sehr schnell nachgefrüft werden kann, ist das Verfahren insgesamt doch extrem ineffizient, da es bei n Aussagenvariablen 2^n mögliche Interpretationen gibt. Für Formeln mit Hunderten von Aussagenvariablen (was in praktischen Anwendungen durchaus realistisch ist) wären also selbst die schnellsten Rechner hoffnungslos überfordert. Natürlich gibt es bessere Verfahren, aber es ist nicht bekannt, ob das exponentielle Wachstum der Berechnungszeit durch raffiniertere Algorithmen vermieden werden kann. Man vermutet, dass dies nicht der Fall ist, dass also das Erfüllbarkeitsproblem der Aussagenlogik (genannt SAT) inhärent exponentiell schwierig ist, da es zu den NP-vollständigen Problemen gehört. Siehe die Vorlesung Berechenbarkeit und Komplexität, in der das erläutert und (hoffentlich) bewiesen wird.

Übung 1.6. Beweisen Sie das *aussagenlogische Interpolationstheorem*: Sei $\psi \to \varphi$ eine aussagenlogische Tautologie. Dann existiert eine aussagenlogische Formel ϑ mit $\tau(\vartheta) \subseteq \tau(\psi) \cap \tau(\varphi)$, so dass $\psi \to \vartheta$ und $\vartheta \to \varphi$ Tautologien sind. Hinweis: Führen Sie einen Induktionsbeweis über die Anzahl der Aussagenvariablen, die in ψ, aber nicht in φ vorkommen.

1.2 Aussagenlogik und Boolesche Funktionen

Eine (n-stellige) Boolesche Funktion ist eine Funktion $f : \{0, 1\}^n \to \{0, 1\}$. Sei B^n die Menge aller n-stelligen Booleschen Funktionen und $B = \bigcup_{n \in \mathbb{N}} B^n$. B^0 enthält die konstanten Funktionen 0 und 1. B^1 enthält vier Funktionen $f_{00}, f_{01}, f_{10}, f_{11}$ mit

$$f_{00}(0) = f_{00}(1) = 0, \qquad f_{11}(0) = f_{11}(1) = 1,$$
$$f_{01}(w) = w, \qquad f_{10}(w) = 1 - w.$$

B^n enthält 2^{2^n} verschiedene Funktionen.

Jede Formel $\psi(X_1, \dots, X_n) \in \mathrm{AL}$ definiert eine Boolesche Funktion $h_\psi \in B^n$, durch die Vorschrift $h_\psi(w_1, \dots, w_n) := [\![\psi(w_1, \dots, w_n)]\!]$. Der folgende Satz zeigt, dass sich umgekehrt jede Boolesche Funktion durch eine aussagenlogische Formel darstellen lässt.

Satz 1.7. *Zu jeder Funktion $f \in B^n$ gibt es eine Formel $\psi(X_1, \dots, X_n)$ mit $h_\psi = f$.*

Beweis. Die Funktionen in B^0 werden durch die Formeln 0 und 1 dargestellt. Sei nun $n > 0$ und $f \in B^n$. Für jede Aussagenvariable X setzen wir $X^1 := X$ und $X^0 := \neg X$. Weiter definieren wir für jedes $\boldsymbol{v} = v_1, \dots, v_n$, die Formel $\varphi^{\boldsymbol{v}} := X_1^{v_1} \wedge \dots \wedge X_n^{v_n}$. Man beachte, dass für alle $\boldsymbol{v}, \boldsymbol{w} \in \{0,1\}^n$ gilt:

$$[\![\varphi^{\boldsymbol{v}}(\boldsymbol{w})]\!] = 1 \qquad \Longleftrightarrow \qquad \boldsymbol{v} = \boldsymbol{w}$$

Die Funktion f wird nun dargestellt durch die Formel

$$\psi(X_1, \dots, X_n) := \bigvee_{\substack{\boldsymbol{v} \in \{0,1\}^n \\ f(\boldsymbol{v})=1}} \varphi^{\boldsymbol{v}}.$$

Wir müssen zeigen, dass $f(\boldsymbol{w}) = [\![\psi(\boldsymbol{w})]\!]$ für alle $\boldsymbol{w} \in \{0,1\}^n$.

Sei $f(\boldsymbol{w}) = 1$. Dann ist $\varphi^{\boldsymbol{w}}$ ein Disjunktionsglied von ψ, und da $[\![\varphi^{\boldsymbol{w}}(\boldsymbol{w})]\!] = 1$ ist $[\![\psi(\boldsymbol{w})]\!] = 1$. Wenn aber $f(\boldsymbol{w}) = 0$, dann gilt für jede Teilformel $\varphi^{\boldsymbol{v}}$ von ψ dass $v_i \neq w_i$ für mindestens ein i und daher $[\![\varphi^{\boldsymbol{v}}(\boldsymbol{w})]\!] = 0$. Also ist $[\![\psi(\boldsymbol{w})]\!] = 0$. □

Aus dem Beweis von Satz 1.7 ergeben sich noch weitere wichtige Konsequenzen.

Disjunktive und konjunktive Normalform. Ein *Literal* ist eine Aussagenvariable X oder deren Negation $\neg X$. Mit $\overline{Y}$ bezeichnen wir das zu Y komplementäre Literal, also $\overline{X} := \neg X$ und $\overline{\neg X} := X$ für jede Aussagenvariable X.

Definition 1.8. Eine Formel $\psi \in AL$ ist in *disjunktiver Normalform* (DNF), wenn sie eine Disjunktion von Konjunktionen über Literale ist, d.h., wenn sie die Form $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} Y_{ij}$ hat, wobei die Y_{ij} Literale sind. Der duale Begriff ist die *konjunktive Normalform* (KNF); Formeln in KNF sind Konjunktionen von Disjunktionen von Literalen, also Formeln der Gestalt $\bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} Y_{ij}$.

Die im Beweis von Satz 1.7 konstruierte Formel

$$\psi(X_1, \dots, X_n) := \bigvee_{\substack{\boldsymbol{v} \in \{0,1\}^n \\ f(\boldsymbol{v})=1}} \varphi^{\boldsymbol{v}} = \bigvee_{\substack{(v_1,\dots,v_n) \in \{0,1\}^n \\ f(v_1,\dots,v_n)=1}} X_1^{v_1} \wedge \dots \wedge X_n^{v_n}$$

zur Darstellung der Booleschen Funktion f ist in disjunktiver Normalform. Da jede Formel eine Boolesche Funktion definiert folgt unmittelbar, dass es zu jeder Formel $\psi \in \mathrm{AL}$ eine äquivalente DNF-Formel gibt.

Die analoge Aussage zur KNF erhalten wir wie folgt. Da zu jeder Formel eine äquivalente Formel in DNF existiert, gilt dies insbesondere auch für $\neg\psi$:

$$\neg\psi \equiv \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} Y_{ij}.$$

Aus den de Morgan'schen Gesetzen folgt, dass für beliebige Formeln $\vartheta_1, \dots, \vartheta_n$ gilt

$$\neg \bigvee_{k=1}^{m} \vartheta_k \equiv \bigwedge_{k=1}^{m} \neg\vartheta_k, \qquad \neg \bigwedge_{k=1}^{m} \vartheta_k \equiv \bigvee_{k=1}^{m} \neg\vartheta_k.$$

Also folgt:

$$\psi \equiv \neg \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} Y_{ij} \equiv \bigwedge_{i=1}^{n} \neg \bigwedge_{j=1}^{m_i} Y_{ij} \equiv \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} \overline{Y_{ij}} =: \psi_K.$$

ψ_K ist in KNF und hat die geforderten Eigenschaften. Damit haben wir folgenden Satz bewiesen.

Satz 1.9. *Zu jeder Formel* $\psi \in$ AL *gibt es äquivalente Formeln* ψ_D *in* DNF *und* ψ_K *in* KNF.

Übung 1.7. Führen Sie einen alternativen Beweis für Satz 1.7 indem Sie per Induktion nach n nachweisen, dass es 2^{2^n} nicht-äquivalente aussagenlogische Formeln $\psi(X_1, \dots, X_n)$ gibt.

Übung 1.8. Geben Sie einen Algorithmus an welcher unter Verwendung elementarer Umformungsregeln, z.B. der de Morganschen Regeln und der Distributivgesetze, eine gegebene aussagenlogische Formel in äquivalente DNF bzw. KNF-Formeln überführt. Wenden Sie dieses Verfahren auf die Formel $(X_1 \to X_2) \wedge ((X_1 \wedge X_3) \to X_2 \wedge X_2 \to X_3)$ an. Zeigen Sie, dass in gewissen Fällen die resultierenden DNF- bzw. KNF-Formeln exponentiell länger werden als die gegebene Formel.

Übung 1.9. Zwei Formeln heissen *erfüllbarkeitsäquivalent*, wenn beide erfüllbar oder beide unerfüllbar sind. (Erfüllbarkeitsäquivalente Formeln müsen natürlich nicht unbedingt äquivalent sein.) Eine aussagenlogische Formel ist in 3-KNF, wenn sie folgende Gestalt hat:

$$\bigwedge_{i=1}^{n} Y_{i1} \vee Y_{i2} \vee Y_{i3} \quad (Y_{ij} \text{ Literale})$$

Zeigen Sie, dass es man zu jeder Formel ψ in KNF eine erfüllbarkeitsäquivalente Formel in 3-KNF konstruieren kann, und zwar mit einem Verfahren dessen Laufzeit polynomial in der Länge von ψ beschränkt ist.

Hinweis: Man fasse überzählige Literale mit Hilfe neuer Aussagenvariablen zusammen.

Übung 1.10. Zeigen Sie, dass das Erfüllbarkeitsproblem für DNF-Formeln durch einen Algorithmus mit linearer Laufzeit (bzgl. der Länge der Formel) gelöst werden kann.

Funktional vollständige Mengen. Die Konstanten 0,1 und die Junktoren $\neg, \wedge, \vee, \to$ können als Funktionen in B^0, B^1 bzw. B^2 aufgefasst werden. Umgekehrt kann man aus jeder Booleschen Funktion $f \in B^n$ einen aussagenlogischen Junktor definieren: Aus Formeln $\varphi_1, \dots, \varphi_n \in$ AL bildet man eine neue Formel $f(\varphi_1, \dots, \varphi_n)$ deren Semantik auf naheliegende Weise festgelegt ist:

$$[\![f(\varphi_1, \dots, \varphi_n)]\!]^{\mathfrak{I}} := f([\![\varphi_1]\!]^{\mathfrak{I}}, \dots, [\![\varphi_n]\!]^{\mathfrak{I}}).$$

Die im Beweis von Satz 1.7 konstruierten Formeln benutzen (für $n > 0$) nur die Junktoren $\wedge, \vee, \neg$. Also lassen sich aus diesen Funktionen (oder Junktoren) alle anderen Booleschen Funktionen kombinieren.

Definition 1.10. Eine Menge $\Omega \subseteq B$ von Booleschen Funktionen ist *funktional vollständig*, wenn sich daraus jede Boolesche Funktion $f : B^n \to B$ $(n \geq 1)$ im Sinne von Satz 1.7 definieren lässt.

Wir wissen, dass neben $\{\wedge, \vee, \neg\}$ auch bereits $\{\wedge, \neg\}$ und $\{\vee, \neg\}$ funktional vollständig sind, da

$$\psi \wedge \varphi \equiv \neg(\neg\psi \vee \neg\varphi)$$
$$\psi \vee \varphi \equiv \neg(\neg\psi \wedge \neg\varphi).$$

Es gibt aber noch weitere funktional vollständige Mengen:

(1) $\{\to, \neg\}$ ist funktional vollständig, da $\{\vee, \neg\}$ funktional vollständig ist und $\psi \vee \varphi \equiv \neg\psi \to \varphi$.

(2) $\{\to, 0\}$ ist funktional vollständig. Dies folgt aus (1) und $\neg\psi \equiv \psi \to 0$.

(3) Sei $\oplus$ die Addition modulo 2 (das 'exklusive oder'). Die Menge $\{\wedge, \oplus, 1\}$ ist funktional vollständig, da $\neg\psi \equiv 1 \oplus \psi$. Boolesche Funktionen entsprechen also genau den Polynomen über dem Körper $\mathbb{F}_2$.

(4) Sei $(u \mid v) := 0$, wenn $u = v = 1$ und $(u \mid v) := 1$ sonst, also $(\psi \mid \varphi) \equiv \neg(\psi \wedge \varphi)$. Dann ist $\{\,|\,\}$ funktional vollständig, da $\neg\psi \equiv \psi \mid \psi$ und $\psi \wedge \varphi \equiv \neg(\psi \mid \varphi) \equiv (\psi \mid \varphi) \mid (\psi \mid \varphi)$.

(5) Hingegen ist $\{\wedge, \vee, \to\}$ nicht funktional vollständig, da für jede nur mit diesen Junktoren gebildete Formel $\psi(X_1, \dots, X_n)$ gilt, dass $\psi[1, \dots, 1] = 1$. Insbesondere kann mit $\wedge, \vee, \to$ keine zu $\neg X$ äquivalente Formel gebildet werden.

Für gewisse Zwecke, z.B. für Beweissysteme oder Schaltkreise, ist es durchaus zweckmässig, Formeln aus anderen funktional vollständigen Mengen als $\{\wedge, \vee, \neg\}$ aufzubauen.

Übung 1.11. Die Funktion $sel \in B^3$ sei definiert durch $sel(u, v, w) = v$, wenn $u = 0$ und $sel(u, v, w) = w$, wenn $u = 1$. Zeigen Sie, dass $\{sel, 0, 1\}$ funktional vollständig ist.

Übung 1.12. Zeigen Sie, dass die Menge $\{\wedge, \vee, 0, 1\}$ funktional unvollständig ist, dass aber jede Erweiterung durch eine Funktion, welche nicht über $\{\wedge, \vee, 0, 1\}$ definierbar ist, funktional vollständig ist.

Übung 1.13. Eine Boolesche Funktion $f \in B^n$ ist *linear*, wenn sie durch eine lineares Polynom $f(X_1, \dots, X_n) = a_0 + a_1 X_1 + \cdots + a_n X_n$ über dem Körper $\mathbb{F}_2$ beschrieben werden kann. Zeigen Sie, dass die meisten Booleschen Funktion nicht linear sind.

Übung 1.14. Die zu $f \in B^n$ *duale Funktion* ist definiert durch $f^\delta(x_1, \dots, x_n) := \neg f(\neg x_1, \dots, \neg x_n)$.

(a) Geben Sie die zu $\vee$, $\wedge$, $\to$, $\neg$ dualen Funktionen an.

(b) Eine Funktion f ist *selbstdual*, wenn $f^\delta = f$. Sei T^n_k die n-stellige Boolesche Funktion mit

$$T^n_k(x_1, \dots, x_n) = 1 \iff |\{i : x_i = 1\}| \geq k.$$

Beschreiben Sie die zu T^n_k duale Funktion. Für welche n, k ist T^n_k selbstdual?

(c) Zeigen Sie, dass die über der Junktorenmenge $\{\neg, T^3_2\}$ definierbaren Funktionen gerade die selbstdualen Funktionen sind.

1.3 Horn-Formeln

Eine in der Praxis sehr wichtige Klasse von Formeln sind Horn-Formeln (benannt nach dem Logiker Alfred Horn). Insbesondere ist das Erfüllbarkeitsproblem für Horn-Formeln durch einen einfachen und effizienten Algorithmus entscheidbar.

Definition 1.11. Eine *(aussagenlogische) Horn-Formel* ist eine Formel $\psi = \bigwedge_i \bigvee_j Y_{ij}$ in KNF, wobei jede Disjunktion $\bigvee_j Y_{ij}$ höchstens ein positives Literal enthält.

Horn-Formeln können auch als Konjunktionen von Implikationen geschrieben werden :

(1) $\neg X_1 \vee \cdots \vee \neg X_k \vee X \;\equiv\; X_1 \wedge \cdots \wedge X_k \to X$

(2) $\neg X_1 \vee \cdots \vee \neg X_k \;\equiv\; X_1 \wedge \cdots \wedge X_k \to 0$

Implikationen vom Typ (1) mit $k = 0$ werden in der Form $(1 \to X)$ geschrieben. Horn-Formeln, die keine solchen Implikationen enthalten sind trivialerweise erfüllbar, indem man alle Aussagenvariablen mit 0 bewertet. Offensichtlich ist auch jede Horn-Formel erfüllbar, die keine Implikation der Form (2) enthält, z.B. indem man alle Aussagenvariablen mit 1 belegt.

Horn-Formeln können in polynomialer Zeit auf Erfüllbarkeit getestet werden mit dem folgendem Markierungsalgorithmus.

Erfüllbarkeitstest für Horn-Formeln

Input: Eine aussagenlogische Hornformel $\psi = \bigwedge_i C_i$
$N = \varnothing$
$M := \{X \in \tau(\psi) : \psi$ enthält C_i der Form $(1 \to X)\}$
while $N \neq M$ **do**
  $N := M$
  $M := M \cup \{X : \psi$ enthält C_i der Form $(X_1 \wedge \cdots \wedge X_k) \to X$ mit $\{X_1, \dots, X_k\} \subseteq M\}$
  if $[\psi$ enthält C_i der Form $(X_1 \wedge \ldots \wedge X_k) \to 0$ mit $\{X_1, \dots, X_k\} \subseteq M]$ **then**
   output "ψ unerfüllbar" **end**
  od
output "ψ erfüllbar", **output** M **end**

Die ausgegebene Menge M definiert eine Belegung $\mathfrak{I}_M$ mit $\mathfrak{I}_M(X) = 1$ gdw. $X \in M$.

Satz 1.12. *Der angegebene Erfüllbarkeitstest für Horn-Formeln ist korrekt. Wenn ψ erfüllbar ist, dann ist $\mathfrak{I}_M$ ein Modell von ψ. Für Formeln mit n Aussagenvariabeln hält der Erfüllbarkeitstest nach höchstens $n+1$ Iterationen der while-Schleife.*

Beweis. Sei $\mathfrak{I}$ ein beliebiges Modell von ψ. Offensichtlich muss $\mathfrak{I}(X) = 1$ sein für alle Aussagenvariabeln X, welche im Laufe dieser Prozedur markiert werden (d.h. die zu M hinzugefügt werden). Weiter kann es keine Teilformel C_i der Form $X_1 \wedge \cdots \wedge X_k \to 0$ in ψ geben, mit $X_1, \dots, X_k \in M$, da sonst $[\![\psi]\!]^{\mathfrak{I}} = 0$. Also stellt der Algorithmus korrekt die Erfüllbarkeit von ψ fest.

Wenn der Algorithmus ausgibt, dass ψ erfüllbar sei, dann ist $\mathfrak{I}_M$ tatsächlich ein Modell von ψ, denn die schliesslich erzeugte Menge M hat folgende Eigenschaften:

(1) Für alle Unterformeln $X_1 \wedge \ldots \wedge X_k \to X$ in ψ gilt: Wenn $\{X_1, \dots, X_k\} \subseteq M$, dann ist $X \in M$ (sonst würde die while-Schleife noch nicht verlassen).

(2) Für alle Unterformeln $X_1 \wedge \ldots \wedge X_k \to 0$ gilt: $\{X_1, \dots, X_k\} \nsubseteq M$ (sonst würde der Algorithmus die Unerfüllbarkeit feststellen).

Da in jedem Durchlauf der Schleife eine neue Aussagenvariable in M eingefügt wird, oder festgestellt wird, dass keine neuen mehr hinzugefügt werden müssen und die Schleife verlassen wird, folgt auch die letzte Behauptung. □

Bemerkung. Das durch den Markierungsalgorithmus gefundene Modell von ψ (wenn eines existiert) ist das *kleinste Modell*, denn für jedes andere Modell $\mathfrak{I} \models \psi$ gilt: Wenn $\mathfrak{I}_M(X) = 1$, dann auch $\mathfrak{I}(X) = 1$.

Im Gegensatz zu DNF- oder KNF-Formeln ist die Klasse der Horn-Formeln *keine* Normalform.

Satz 1.13. *Es gibt aussagenlogische Formeln die nicht zu einer Horn-Formel äquivalent sind.*

Beweis. Horn-Formeln sind entweder unerfüllbar oder haben ein kleinstes Modell. Dies trifft z.B. nicht zu auf die Formel $X \vee Y$. □

1.4 Der Kompaktheitssatz der Aussagenlogik

In vielen Anwendungen der Aussagenlogik hat man Erfüllbarkeit und Folgerungensbeziehungen für *unendliche* Formelmengen zu untersuchen. Ein grundlegender Satz, der Kompaktheits- oder Endlichkeitssatz, erleichtert diese Aufgabe, indem er sie auf die Untersuchung *endlicher* Teilmengen zurückführt.

Bevor wir ihn formulieren, erläutern wir die *Folgerungsbeziehung* zwischen Formelmengen und Formeln, einer der wichtigsten Begriffe in der Logik überhaupt, nicht nur für die Aussagenlogik sondern insbesondere für ausdrucksstärke Logiken und deren Anwendungen.

Definition 1.14. (Semantische Folgerungsbeziehung) Ein Modell einer Formelmenge $\Phi \subseteq \mathrm{AL}$ ist eine Interpretation $\mathfrak{I}$, so dass $[\![\varphi]\!]^{\mathfrak{I}} = 1$ für alle $\varphi \in \Phi$. Wir sagen, ψ *folgt aus* Φ (kurz: $\Phi \models \psi$) genau dann, wenn jede zu $\Phi \cup \{\psi\}$ passende Interpretation, welche Modell von Φ ist, auch Modell von ψ ist. Wenn $\Phi = \{\varphi\}$ schreiben wir auch $\varphi \models \psi$ anstelle von $\{\varphi\} \models \psi$.

Wenn $\Phi \models \psi$, dann legt die durch Φ festgelegte (axiomatisierte) Information bereits fest, dass auch ψ gilt, unabhängig von Variationen zwischen verschiedenen Modellen von Φ.

Man beachte, das dasselbe Symbol $\models$ sowohl für die Modellbeziehung ($\mathfrak{I} \models \psi$) wie auch für die Folgerungsbeziehung ($\Phi \models \psi$) verwendet wird. Missverständnisse sind ausgeschlossen, da die linke Seite die Bedeutung festlegt.

Übung 1.15. (Beispiele und elementare Eigenschaften der Folgerungsbeziehung) Verifizieren Sie die folgenden Aussagen:

(a) $\{\psi, \varphi\} \models \psi \wedge \varphi$
$\{\psi, \psi \rightarrow \varphi\} \models \varphi$

(b) Wenn $\Phi \cup \{\psi\} \models \varphi$ und $\Phi \cup \{\neg\psi\} \models \varphi$, dann gilt bereits $\Phi \models \varphi$.

(c) $\Phi \cup \{\psi\} \models \varphi$ genau dann, wenn $\Phi \models (\psi \rightarrow \varphi)$.

(d) ψ ist eine Tautologie genau dann, wenn ψ aus der leeren Menge folgt. (Dies rechtfertigt die Notation $\models \psi$, als abgekürzte Schreibweise für $\varnothing \models \psi$.)

(e) Es gilt $\Phi \models \varphi$ für jedes $\varphi \in \Phi$.

(f) Wenn $\Phi \models \psi$ dann gilt auch $\Phi' \models \psi$ für alle Obermengen $\Phi' \supseteq \Phi$.

(g) ψ und φ sind äquivalent genau dann, wenn $\psi \models \varphi$ und $\varphi \models \psi$.

(h) $\Phi \models \psi$ gilt genau dann, wenn $\Phi \cup \{\neg\psi\}$ unerfüllbar ist.

(i) Wenn $\Phi \models \psi$ und $\Phi \models \neg\psi$, dann ist Φ unerfüllbar. Umgekehrt gilt für unerfüllbare Formelmengen Φ, dass $\Phi \models \psi$ für *alle* $\psi \in \mathrm{AL}$.

(j) $\Phi \cup \{\psi\} \models \varphi$ genau dann, wenn $\Phi \models \psi \rightarrow \varphi$.

Satz 1.15 (Kompaktheits- oder Endlichkeitssatz). *Sei* $\Phi \subseteq \mathrm{AL}, \psi \in \mathrm{AL}$.

(i) Φ ist erfüllbar genau dann, wenn jede endliche Teilmenge von Φ erfüllbar ist.

(ii) $\Phi \models \psi$ genau dann, wenn eine endliche Teilmenge $\Phi_0 \subseteq \Phi$ existiert, so dass $\Phi_0 \models \psi$.

Wir lassen hier Formelmengen beliebiger Mächtigkeit zu und verwenden im Beweis das *Lemma von Zorn*, ein fundamentales Beweisprinzip in der Mathematik. Wenn man nur abzählbare Formelmengen Φ (und daher auch nur abzählbare Mengen von Aussagenvariablen) zulässt, dann könnte man den Beweis induktiv und ohne das Lemma von Zorn (aber nicht wirklich einfacher) führen. Ein Element einer partiell geordneten Menge heisst maximal, wenn es kein grösseres Element gibt.

Lemma 1.16 (Zorn). *Sei $(A, <)$ eine nicht-leere partielle Ordnung in der jede Kette nach oben beschränkt ist. Dann besitzt $(A, <)$ ein maximales Element.*

Im Fall den wir hier betrachten, wird A ein bestimmtes System von Formelmengen (also eine Menge von Mengen) sein, welches durch die Inklusionsbeziehung $\subseteq$ partiell geordnet ist. Eine Kette ist dann also eine Teilmenge B von A, so dass für alle $X, Y \in B$ entweder $X \subseteq Y$ oder $Y \subseteq X$ gilt. Die Voraussetzung, dass eine solche Kette B nach oben beschränkt sei, bedeutet, dass in A eine Menge S_B existiert, so dass $Y \subseteq S_B$ für alle $Y \in B$. Wenn diese Voraussetzung für alle Ketten B nachgewiesen werden kann, dann gibt es nach dem Lemma von Zorn ein maximales Element für ganz A, welches uns dann unmittelbar das gewünschte Modell liefern wird.

Nach diesen vorbereitenden Bemerkungen können wir nun den Kompaktheitssatz beweisen.

Beweis des Kompaktheitssatzes. Zu *(i):* Es ist klar, dass mit Φ auch jede endliche Teilmenge von Φ erfüllbar ist.

Für die Umkehrung nehmen wir an, dass jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar ist und setzen

$$A := \{\Psi : \Psi \supseteq \Phi \text{ und jede endliche Teilmenge von } \Psi \text{ ist erfüllbar}\}.$$

A ist partiell geordnet durch die Inklusionsbeziehung und nicht leer (da $\Phi \in A$).

Wir zeigen zuerst, dass die Voraussetzung des Zornschen Lemmas erfüllt ist. Sei $K \subseteq A$ eine Kette, d.h. es gilt $\Theta \subseteq \Psi$ oder $\Psi \subseteq \Theta$ für alle $\Psi, \Theta \in K$. Offensichtlich ist $\Gamma := \bigcup K$, die Vereinigung aller Mengen aus K, eine obere Schranke für K. Zu zeigen ist, dass Γ selbst in A enthalten ist, d.h., dass jede endliche Teilmenge $\Gamma_0 \subseteq \Gamma$ erfüllbar ist. Jede Formel $\gamma \in \Gamma_0$ ist in einer Menge $\Psi(\gamma) \in K$ enthalten. Da K eine Kette ist gibt es unter den endlich vielen Mengen $\Psi(\gamma)$ (für $\gamma \in \Gamma_0$) eine maximale, welche ganz Γ_0 enthält. Jede endliche Teilmenge dieser Menge ist erfüllbar, insbesondere also Γ_0.

Nach dem Lemma von Zorn hat demnach A ein maximales Element $\Phi_{\max}$. Wir behaupten, dass für jede Formel ψ entweder $\psi \in \Phi_{\max}$ oder $\neg\psi \in \Phi_{\max}$. Andernfalls betrachten wir die Erweiterungen $\Phi_{\max} \cup \{\psi\}$ und $\Phi_{\max} \cup \{\neg\psi\}$. Aufgrund der Maximalität von $\Phi_{\max}$ gehört keine dieser Mengen zu A. Also gibt es endliche Teilmengen $\Psi_0, \Psi_1 \subseteq \Phi_{\max}$ so dass $\Psi_0 \cup \{\psi\}$ und $\Psi_1 \cup \{\neg\psi\}$ unerfüllbar sind. Aber dann ist $\Psi_0 \cup \Psi_1$ eine endliche unerfüllbare Teilmenge von $\Phi_{\max}$, im Widerspruch zu $\Phi_{\max} \in A$.

Wir definieren nun eine Interpretation $\mathfrak{I}$ durch die Vorschrift

$$\mathfrak{I}(X) = 1 \iff X \in \Phi_{\max}.$$

Per Induktion über den Formelaufbau zeigen wir, dass $\mathfrak{I} \models \psi$ genau dann, wenn $\psi \in \Phi_{\max}$.

(a) Für atomare ψ folgt dies unmittelbar aus der Definition.

(b) Sei $\psi = \neg\varphi$. Dann ist nach Induktionsvorausetzung und nach der soeben gezeigten Eigenschaft von $\Phi_{\max}$

$$\mathfrak{I} \models \psi \iff \mathfrak{I} \not\models \varphi \iff \varphi \notin \Phi_{\max} \iff \psi \in \Phi_{\max}.$$

(c) Sei $\psi = \varphi \wedge \vartheta$. Nach Induktionsvoraussetzung folgt, dass $\mathfrak{I} \models \psi$ genau dann wenn $\varphi, \vartheta \in \Phi_{\max}$. Aber das ist genau dann der Fall, wenn auch $\psi \in \Phi_{\max}$.

Wenn nämlich $\psi \notin \Phi_{\max}$, dann $\neg\psi \in \Phi_{\max}$ was unmöglich ist, da $\Phi_{\max}$ dann mit $\{\varphi, \vartheta, \neg(\varphi \wedge \vartheta)\}$ eine unerfüllbare endliche Teilmenge enthalten würde. Wenn aber $\psi \in \Phi_{\max}$, dann müssen auch φ und ϑ in $\Phi_{\max}$ liegen, da sonst $\Phi_{\max}$ mit $\{\varphi \wedge \vartheta, \neg\varphi\}$ oder $\{\varphi \wedge \vartheta, \neg\vartheta\}$ wieder eine endliche unerfüllbare Teilmenge enthielte.

(d) Die Argumentation in allen andern Fällen ist analog. (Es wird empfohlen, zur Übung mindestens einen dieser Fälle, z.B. für Formeln $(\varphi \rightarrow \vartheta)$ selbst nachzuvollziehen.)

Also ist $\mathfrak{I}$ ein Modell von $\Phi_{\max}$ und damit auch von Φ.

Zu *(ii)*: Falls $\Phi_0 \models \psi$ für $\Phi_0 \subseteq \Phi$, dann gilt offensichtlich auch $\Phi \models \psi$. Es gelte umgekehrt $\Phi \models \psi$. Beweis durch Widerspruch: Zu jedem endlichen $\Phi_0 \subseteq \Phi$ gibt es ein $\mathfrak{I} : \tau \rightarrow \{0, 1\}$ mit $\mathfrak{I} \models \Phi_0$ aber $[\![\psi]\!]^{\mathfrak{I}} = 0$. Dies bedeutet, dass $\Phi_0 \cup \{\neg\psi\}$ für jedes endliche $\Phi_0 \subseteq \Phi$ erfüllbar ist. Also ist jede endliche Teilmenge von $\Phi \cup \{\neg\psi\}$ erfüllbar und damit, nach *(i)*, auch $\Phi \cup \{\neg\psi\}$ selbst. Dies ist aber ein Widerspruch zu $\Phi \models \psi$. □

Anwendung: Das Lemma von König. Ein *Baum mit Wurzel* w ist ein zusammenhängender, zykelfreier, gerichteter Graph $T = (V, E)$ mit einem ausgezeichnetem Knoten $w \in V$, so dass keine Kante in w endet (d.h. $(v, w) \notin E$ für alle $v \in V$) und in jedem andern Knoten genau eine Kante endet. Ein solcher Baum heisst *endlich verzweigt*, wenn von jedem v nur endlich viele Kanten ausgehen.

Lemma 1.17 (König). *Sei T ein endlich verzweigter Baum mit Wurzel w, in dem es beliebig lange endliche Wege gibt. Dann gibt es auch einen unendlichen Weg in T, der bei der Wurzel w beginnt.*

Beweis. Für den gegebenen Baum $T = (V, E)$ mit Wurzel w und $n \in \mathbb{N}$ sei

$$S_n = \{v \in V : \text{ es gibt einen Weg der Länge } n \text{ von } w \text{ nach } v\}.$$

Alle S_n sind endlich, da der Baum endlich verzweigt ist. Weiter ist $S_0 = \{w\}$ und alle S_n nicht leer, da es beliebig lange Wege in T gibt. Ein unendlicher, von w ausgehender Weg ist eine Menge $W \subseteq V$ welche folgende Bedingungen erfüllt:

(1) $|W \cap S_n| = 1$ für alle n;

(2) Wenn $v \in W$ und $(u, v) \in E$, dann ist auch $u \in W$.

Zu zeigen ist die Existenz einer solchen Menge W. Dazu ordnen wir jedem $v \in V$ eine Aussagenvariable X_v zu und setzen

$$\begin{aligned}
\alpha_n &:= \bigvee_{v \in S_n} X_v \\
\beta_n &:= \bigwedge_{u,v \in S_n, u \neq v} \neg(X_u \wedge X_v) \\
\Phi &:= \{\alpha_n : n \in \mathbb{N}\} \cup \{\beta_n : n \in \mathbb{N}\} \cup \{(X_v \to X_u) : (u,v) \in E\}
\end{aligned}$$

Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ ist erfüllbar. Um dies einzusehen, nehmen wir das grösste $n \in \mathbb{N}$ mit $\alpha_n \in \Phi_0$ oder $\beta_n \in \Phi_0$. Dann wählen wir ein $z \in S_n$ und den von w nach z führenden Weg $W(w,z)$. Sei

$$\mathfrak{I}(X_v) := \begin{cases} 1 & v \in W(w,z) \\ 0 & \text{sonst.} \end{cases}$$

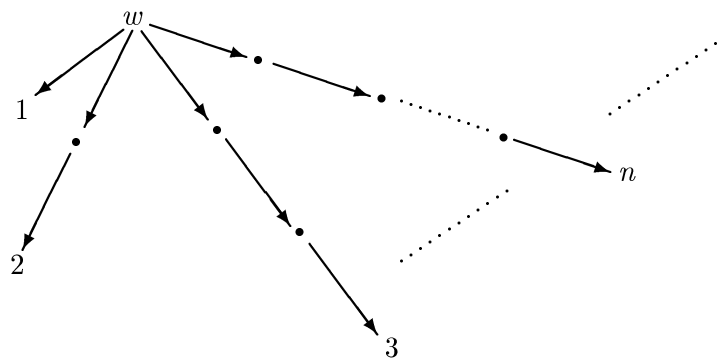
Offensichtlich ist $\mathfrak{I}$ Modell von Φ_0. Mit dem Kompaktheitssatz folgt, dass es ein Modell $\mathfrak{I}$ für Φ gibt. Setze $W := \{v \in V : \mathfrak{I}(X_v) = 1\}$. Es folgt, dass W einen unendlichen Weg von w aus definiert:

(1) Da $\alpha_n, \beta_n \in \Phi$, gibt es genau ein v in $W \cap S_n$.

(2) Sei $v \in W$ und $(u,v) \in E$. Da $\mathfrak{I} \models X_v$ und $\mathfrak{I} \models X_v \to X_u$ gilt auch $\mathfrak{I} \models X_u$, also $u \in W$.

□

Bemerkung. Man beachte, dass das Lemma von König nicht trivial ist. Es gilt z.B. nicht für Bäume mit unendlichen Verzweigungen. Betrachte etwa den folgenden Baum.



In diesem Baum gibt es für jedes n, ausgehend von w, einen Weg der Länge n, aber es gibt keinen unendlichen Weg.

Übung 1.16. Ein *Dominosystem* sei eine endliche Menge von quadratischen Dominosteinen gleicher Grösse, deren vier Kanten (oben, unten, links, rechts) gefärbt sind. Eine *Parkettierung* der Ebene (oder eines Teils davon) ist eine vollständige Überdeckung mit Dominosteinen, ohne Lücken und Überlappungen, so dass aneinandergrenzende Kanten dieselbe Farbe tragen. (Rotation der Steine ist nicht erlaubt.) Zeigen Sie mit Hilfe des Lemmas von König, dass für jedes Dominosystem folgendes gilt: Wenn beliebig grosse endliche Quadrate parkettiert werden können, dann auch die ganze Ebene.

Übung 1.17. Eine Formelmenge $\Phi \subseteq \mathrm{AL}$ ist *endlich axiomatisierbar* wenn eine endliche Formelmenge $\Phi_0 \subseteq \mathrm{AL}$ existiert, welche die gleichen Modelle hat wie Φ. Sei $\Phi = \{\varphi_n : n \in \mathbb{N}\}$ eine Formelmenge, so dass für alle $n \in \mathbb{N}$ gilt: $\varphi_{n+1} \models \varphi_n$, aber $\varphi_n \not\models \varphi_{n+1}$. Zeigen Sie, dass Φ nicht endlich axiomatisierbar ist.

Übung 1.18. Ein ungerichteter Graph $G = (V, E)$ heisst *k-färbbar*, wenn es eine Funktion $f : V \to \{1, \ldots, k\}$ gibt, so dass $f(p) \neq f(q)$ für alle Kanten $(p, q) \in E$. Zeigen Sie, dass ein ungerichteter Graph G *k-färbbar* ist, wenn jeder endliche Untergraph von G *k-färbbar* ist. Hinweis: Konstruieren Sie zu jedem endlichen Untergraphen von G eine aussagenlogische Formel, die genau dann erfüllbar ist, wenn der Untergraph k-färbbar ist. Führen Sie dazu zu jedem Knoten $g \in V$ und jeder Farbe i, $1 \leq i \leq k$, eine Aussagenvariable $X_{g,i}$ ein, die besagt, dass der Knoten g die Farbe i hat.

Übung 1.19. Sei $A \subseteq \{0,1\}^*$ eine unendliche Menge von Wörtern. Zeigen Sie, dass es eine unendliche Folge $w_0, w_1, w_2, \ldots$ gibt, so dass jedes w_i ein Anfangsstück von w_{i+1} und von mindestens einem Wort aus A ist.

Übung 1.20. (Definierbarkeitstheorem) Sei $\Phi \subseteq \mathrm{AL}$ eine Formelmenge, $X \in \tau(\Phi)$ eine Aussagenvariable. X heisst *explizit definierbar* in Φ, wenn eine Formel $\varphi \in \mathrm{AL}$ existiert, welche X nicht enthält, so dass $\Phi \models X \leftrightarrow \varphi$. (In Modellen von Φ ist also der Wahrheitswert von X durch eine Formel, die nicht von X abhängt, explizit festgelegt). Demgegenüber heisst X *implizit definierbar* in Φ, wenn für alle Modelle $\mathfrak{I}, \mathfrak{I}'$ von Φ gilt: Wenn $\mathfrak{I}(Z) = \mathfrak{I}'(Z)$ für alle Ausssagenvariablen $Z \neq X$, dann auch $\mathfrak{I}(X) = \mathfrak{I}'(X)$. (In Modellen von Φ ist also der Wahrheitswert von X durch die Wahrheitswerte der andern Variablen implizit festgelegt).

Beweisen Sie das *aussagenlogische Definierbarkeitstheorem*: Wenn X implizit in Φ definierbar ist, dann ist X auch explizit in Φ definierbar.

Hinweis: Die Formelmenge Φ' entstehe dadurch, dass man X in allen Formeln von Φ durch eine neue Aussagenvariable $X' \notin \tau(\Phi)$ ersetzt. Die implizite Definierbarkeit von X in Φ besagt dann, dass $\Phi \cup \Phi' \models X \leftrightarrow X'$. Benutzen Sie den Kompaktheitssatz um Φ durch eine endliche Formelmenge zu ersetzen und verwenden Sie das aussagenlogische Interpolationstheorem (Übung 1.6) um eine explizite Definition von X in Φ zu konstruieren.

1.5 Aussagenlogische Resolution

Resolution ist ein syntaktisches Verfahren, um die *Unerfüllbarkeit* von Formeln in KNF nachzuweisen. Es ist dabei nützlich, Formeln in KNF als Mengen von Klauseln darzustellen.

Definition 1.18. Eine *Klausel* ist eine endliche Menge von Literalen. Mit $\Box$ bezeichnet man die leere Klausel. Einer Formel $\psi = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} Y_{ij}$ in KNF wird eine endliche *Klauselmenge* $K(\psi)$ wie folgt zugeordnet: Jeder Disjunktion $\bigvee_{j=1}^{m_i} Y_{ij}$ ordnet man die Klausel $C_i = \{Y_{ij} : j = 1, \ldots, m_i\}$ zu und setzt $K(\psi) := \{C_1, \ldots, C_n\}$.

Bemerkung: Die Mengennotation ergibt gewisse Vereinfachungen: Elemente einer Menge haben keine Reihenfolge und keine Multiplizität. Daher gilt:

- Formeln, die sich nur durch Reihenfolge der auftretenden Teilformeln unterscheiden, ergeben dieselbe Klauselmenge.
- Mehrfach auftretende Literale in Disjunktionen, bzw. mehrfach auftretende Klauseln verschmelzen zu einem einzigen Element der Klauseln bzw. Klauselmengen.

Beispiel. Die Formeln $(X_1 \vee \neg X_2) \wedge X_3$, $(X_1 \vee X_1 \vee \neg X_2) \wedge (X_3 \vee X_3) \wedge X_3$ und $X_3 \wedge (X_1 \vee \neg X_2) \wedge (\neg X_2 \vee X_1)$ haben alle dieselbe Klauselmenge $K = \{\{X_1, \neg X_2\}, \{X_3\}\}$.

Umgekehrt entspricht einer Klausel C die Formel $\bigvee_{Y \in C} Y$. Einer endlichen Klauselmenge K entspricht die Formel $\bigwedge_{C \in K} \bigvee_{Y \in C} Y$.

Wir können also Klauseln und Klauselmengen wie Formeln und Formelmengen behandeln und benutzen Begriffe wie Erfüllbarkeit und Äquivalenz entsprechend. Insbesondere ist eine Klauselmenge erfüllbar, wenn es eine Interpretation $\mathfrak{I}$ gibt, so dass jede Klausel $C \in K$ ein Literal Y enthält mit $[\![Y]\!]^{\mathfrak{I}} = 1$. Beachte:

- Die leere Klauselmenge ist erfüllbar.
- Wenn $\Box \in K$, dann ist K unerfüllbar.

Definition 1.19. Seien C, C_1, C_2 Klauseln. C ist *Resolvente* von C_1 und C_2 genau dann, wenn es ein Literal Y gibt mit $Y \in C_1, \overline{Y} \in C_2$ und $C = (C_1 - \{Y\}) \cup (C_2 - \{\overline{Y}\})$. Dies wird folgendermassen notiert:

$$\begin{tikzcd}[column sep=small] C_1 \arrow[dr, dash] & & C_2 \arrow[dl, dash] \\ & C & \end{tikzcd}$$

Beispiele.

$$\begin{tikzcd}[column sep=small] \{X_1, X_3, \neg X_4\} \arrow[dr, dash] & & \{\neg X_2, X_4\} \arrow[dl, dash] \\ & \{X_1, \neg X_2, X_3\} & \end{tikzcd} \qquad \begin{tikzcd}[column sep=small] \{X_1\} \arrow[dr, dash] & & \{\neg X_1\} \arrow[dl, dash] \\ & \Box & \end{tikzcd}$$

Lemma 1.20 (Resolutionslemma). *Sei K eine Klauselmenge, $C_1, C_2 \in K$ und C Resolvente von C_1 und C_2. Dann sind K und $K \cup \{C\}$ äquivalent.*

Beweis. Wenn $[\![K \cup \{C\}]\!]^{\mathfrak{I}} = 1$, dann offensichtlich erst recht $[\![K]\!]^{\mathfrak{I}} = 1$. Sei umgekehrt $[\![K]\!]^{\mathfrak{I}} = 1$ und $C = (C_1 - \{Y\}) \cup (C_2 - \{\overline{Y}\})$.

(a) Wenn $[\![Y]\!]^{\mathfrak{I}} = 1$, dann ist $[\![C_2 - \{\overline{Y}\}]\!]^{\mathfrak{I}} = 1$, da sonst $[\![C_2]\!]^{\mathfrak{I}} = 0$. Also ist $[\![C]\!]^{\mathfrak{I}} = 1$.

(b) Wenn $[\![Y]\!]^{\mathfrak{I}} = 0$, dann ist $[\![C_1 - \{Y\}]\!]^{\mathfrak{I}} = 1$ und also wiederum $[\![C]\!]^{\mathfrak{I}} = 1$.

Also ist $[\![K \cup \{C\}]\!]^{\mathfrak{I}} = 1$. $\Box$

Definition 1.21. Für jede Klauselmenge K sei

(1) $Res(K) := K \cup \{C : C \text{ Resolvente zweier Klauseln aus } K\}$.

(2) $Res^0(K) := K,\ Res^{n+1}(K) := Res(Res^n(K))$.

(3) $Res^*(K) := \bigcup_{n \in \mathbb{N}} Res^n(K)$.

Korrektheit und Vollständigkeit des Resolutionskalküls. Ein Beweiskalkül ist *korrekt*, wenn keine falschen Aussagen darin ableitbar sind, und vollständig, wenn alle wahren Aussagen ableitbar sind. Der Resolutionskalkül ist ein Verfahren, um die *Unerfüllbarkeit* einer Klauselmenge K nachzuweisen, indem durch wiederholte Anwendung des Operators Res die leere Klausel abgeleitet wird. Die Korrektheit und Vollständigkeit des Resoltionskalküls wird durch den Resolutionssatz ausgedrückt.

Satz 1.22 (Resolutionssatz). *Eine Klauselmenge K ist unerfüllbar genau dann, wenn $\Box \in Res^*(K)$.*

Beweis. Korrektheit. Aus dem Resolutionslemma folgt $K \equiv Res(K)$ und damit per Induktion $K \equiv Res^*(K)$. Wenn also $\Box \in Res^*(K)$ dann ist $Res^*(K)$ und damit auch K unerfüllbar.

Vollständigkeit. Sei K unerfüllbar. Nach dem Kompaktheitssatz gibt es eine endliche unerfüllbare Teilmenge $K_0 \subseteq K$. Dann gibt es ein $n \in \mathbb{N}$, so dass K_0 höchstens die Aussagenvariablen $X_0, \dots, X_{n-1}$ enthält. Wir zeigen per Induktion nach n, dass $\Box \in Res^*(K_0) \subseteq Res^*(K)$.

Sei $n = 0$. Es gibt nur zwei Klauselmengen ohne Aussagenvariablen, nämlich $\varnothing$ und $\{\Box\}$. Da die leere Klauselmenge erfüllbar ist, muss $K_0 = \{\Box\}$ sein. Für den Induktionsschluss nehmen wir an, dass alle Aussagenvariablen von K_0 in $\{X_0, \dots, X_n\}$ enthalten seien. Wir konstruieren zwei Klauselmengen K_0^+, K_0^- in denen X_n nicht vorkommt: $K_0^+ := \{C - \{\neg X_n\} : X_n \notin C, C \in K_0\}$ (d.h. wir streichen aus K_0 alle Klauseln, in denen X_n vorkommt und streichen $\neg X_n$ aus allen verbleibenden Klauseln). Indem wir die Rollen von X_n und $\neg X_n$ vertauschen, erhalten wir $K_0^- := \{C - \{X_n\} : \neg X_n \notin C, C \in K_0\}$.

K_0^+ und K_0^- sind unerfüllbar. Anderfalls gäbe es etwa ein $\mathfrak{I} : \{X_0, \dots, X_{n-1}\} \to \{0, 1\}$ so, dass $[\![K_0^+]\!]^{\mathfrak{I}} = 1$. Erweitere $\mathfrak{I}$ durch $\mathfrak{I}(X_n) = 1$. Es gilt dann $[\![K_0]\!]^{\mathfrak{I}} = 1$, im Widerspruch zur Unerfüllbarkeit von K_0.

Aus der Induktionsvoraussetzung folgt, dass $\Box \in Res^*(K_0^+)$ und $\Box \in Res^*(K_0^-)$. Also gibt es Klauseln $C_1, C_2, \dots, C_m$, so dass $C_m = \Box$ und für $i = 1, \dots, m$ gilt $C_i \in K_0^+$ oder C_i ist Resolvente von C_j, C_k für $j, k < i$. Einige der Klauseln C_i können aus Klauseln in K_0 durch Streichen von $\neg X_n$ entstanden sein. Wenn nicht, dann sind $C_1, \dots, C_m$ auch in $Res^*(K_0)$, also $\Box \in Res^*(K_0)$. Wenn ja, erhalten wir durch Wiedereinfügen von $\neg X_n$ eine Folge von Klauseln $C'_1, \dots, C'_m$ welche beweist, dass $\{\neg X_n\} \in Res^*(K_0)$.

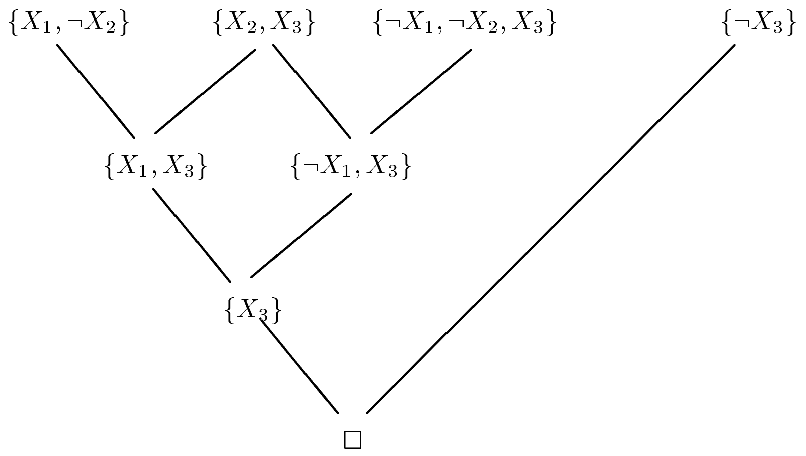
$$\begin{tikzcd} C_j \arrow[dr, dash] & & C_k \arrow[dl, dash] \\ & C_i & \end{tikzcd} \quad \Longrightarrow \quad \begin{tikzcd} C_j \cup \{\neg X_n\} \arrow[dr, dash] & & \{C_k\} \arrow[dl, dash] \\ & C_i \cup \{\neg X_n\} & \end{tikzcd}$$

Analog folgt aus $\Box \in Res^*(K_0^-)$, dass entweder $\Box \in Res^*(K_0)$ oder $\{X_n\} \in Res^*(K_0)$. Mit

$$\begin{tikzcd} \{\neg X_n\} \arrow[dr, dash] & & \{X_n\} \arrow[dl, dash] \\ & \Box & \end{tikzcd}$$

folgt, dass $\Box \in Res^*(K_0)$. $\Box$

Beispiel. Sei $\psi = (X_1 \vee \neg X_2) \wedge \neg X_3 \wedge (\neg X_1 \vee \neg X_2 \vee X_3) \wedge (X_2 \vee X_3)$. Dann ist $K = K(\psi) = \{\{X_1, \neg X_2\}, \{\neg X_3\}, \{\neg X_1, \neg X_2, X_3\}, \{X_2, X_3\}\}$. Die leere Klausel ist wie folgt aus $K(\psi)$ ableitbar:



Wenn K nur die Aussagenvariablen $X_0, \dots, X_{n-1}$ enthält, dann gilt dies auch für $Res^*(K)$, denn eine Resolvente zweier Klauseln C, C', enthält nur Literale, die bereits in C oder C' enthalten sind. Insbesondere folgt, dass die Kette

$$K = Res^0(K) \subseteq Res^1(K) \subseteq \dots \subseteq Res^m(K) \subseteq \dots$$

nach höchstens 2^{2n} Schritten abbricht, d.h. $Res^*(K) = Res^{2^{2n}}(K)$, denn es gibt nur 2^{2n} verschiedene Klauseln mit Literalen $X_0, \dots, X_{n-1}, \neg X_0, \dots, \neg X_{n-1}$.

Für endliche Klauselmengen K erhält man also folgenden Algorithmus um zu entscheiden, ob K erfüllbar ist:

Erfüllbarkeitstest mit Resolution

Input: K (endliche Klauselmenge)
$R := \varnothing, S := K$
while $R \neq S$ **do**
    $R := S$
    $S := Res(R)$
    if $\Box \in S$ **then**
        output „K unerfüllbar" **end**
    od
output „K erfüllbar" **end**

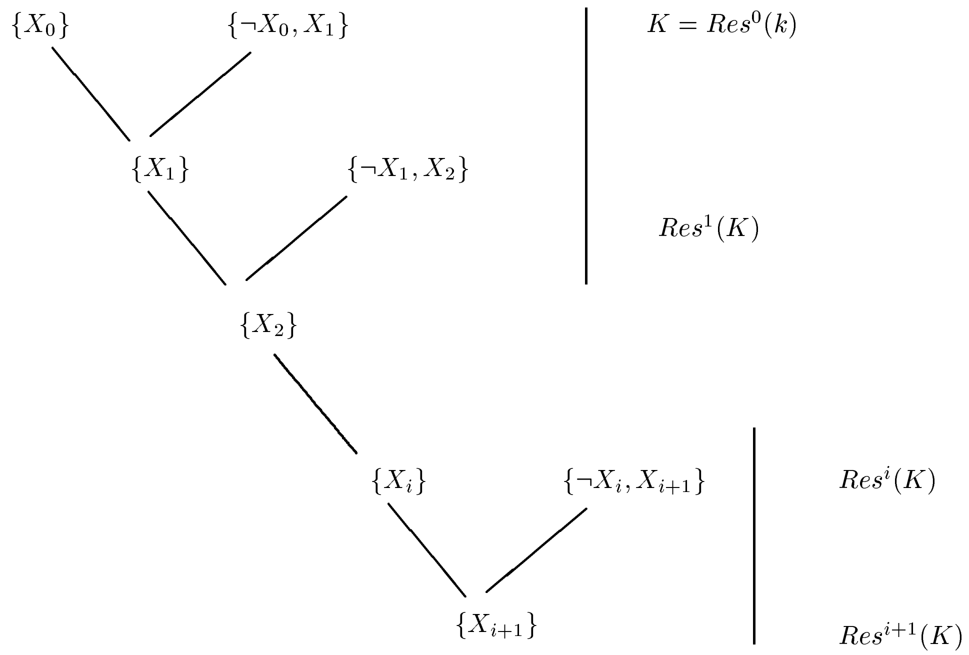
Dieser Algorithmus hat (im worst case) exponentielle Komplexität. Es ist auch nicht zu erwarten, dass es einen effizienten (in polynomialer Zeit laufenden) Algorithmus für dieses Problem gibt, denn das Erfüllbarkeitsproblem für KNF-Formeln ist NP-vollständig.

Die Erfüllbarkeit einer Formel ist durch eine Existenzaussage ausgedrückt (es gibt ein Modell). Die Unerfüllbarkeit (oder die Allgemeingültigkeit) einer Formel ist eine Aussage über alle möglichen Interpretationen, ihrer Natur nach also eine universelle Aussage. Der Resolutionskalkül (wie jeder korrekte und vollständige Beweiskalkül) erlaubt nun, solche universellen Ausagen durch äquivalente Existenzaussagen auszudrücken: ψ ist unerfüllbar, wenn eine Deduktion der leeren Klausel existiert.

Man beachte aber folgende Asymmetrie: Das Aufschreiben einer Modells für ψ (also eines 'Zeugen' für die Erfüllbarkeit) ist mit viel weniger Aufwand verbunden, als (im worst case) das Aufschreiben eines Resolutionsbeweises (also eines 'Zeugen' für die Unerfüllbarkeit). Dies hängt mit einem der wichtigsten Probleme der Komplexitätstheorie zusammen, dem Problem ob NP = Co-NP.

Für unendliche Klauselmengen kann es durchaus passieren, dass $Res(K) - K$ unendlich ist, oder dass die Kette $K = Res^0(K) \subset Res^1(K) \subset \cdots \subset Res^n(K) \subset \ldots$ nicht stationär wird (auch wenn K erfüllbar ist).

Beispiel. Sei $K = \{\{X_0\}\} \cup \{\{\neg X_i, X_{i+1}\} : i \in \mathbb{N}\}$.



Einheitsresolution für Horn-Formeln. Die einer Horn-Formel zugeordnete Klauselmenge $K(\psi)$ enthält nur Klauseln der Form $\{\neg X_1, \ldots, \neg X_k\}$ (nur negative Literale) oder $\{\neg X_1, \ldots, \neg X_k, X\}$ (ein positives Literal). Solche Klauseln heissen *Horn-Klauseln.* Für $k = 0$ ergibt sich, dass die leere Klausel $\Box$ und die Klauseln $\{X\}$, welche aus einer einzigen Aussagenvariabeln bestehen, auch Horn-Klauseln sind. Wir präsentieren nun eine eingeschränkte Variante des Resolutionskalküls, welche vollständig ist für Horn-Formeln.

Definition 1.23. Seien C, C_1, C_2 Klauseln. C ist *Einheitsresolvente* von C_1 und C_2, wenn C Resolvente von C_1 und C_2 ist und entweder $|C_1| = 1$ oder $|C_2| = 1$.

Bei der Einheitsresolution besteht also mindestens eine der Ausgangsklauseln nur aus einem einzigen Literal.

Satz 1.24 (Vollständigkeit der Einheitsresolution für Horn-Formeln). *Eine aussagenlogische Horn-Formel ψ ist unerfüllbar genau dann, wenn $\Box$ durch Einheitsresolution aus $K(\psi)$ ableitbar ist.*

Beweis. Es ist klar, dass ψ unerfüllbar ist, wenn $\Box$ aus $K(\psi)$ durch Einheitsresolution (also insbesondere durch Resolution) ableitbar ist.

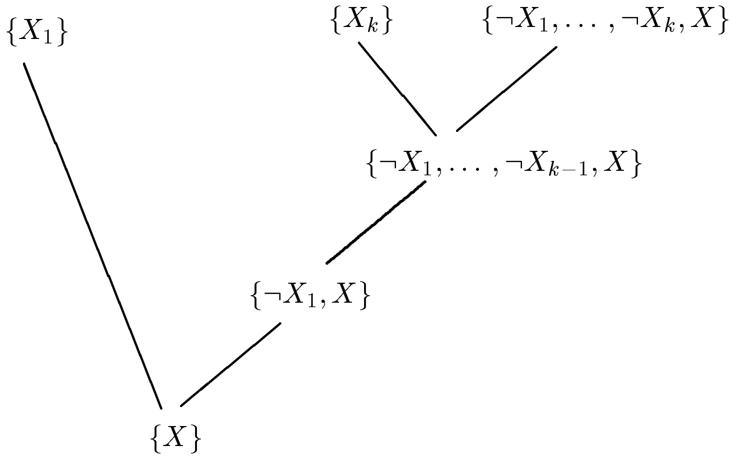
Für die Umkehrung betrachten wir den Erfüllbarkeitstest für Horn-Formeln. Setze:

$$\begin{aligned} M^0 &:= \{X : K(\psi) \text{ enthält die Klausel } \{X\}\} \\ M^{i+1} &:= M^i \cup \{X : \text{ es gibt } X_1, \dots, X_k \in M_i, \text{ so dass } K(\psi) \text{ die Klausel} \\ &\qquad\qquad \{\neg X_1, \dots, \neg X_k, X\} \text{ enthält}\}. \end{aligned}$$

$$M^* := \bigcup_{i \in \mathbb{N}} M^i.$$

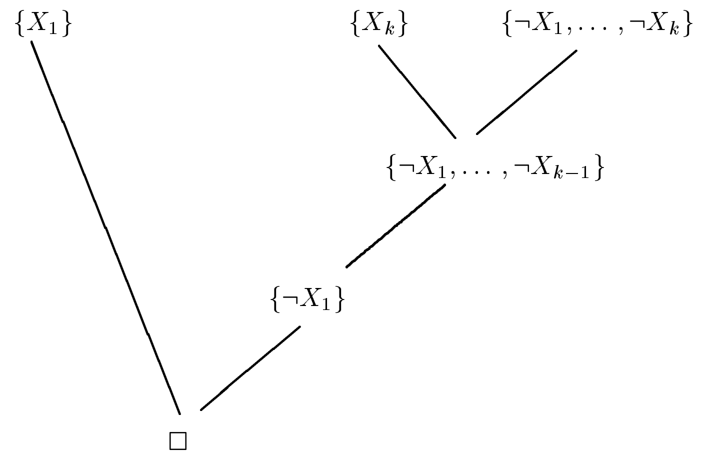
Die Korrektheit des Erfüllbarkeitstests (Satz 1.12) ergibt: ψ ist unerfüllbar genau dann, wenn $X_1, \dots, X_k \in M^*$ existieren, so dass $\{\neg X_1, \dots, \neg X_k\} \in K(\psi)$. Wir zeigen: Wenn $X \in M^*$, dann ist $\{X\}$ per Einheitsresolution aus $K(\psi)$ ableitbar.

Für $X \in M^0$ ist dies klar. Wenn $X \in M^{i+1}$, dann ist entweder $X \in M^i$ (dann greift die Induktionsvoraussetzung) oder es gibt $X_1, \dots, X_k \in M^i$, so dass $\{\neg X_1, \dots, \neg X_k, X\} \in K(\psi)$.



Ableitung von $\{X\}$ per Einheitsresolution.

Wenn ψ unerfüllbar ist, dann gibt es also $\{\neg X_1, \dots, \neg X_k\} \in K(\psi)$, so dass die Einerklauseln $\{X_1\}, \dots, \{X_k\}$ per Einheitsresolution aus $K(\psi)$ ableitbar sind. Damit folgt nun sofort, dass $\Box$ per Einheitsresolution aus $K(\psi)$ abgeleitet werden kann.



Ableitung von $\Box$ per Einheitsresolution.

Damit ist die Vollständigkeit der Einheitsresolution für Horn-Formeln bewiesen. $\Box$

1.6 Der aussagenlogische Sequenzenkalkül

Wir beschreiben durch *Axiome* und *Schlussregeln* einen im wesentlichen auf Gentzen zurückgehenden Beweiskalkül SK, den *Sequenzenkalkül.* Dieser Kalkül operiert auf Paaren von endlichen Formelmengen, welche wir *Sequenzen* nennen. Im Folgenden bezeichnen Γ, Δ endliche Mengen aussagenlogischer Formeln. Wir schreiben Γ, Δ für $\Gamma \cup \Delta$ und Γ, ψ für $\Gamma \cup \{\psi\}$. Die Ausdrücke $\bigwedge \Gamma$ bzw. $\bigvee \Gamma$ stehen für die Konjunktion bzw. Disjunktion über alle Formeln in Γ.

Definition 1.25. Eine *Sequenz* ist ein Ausdruck der Form $\Gamma \Rightarrow \Delta$ für endliche Formelmengen $\Gamma, \Delta \subseteq \mathrm{AL}$. Wir nennen Γ das *Antezedens* und Δ das *Sukzedens* der Sequenz $\Gamma \Rightarrow \Delta$.

Die Sequenz $\Gamma \Rightarrow \Delta$ ist *gültig*, wenn jedes Modell von Γ auch ein Modell mindestens einer Formel aus Δ ist, d.h. wenn $\bigwedge \Gamma \models \bigvee \Delta$. Wenn also $\Gamma \Rightarrow \Delta$ *nicht* gültig ist, dann existiert eine Interpretation $\mathfrak{I}$ in der alle Formeln aus Γ wahr und alle Formeln aus Δ falsch sind. In diesem Fall sagen wir, dass $\mathfrak{I}$ die Sequenz $\Gamma \Rightarrow \Delta$ *falsifiziert*.

Beispiele. (1) Jede Sequenz $\Gamma \Rightarrow \Delta$ mit $\Gamma \cap \Delta \neq \varnothing$ ist gültig. Solche Sequenzen sind die *Axiome* des Sequenzenkalküls.

(2) Seien Γ, Δ Mengen von *Aussagenvariablen.* Die Sequenz $\Gamma \Rightarrow \Delta$ ist falsifizierbar genau dann, wenn Γ und Δ disjunkt sind.

(3) Eine Sequenz der Form $\Gamma \Rightarrow \varnothing$ ist gültig genau dann, wenn Γ unerfüllbar ist.

(4) Eine Sequenz $\varnothing \Rightarrow \Delta$ ist gültig genau dann, wenn $\bigvee \Delta$ gültig ist.

Die genaue Formulierung eines Beweiskalküls hängt von den verwendeten Junktoren ab. Wir behandeln hier den aussagenlogischen Sequenzenkalkül für Formeln, welche aus den Junktoren $\neg$, $\wedge, \vee$ und $\rightarrow$ aufgebaut sind.

Definition 1.26. Die *Axiome* von SK sind alle Sequenzen der Form $\Gamma, \psi \Rightarrow \Delta, \psi$. Die *Schlussregeln* von SK sind:

$$(\neg \Rightarrow)\quad \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma, \neg\psi \Rightarrow \Delta} \qquad\qquad (\Rightarrow \neg)\quad \frac{\Gamma, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\psi}$$

$$(\vee \Rightarrow)\quad \frac{\Gamma, \psi \Rightarrow \Delta \qquad \Gamma, \vartheta \Rightarrow \Delta}{\Gamma, \psi \vee \vartheta \Rightarrow \Delta} \qquad\qquad (\Rightarrow \vee)\quad \frac{\Gamma \Rightarrow \Delta, \psi, \vartheta}{\Gamma \Rightarrow \Delta, \psi \vee \vartheta}$$

$$(\wedge \Rightarrow)\quad \frac{\Gamma, \psi, \vartheta \Rightarrow \Delta}{\Gamma, \psi \wedge \vartheta \Rightarrow \Delta} \qquad\qquad (\Rightarrow \wedge)\quad \frac{\Gamma \Rightarrow \Delta, \psi \qquad \Gamma \Rightarrow \Delta, \vartheta}{\Gamma \Rightarrow \Delta, \psi \wedge \vartheta}$$

$$(\rightarrow\Rightarrow)\quad \frac{\Gamma \Rightarrow \Delta, \psi \qquad \Gamma, \vartheta \Rightarrow \Delta}{\Gamma, \psi \rightarrow \vartheta \Rightarrow \Delta} \qquad\qquad (\Rightarrow\rightarrow)\quad \frac{\Gamma, \psi \Rightarrow \Delta, \vartheta}{\Gamma \Rightarrow \Delta, \psi \rightarrow \vartheta}$$

Hier können jeweils für Γ, Δ, Σ beliebige endliche Formelmengen und für ψ, φ, ϑ beliebige Formeln eingesetzt werden. Jede Regel besteht aus einer oder zwei Sequenzen in der oberen Zeile, genannt *Prämissen* und einer Sequenz in der unteren Zeile, genannt *Konklusion*.

Definition 1.27. Die Menge der *ableitbaren Sequenzen* von SK ist die induktiv durch die Axiome und Schlussregeln definierte Sequenzenmenge, d.h. die kleinste Menge, welche alle Axiome umfasst und mit jeder Instanz der oberen Zeile einer Schlussregel auch die entsprechende Instanz der unteren Zeile enthält.

Ein *Beweis in* SK ist ein Baum, dessen Knoten auf folgende Weise mit Sequenzen beschriftet sind:

(1) Jedes Blatt ist mit einem Axiom beschriftet.

(2) Jeder innere Knoten des Baumes ist mit der unteren Zeile einer Schlussregel von SK beschriftet; die Kinder dieses Knotens müssen dann gerade mit den in der oberen Zeile dieser Regel auftretenden Sequenz beschriftet sein. Also hat jeder innere Knoten ein oder zwei Kinder.

Es folgt, dass eine Sequenz genau dann in SK ableitbar ist, wenn sie als Beschriftung eines Knotens in einem Beweis von SK auftritt.

Beispiel. Hier ist ein Beweis für die Sequenz $\psi, (\varphi \vee \vartheta) \Rightarrow (\psi \wedge \varphi), (\psi \wedge \vartheta)$.

$$\frac{\dfrac{\psi, \varphi \Rightarrow \psi, (\psi \wedge \vartheta) \qquad \psi, \varphi \Rightarrow \varphi, (\psi \wedge \vartheta)}{\psi, \varphi \Rightarrow (\psi \wedge \varphi), (\psi \wedge \vartheta)} \qquad \dfrac{\psi, \vartheta \Rightarrow (\psi \wedge \varphi), \psi \qquad \psi, \vartheta \Rightarrow (\psi \wedge \varphi), \vartheta}{\psi, \vartheta \Rightarrow (\psi \wedge \varphi), (\psi \wedge \vartheta)}}{\psi, (\varphi \vee \vartheta) \Rightarrow (\psi \wedge \varphi), (\psi \wedge \vartheta)}$$

Wie bei jedem Beweiskalkül sind auch beim Sequenzenkalkül zwei grundlegende Eigenschaften zu überprüfen:

Korrektheit: Es können *nur* gültige Objekte abgeleitet werden.

Vollständigkeit: Es können *alle* gültigen Objekte abgeleitet werden.

Die Korrektheit des Sequenzenkalküls ist leicht nachzuweisen.

Lemma 1.28. *Für jede Regel des Sequenzenkalküls und jede aussenlogische Interpretation $\mathfrak{I}$ (deren Definitionsbereich alle vorkommenden Aussagenvariablen umfasst) gilt: $\mathfrak{I}$ falsifiziert die Konklusion der Regel genau dann wenn $\mathfrak{I}$ eine Prämisse der Regel falsifiziert. Es folgt, dass die Konklusion gültig ist genau dann, wenn die Prämissen gültig sind.*

Übung 1.21. Beweisen Sie dieses Lemma.

Eine unmittelbare Konsequenz ist der Korrektheitssatz für SK.

Satz 1.29 (Korrektheit des Sequenzenkalküls). *Jede in* SK *ableitbare Sequenz* $\Gamma \Rightarrow \Delta$ *ist gültig.*

Aus dem Sequenzenkalkül gewinnen wir unmittelbar auch einen formalen Ableitungsbegriff für *Formeln* (statt Sequenzen).

Definition 1.30. Sei $\Phi \subseteq \mathrm{AL}$ eine Formelmenge. Eine aussagenlogische Formel ψ ist *ableitbar* aus der Hypothesenmenge Φ, (kurz: $\Phi \vdash \psi$), wenn eine endliche Teilmenge Γ von Φ existiert, so dass die Sequenz $\Gamma \Rightarrow \psi$ im Sequenzenkalkül ableitbar ist. Insbesondere ist ψ aus der leeren Hypothesenmenge ableitbar (kurz: $\vdash \psi$) wenn die Sequenz $\varnothing \Rightarrow \psi$ in SK abgeleitet werden kann.

Der Sequenzenkalkül erlaubt die *systematische Suche und Analyse* von Beweisen. Dies ist ein wichtiger Vorteil gegenüber vielen andern Beweiskalkülen (z.B. dem Hilbertkalkül). Wir werden einen Algorithmus angeben, welcher zu jeder gegebenen Sequenz $\Gamma \Rightarrow \Delta$ entweder einen Beweis konstruiert, oder aber eine Interpretation findet, welche jede Formal aus Γ, aber keine aus Δ erfüllt und damit den Nachweis liefert, dass $\Gamma \Rightarrow \Delta$ nicht ableitbar ist.

Wir erläutern diesen Algorithmus zunächst an zwei Beispielen.

Beispiele. (1) Betrachte die Formel $\psi := (X \rightarrow Y) \rightarrow (\neg Y \rightarrow \neg X)$. Wir suchen also einen Beweis in SK für die Sequenz $\varnothing \Rightarrow \psi$. Wir beobachten zunächst, dass ψ die Form $(\varphi \rightarrow \vartheta)$ hat. Die einzige Regel, die zu einer Sequenz der Form $\varnothing \Rightarrow (\varphi \rightarrow \vartheta)$ führen kann ist die Regel $(\Rightarrow\rightarrow)$. Diese Regel kann aber nur angewandt werden, wenn vorher die Sequenz $\varphi \Rightarrow \vartheta$, d. h. die Sequenz $(X \rightarrow Y) \Rightarrow (\neg Y \rightarrow \neg X)$ abgeleitet wurde. Wir beginnen also die Konstruktion des Ableitungsbaums so:

$$\frac{(X \rightarrow Y) \Rightarrow (\neg Y \rightarrow \neg X)}{\varnothing \Rightarrow (X \rightarrow Y) \rightarrow (\neg Y \rightarrow \neg X)}$$

Um nun $(X \rightarrow Y) \Rightarrow (\neg Y \rightarrow \neg X)$ abzuleiten, können wir entweder mit der Regel $(\rightarrow\Rightarrow)$ auf dem Antezedens oder mit der Regel $(\Rightarrow\rightarrow)$ auf dem Sukzedens arbeiten. Die erste Möglichkeit führt zu einer Verzweigung des Ableitungsbaums:

$$\frac{\dfrac{\varnothing \Rightarrow X, (\neg Y \rightarrow \neg X) \qquad Y \Rightarrow (\neg Y \rightarrow \neg X)}{(X \rightarrow Y) \Rightarrow (\neg Y \rightarrow \neg X)}}{\varnothing \Rightarrow (X \rightarrow Y) \rightarrow (\neg Y \rightarrow \neg X)}$$

Die beiden Blätter werden nun mit den Regeln $(\Rightarrow\rightarrow)$ und dann $(\neg \Rightarrow)$ und $(\Rightarrow \neg)$ weiter bearbeitet. Dies führt schliesslich zu folgendem Ableitungsbaum:

$$\dfrac{\dfrac{\dfrac{\dfrac{X, \neg Y \Rightarrow X}{\neg Y \Rightarrow X, \neg X}}{\varnothing \Rightarrow X, (\neg Y \to \neg X)} \qquad \dfrac{\dfrac{Y \Rightarrow \neg X, Y}{Y, \neg Y \Rightarrow \neg X}}{Y \Rightarrow (\neg Y \to \neg X)}}{(X \to Y) \Rightarrow (\neg Y \to \neg X)}}{\varnothing \Rightarrow (X \to Y) \to (\neg Y \to \neg X)}$$

Die Blätter dieses Baumes sind Axiome und wir haben damit einen Beweis für die gegebene Sequenz gefunden.

Wenn wir nach dem ersten Ableitungsschritt die zweite Möglichkeit gewählt hätten und mit der Regel ($\Rightarrow\to$) auf dem Sukzedens weitergearbeitet hätten, dann wären wir schliesslich zum Beweis

$$\dfrac{\dfrac{\dfrac{\dfrac{X \Rightarrow X, Y \qquad X, Y \Rightarrow Y}{(X \to Y), X \Rightarrow Y}}{X \to Y, \neg Y \Rightarrow \neg X}}{(X \to Y) \Rightarrow (\neg Y \to \neg X)}}{\varnothing \Rightarrow (X \to Y) \to (\neg Y \to \neg X)}$$

gekommen. Wir sehen also, dass es verschiedene Beweise derselben Sequenz gibt.

(2) Als zweites Beispiel betrachten wir die Sequenz $(X \vee Y) \Rightarrow (X \wedge Y)$. Die Konstruktion des Ableitungsbaums führt mit der Regel ($\Rightarrow \wedge$) zunächst auf den Baum

$$\frac{X \vee Y \Rightarrow X \quad X \vee Y \Rightarrow Y}{X \vee Y \Rightarrow X \wedge Y}.$$

Mit der Regel ($\vee \Rightarrow$) erhalten wir dann den Ableitungsbaum

$$\dfrac{\dfrac{X \Rightarrow X \quad Y \Rightarrow X}{X \vee Y \Rightarrow X} \qquad \dfrac{X \Rightarrow Y \quad Y \Rightarrow Y}{X \vee Y \Rightarrow Y}}{X \vee Y \Rightarrow X \wedge Y}$$

Die Blätter bestehen nur aus Aussagenvariablen, aber nur die äussern beiden sind Axiome. Die beiden Blätter $Y \Rightarrow X$ und $X \Rightarrow Y$ werden durch die Interpretationen falsifiziert, welche eine der Aussagenvariablen X, Y mit wahr, die andere aber mit falsch belegen. Diese Interpretationen falsifizieren auch die Ausgangssequenz $(X \vee Y) \Rightarrow (X \wedge Y)$. Der Versuch, einen Beweis für diese Sequenz zu konstruieren führt also zu einer Interpretation welche die Sequenz falsifiziert und damit (wegen der Korrektheit des Sequenzenkalküls) nachweist, dass kein Beweis existiert.

Die systematische Beweissuche beruht darauf, dass zu jeder Sequenz $\Gamma \Rightarrow \Delta$ und jeder darin vorkommenden nicht-atomaren Formel ψ genau eine Regel mit der Konklusion $\Gamma \Rightarrow \Delta$ existiert in deren Prämissen ψ nicht vorkommt. Der Algorithmus baut nun wie in den beiden Beispielen, ausgehend von der zu beweisenden Sequenz einen Ableitungsbaum auf, indem er rückwärts von der Konklusion und einer daraus ausgewählten Formel die entsprechende Regel bestimmt und den Baum um die Prämissen dieser Regel erweitert, bis entweder eine rein atomare, falsifizierbare Sequenz gefunden wird oder alle Blätter mit Axiomen beschriftet sind.

Definition 1.31. Ein *Ableitungsbaum* T für eine Sequenz S ist ein Baum, dessen Wurzel mit S beschriftet ist, so dass jeder innere Knoten von T mit der unteren Zeile einer Schlussregel und die Kinder dieses Knotens mit den in der oberen Zeile derselben Regel auftretenden Sequenzen beschriftet sind.

Ein mit einem Axiom beschriftetes Blatt eines Ableitungsbaumes nennen wir *positiv*. Ein Blatt ist *negativ*, wenn es mit einer Sequenz $\Gamma \Rightarrow \Delta$ beschriftet ist, wobei Γ und Δ disjunkte Mengen von Aussagenvariablen sind. Ein Ableitungsbaum ist *vollständig*, wenn alle seine Blätter positiv oder negativ sind.

Ein Beweis ist demnach ein Ableitungsbaum, dessen Blätter alle positiv sind (und welcher daher insbesondere vollständig ist). Ein Ableitungsbaum, der ein negatives Blatt enthält, nennen wir eine *Widerlegung*.

Wir sind nun in der Lage, einen Algorithmus anzugeben, welcher zu jeder gegebenen aussagenlogischen Sequenz entweder einen Beweis oder eine Widerlegung findet.

Beweissuche im aussagenlogischen Sequenzenkalkül

Input: Eine aussagenlogische Sequenz $\Gamma \Rightarrow \Delta$

Ein Ableitungsbaum für $\Gamma \Rightarrow \Delta$ wird induktiv wie folgt aufgebaut. Zu Beginn sei T der Baum, der nur aus der Wurzel besteht, beschriftet mit $\Gamma \Rightarrow \Delta$. Solange T noch unmarkierte Blätter enthält, werden folgende Operationen ausgeführt:

Wähle ein unmarkiertes Blatt ℓ; sei $\Gamma' \Rightarrow \Delta'$ die Beschriftung von ℓ.

Wenn ℓ negativ ist, dann wird die Interpretation konstruiert welche alle Aussagenvariablen in Γ' mit wahr und alle andern mit falsch bewertet. Diese wird als falsifizierende Interpretation für $\Gamma \Rightarrow \Delta$ ausgegeben. Die Prozedur ist damit beendet.

Wenn ℓ positiv ist wird ℓ mit (+) markiert.

Andernfalls wird eine nicht-atomare Formel ψ aus $\Gamma' \Rightarrow \Delta'$ ausgewählt und die (eindeutig festgelegte) Regel bestimmt deren Konklusion $\Gamma' \Rightarrow \Delta'$ ist und deren Prämissen ψ nicht mehr enthalten. Dann wird T um ein oder zwei Nachfolgeknoten von ℓ erweitert, welche mit den Prämissen dieser Regel beschriftet werden.

Wenn alle Blätter mit (+) markiert sind, wird T als Beweis für $\Gamma \Rightarrow \Delta$ ausgegeben und die Prozedur beendet.

Satz 1.32. *Der angegebene Suchalgorithmus terminiert auf jeder gegebenen Sequenz* $\Gamma \Rightarrow \Delta$ *in endlich vielen Schritten. Er findet einen Beweis genau dann wenn* $\Gamma \Rightarrow \Delta$ *gültig ist; andernfalls findet er eine falsifizierende Interpretation für* $\Gamma \Rightarrow \Delta$.

Beweis. Die Komplexität einer Sequenz sei die Anzahl, der in ihr vorkommenden Junktoren. Für jede Regel von SK gilt, dass die Komplexität der Konklusion echt grösser ist als die Komplexität der Prämissen. Deshalb kann die Tiefe des konstruierten Ableitungsbaum nicht grösser sein als die Komplexität der Ausgangssequenz; der Algorithmus muss also terminieren.

Wenn der Algorithmus auf $\Gamma \Rightarrow \Delta$ einen Ableitungsbaum T findet dessen Blätter alle mit (+) markiert sind (deren Beschriftungen also Axiome sind), dann ist T offensichtlich ein Beweis für $\Gamma \Rightarrow \Delta$. Aufgrund der Korrektheit des Sequenzenkalküls ist $\Gamma \Rightarrow \Delta$ dann gültig.

Andernfalls enthält der konstruierte Ableitungsbaum ein negatives Blatt, mit einer Beschriftung $\Gamma' \Rightarrow \Delta'$, so dass Γ' und Δ' disjunkte Mengen von Aussagenvariablen sind. Indem man die Aussagenvariablen in Γ' mit wahr, diejenigen in Δ' mit falsch, und alle übrigen beliebig belegt, gewinnt man eine Interpretation welche $\Gamma' \Rightarrow \Delta'$ falsifiziert. Aus Lemma 1.28 folgt dass diese Interpretation auch die Ausgangssequenz $\Gamma \Rightarrow \Delta$ falsifiziert. $\square$

Der Sequenzenkalkül liefert also sogar ein *Entscheidungsverfahren* für die gültigen aussagenlogischen Sequenzen und damit auch für die aussagenlogischen Tautologien. Insbesondere folgt aus Satz 1.32, dass der aussagenlogische Sequenzenkalkül vollständig ist.

Korollar 1.33 (Vollständigkeit des Sequenzenkalküls). *Jede gültige aussagenlogische Sequenz ist im Sequenzenkalkül ableitbar.*

Übung 1.22. Konstruieren Sie Beweise oder falsifizierende Interpretationen für die folgenden Sequenzen:

(a) $(\psi \wedge \neg\varphi), (\psi \rightarrow \varphi), (\vartheta \rightarrow \eta), \psi \Rightarrow \vartheta$

(b) $(X \rightarrow Y) \Rightarrow (Y \rightarrow Z)$

Übung 1.23. Konstruieren Sie Beweise in SK für die folgenden aussagenlogischen Tautologien:

(a) $\neg\neg\psi \rightarrow \psi$

(b) $\psi \rightarrow (\varphi \rightarrow \psi)$

(c) $(\psi \rightarrow \varphi) \rightarrow ((\psi \rightarrow (\varphi \rightarrow \vartheta)) \rightarrow (\psi \rightarrow \vartheta)$

Übung 1.24. Geben Sie Schlussregeln $(\oplus \Rightarrow)$ und $(\Rightarrow \oplus)$ für den Junktor $\oplus$ ("exklusives oder") an. Konstruieren Sie im entsprechend erweiterten Sequenzenkalkül einen Beweis für die Sequenz $(\psi \oplus \varphi) \oplus \vartheta \Rightarrow \psi \oplus (\varphi \oplus \vartheta)$.

Übung 1.25. Modifizieren Sie den Suchalgorithmus für den Sequenzenkalkül zu einem Entscheidungsverfahren für die Erfüllbarkeit aussagenlogischer Formeln, also zu einem Algorithmus, welcher zu jeder gegebenen aussagenlogischen Formel ψ entscheidet, ob ψ erfüllbar ist oder nicht.

Kapitel 2

Strukturen und Homomorphismen

Bemerkung. Mit einem Stern (*) versehene Abschnitte werden in der Vorlesung **nicht** behandelt.

In diesem Kapitel entwickeln wir den Begriff einer mathematischen *Struktur*. Er ist hinreichend allgemein um fast alle in der Mathematik und der Informatik auftretenden Strukturen zu erfassen (z.B. algebraische und geometrische Strukturen, Räume, Datenstrukturen, Datenbanken, Transitionssysteme etc.). Wir behandeln wichtige Beziehungen zwischen Strukturen und werden zahlreiche Beispiele beschreiben. Ausserdem führen wir Abbildungen zwischen Strukturen ein, welche (in unterschiedlichem Masse) *strukturerhaltend* sind, definieren *Kongruenzrelationen* auf Strukturen und *Quotientenstrukturen*.

2.1 Einige Grundbegriffe

Kartesische Produkte. Seien A und B Mengen. Dann ist

$$\begin{aligned} A \times B &:= \{(a,b) : a \in A, b \in B\} \\ A^n &:= \{(a_1, \dots, a_n) : a_i \in A \text{ für } i = 1, \dots, n\} \end{aligned}$$

Insbesondere ist $A^0 = \{\Box\}$, wobei $\Box$ das leere Tupel ist.

Relationen und Funktionen. Eine n-stellige Relation auf einer Menge A ist eine Teilmenge $R \subseteq A^n$. Insbesondere gibt es, unabhängig von der Grundmenge A, genau zwei nullstellige Relationen: $R_0 = \varnothing$ und $R_1 = \{\Box\}$. Nullstellige Relationen heissen auch *Boolsche Relationen* oder *Aussagen*. Dabei wird R_0 mit *falsch* oder 0 identifziert, R_1 mit *wahr* oder 1.

Eine n-stellige Funktion auf A, geschrieben $f : A^n \to A$, ordnet jedem Tupel $\bar{a} \in A^n$ ein Element $f(\bar{a}) \in A$ zu. Nullstellige Funktionen $f : \{\Box\} \to A$ werden also durch den einzigen Funktionswert $f(\Box)$ bestimmt und können daher mit *Konstanten* identifiziert werden. Der *Graph* einer n-stelligen Funktion $f : A^n \to A$ ist die $(n+1)$-stellige Relation

$$G_f := \{(\bar{a}, b) \in A^{n+1} : f(\bar{a}) = b\}.$$

Eigenschaften von Funktionen. Eine Funktion $f : A \to B$ ist

- *injektiv*, wenn für alle $a \neq a'$ aus A auch die Funktionswerte $f(a)$ und $f(a')$ verschieden sind.
- *surjektiv*, wenn es für jedes $b \in B$ ein $a \in A$ gibt, so dass $f(a) = b$.
- *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist.

Mit $\mathbb{N}$ bezeichnen wir die Menge $\{0, 1, 2, \dots\}$ der natürlichen Zahlen.

Mächtigkeit von Mengen. Zwei Mengen A und B heissen *gleichmächtig* (kurz: $|A| = |B|$), wenn es eine bijektive Abbildung von A nach B gibt. A heisst *abzählbar*, wenn es eine surjektive Funktion $f : \mathbb{N} \twoheadrightarrow A$ gibt. A lässt sich dann als $\{f(n) : n \in \mathbb{N}\}$ schreiben.

Lemma 2.1. *Jede abzählbare Menge ist entweder endlich oder gleichmächtig zu* $\mathbb{N}$.

Beweis. Sei A abzählbar und $f : \mathbb{N} \to A$ surjektiv. Wenn A endlich ist, ist nichts zu beweisen. Für unendliches A konstruieren wir eine Bijektion $g : \mathbb{N} \to A$ wie folgt:

$$\begin{aligned} g(0) &:= f(0) \\ g(n+1) &:= f(k) \quad \text{für das kleinste } k \in \mathbb{N} \text{ mit } f(k) \notin \{g(0), \dots, g(n)\}. \end{aligned}$$

Offensichtlich ist g wohldefiniert: Da A unendlich ist, ist $\{g(0), \dots, g(n)\}$ eine echte Teilmenge von A. Also muss es wegen der Surjektivität von f ein k geben mit $f(k) \notin \{g(0), \dots, g(n)\}$, also auch ein kleinstes solches k.

Zweitens ist g surjektiv: Aus der Konstruktion von g folgt sofort, dass zu jedem $k \in \mathbb{N}$ ein $n \leq k$ existiert mit $g(n) = f(k)$. Da f surjektiv ist, ist auch g surjektiv.

Schliesslich ist g injektiv, da nach Definition $g(n+1) \neq g(m)$ für alle $m \leq n$.

Also ist A gleichmächtig zu $\mathbb{N}$. □

Potenzmenge. Sei A eine Menge. Dann ist $Pot(A) := \{B : B \subseteq A\}$ die *Potenzmenge* von A.

Satz 2.2. *Keine Menge ist gleichmächtig zu ihrer Potenzmenge.*

Beweis. Wir zeigen, dass keine Funktion $f : A \to Pot(A)$ surjektiv sein kann. Zu diesem Zweck betrachten wir für ein beliebiges solches f die Menge $B_f := \{a \in A : a \notin f(a)\}$.

Wir behaupten, dass B_f nicht im Bild von f ist. Sonst wäre $f(b) = B_f$ für ein $b \in A$. Dies kann aber nicht sein, da dann

$$b \in f(b) \quad \iff \quad b \in B_f \quad \iff \quad b \notin f(b).$$

(Die erste Äquivalenz folgt da $f(b) = B_f$, die zweite aus der Definition von B_f.) □

Dieser Beweis beruht auf einem *Diagonalisierungsargument*. Wir illustrieren dies am Fall $A = \mathbb{N}$. Wenn $Pot(\mathbb{N})$ abzählbar wäre, dann gäbe es eine Aufzählung $A_0, A_1, \dots$ aller Teilmengen von $\mathbb{N}$, welche wir wie folgt darstellen könnten:

$$\begin{array}{c|ccccc} & 0 & 1 & 2 & 3 & \dots \\ \hline A_0 & 1 & 0 & 0 & 1 & \dots \\ A_1 & 0 & 1 & 0 & 0 & \dots \\ A_2 & 1 & 1 & 0 & 0 & \dots \\ A_3 & 1 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Ein Eintrag 1 (bzw. 0) am Punkt (i, j) soll andeuten, dass $j \in A_i$ (bzw. $j \notin A_i$). Mit Diagonalisierung ist nun gemeint, dass wir die Menge

$$D := \{n \in \mathbb{N} : n \notin A_n\}$$

betrachten (dies entspricht der Menge B_f im soeben geführten Beweis). Wenn die Aufzählung $A_0, A_1, \ldots$ tatsächlich alle Teilmengen von $\mathbb{N}$ erfassen würde, dann wäre $D = A_k$ für ein geeignetes k. Das kann aber nicht sein da $k \in D \;\Leftrightarrow k \notin A_k$.

Wir folgern also, dass $Pot(\mathbb{N})$ überabzählbar ist.

Übung 2.1. Beweisen Sie die folgenden Aussagen.

(a) A ist abzählbar, wenn eine injektive Funktion $f : A \to \mathbb{N}$ existiert.

(b) Wenn A, B abzählbar sind, dann auch $A \cup B$ und $A \times B$.

(c) Jede abzählbare Vereinigung von abzählbaren Mengen ist selbst abzählbar.

(d) Wenn A abzählbar ist, dann auch die Menge

$$A^* := \{w_0 \cdots w_{n-1} : n \in \mathbb{N}, w_i \in A\}$$

aller (endlichen) Wörter über dem Alphabet A.

(e) Die Menge $\{0, 1\}^\omega$ aller unendlichen 0-1 Folgen ist überabzählbar.

2.2 Strukturen

Mathematische Strukturen bestehen aus einem Universum und aus ausgezeichneten Funktionen und Relationen auf diesem Universum. Beispiele sind

- die additive Gruppe der ganzen Zahlen: $(\mathbb{Z}, +, 0)$
- der geordnete Körper der reellen Zahlen: $(\mathbb{R}, +, \cdot, 0, 1, <)$
- Graphen: Die Punkte des Graphen sind das Universum, die zweistellige Relation E beschreibt die Kantenbeziehung.

Die Namen (Symbole) für die in einer Struktur auftretenden Relationen und Funktionen bilden die Signatur der Struktur.

Definition 2.3. Eine *Signatur* τ ist eine Menge von Funktions- und Relationssymbolen. Jedes dieser Symbole hat eine feste endliche Stelligkeit. Formal:

$$\tau := \bigcup_{n \in \mathbb{N}} R^n(\tau) \cup \bigcup_{n \in \mathbb{N}} F^n(\tau)$$

wobei $R^n(\tau)$ eine Menge von n-stelligen Relationssymbolen und $F^n(\tau)$ eine Menge von n-stelligen Funktionssymbolen ist. (Alle diese Mengen können auch leer sein.)

Eine Signatur heisst *relational*, wenn sie nur Relationssymbole enthält (d.h. $F^n(\tau) = \varnothing$ für alle $n \in \mathbb{N}$), bzw. *funktional* oder *algebraisch*, wenn sie ausschliesslich Funktionssymbole enthält. Nullstellige Funktionssymbole heissen auch *Konstantensymbole*.

Andere Bezeichnungen für eine Signatur sind *Symbolmenge* oder *Vokabular*.

Beispiele. (1) Die Signatur der Arithmetik ist $\tau_{ar} = \{+, \cdot, 0, 1\}$, wobei $+$ und $\cdot$ zweistellige Funktionsymbole, 0 und 1 Konstantensymbole sind.

(2) Die Signatur der geordneten Arithmetik ist $\tau_{ar}^{<} = \{+, \cdot, 0, 1, <\}$. Sie erweitert τ_{ar} um das zweistellige Relationssymbol $<$.

(3) Die Signatur von Graphen $\tau_G = \{E\}$, wobei E ein zweistelliges Relationssymbol ist.

Notation. Normalerweise verwenden wir

- $P, Q, R, \ldots, P_i, \ldots$ für Relationssymbole,
- $f, g, h, \ldots, f_i, \ldots$ für Funktionssymbole,
- $c, d, e, \ldots, c_i, \ldots$ für Konstantensymbole,
- σ, τ für Signaturen.

Relations- und Funktionssymbole in einer Signatur τ können natürlich in vielfältiger Weise durch konkrete Relationen und Funktionen interpretiert werden. Allgemein wird eine Struktur festgelegt durch Angabe ihres Universums und der Interpretation der Relations- und Funktionssmbole über diesem Universum.

Definition 2.4. Eine τ-*Struktur* $\mathfrak{A}$ besteht aus

(1) einer nichtleeren Menge A, dem *Universum* (oder *Träger*) von $\mathfrak{A}$,

(2) einer Interpretationsfunktion welche jedem Relationssymbol $P \in R^n(\tau)$ eine Relation $P^{\mathfrak{A}} \subseteq A^n$ und jedem Funktionssymbol $f \in F^n(\tau)$ eine Funktion $f^{\mathfrak{A}} : A^n \to A$ zuordnet.

Eine Struktur mit funktionaler Signatur τ heisst auch eine τ-*Algebra*.

Notation. Strukturen bezeichnen wir meist mit gotischen Buchstaben $\mathfrak{A}, \mathfrak{B}\, \mathfrak{C}, \ldots$, der entsprechende lateinische Buchstabe $A, B, C, \ldots$ steht für das Universum der Struktur. Mit $\mathfrak{A} = (A, P_1^{\mathfrak{A}}, P_2^{\mathfrak{A}}, \ldots, f_1^{\mathfrak{A}}, f_2^{\mathfrak{A}}, \ldots)$ bezeichnen wir also eine Struktur der Signatur $\tau = \{P_1, P_2, \ldots, f_1, f_2 \ldots\}$ mit Universum A.

Beachte. Es ist wichtig zwischen Relations- und Funktions*symbolen* R_i, f_j und ihrer Interpretation durch konkrete Relationen $R_i^{\mathfrak{A}}$ bzw. Funktionen $f_j^{\mathfrak{A}}$ zu unterscheiden.

Wir werden eine Reihe von Beispielen im nächsten Abschnitt diskutieren. Zuvor beschreiben wir zwei grundlegende Möglichkeiten, wie eine Struktur in einer andern enthalten sein kann.

Definition 2.5. $\mathfrak{A}, \mathfrak{B}$ seien τ-Strukturen. $\mathfrak{A}$ ist *Substruktur* von $\mathfrak{B}$, (kurz: $\mathfrak{A} \subseteq \mathfrak{B}$), wenn

(1) $A \subseteq B$,

(2) für alle $n \in \mathbb{N}$, $R \in R^n(\tau)$ gilt: $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$,

(3) für alle $n \in \mathbb{N}$, $f \in F^n(\tau)$ gilt $f^{\mathfrak{A}} = f^{\mathfrak{B}}|_A$, d.h. $f^{\mathfrak{A}}$ ist die *Restriktion* von $f^{\mathfrak{B}}$ auf A.

Wenn $\mathfrak{A}$ Substruktur von $\mathfrak{B}$, so heisst $\mathfrak{B}$ *Erweiterung* von $\mathfrak{A}$.

Ist $\mathfrak{A}$ eine Substruktur der τ-Struktur $\mathfrak{B}$, so ist A *τ-abgeschlossen*, d.h., für alle $f \in F^n(\tau)$ und alle $a_1, \ldots, a_n \in A$ ist $f^{\mathfrak{B}}(a_1, \ldots, a_n) \in A$. Umgekehrt gilt auch: Sei $\mathfrak{B}$ eine τ-Struktur. Zu jeder nicht-leeren, τ-abgeschlossenen Teilmenge $A \subseteq B$ gibt es genau eine Substruktur von $\mathfrak{B}$ mit Träger A. Wir nennen sie die *von A in $\mathfrak{B}$ induzierte Substruktur.*

Beispiel. $2\mathbb{N} := \{2n : n \in \mathbb{N}\}$ ist $\{+\}$-abgeschlossen. Also ist $(2\mathbb{N}, +) \subseteq (\mathbb{N}, +)$. Hingegen ist $2\mathbb{N}+1 := \{2n+1 : n \in \mathbb{N}\}$ nicht $\{+\}$-abgeschlossen und kann somit nicht Träger einer Substruktur von $(\mathbb{N}, +)$ sein.

Während beim Begriffspaar Substruktur/Erweiterung die Signatur fest bleibt und das Universum verändert wird, ist dies beim Begriffspaar Redukt/Expansion genau umgekehrt.

Definition 2.6. Seien $\sigma \subseteq \tau$ Signaturen, und sei $\mathfrak{B}$ eine τ-Struktur. Das *σ-Redukt* $\mathfrak{B} \upharpoonright \sigma$ von $\mathfrak{B}$ ist die σ-Struktur, die wir aus $\mathfrak{B}$ erhalten, wenn wir die Relationen und Funktionen in $\tau - \sigma$ einfach weglassen. Ist $\mathfrak{A}$ Redukt einer τ-Struktur $\mathfrak{B}$, so nennen wir $\mathfrak{B}$ eine *τ-Expansion* von $\mathfrak{A}$.

Beispiel. Die additive Gruppe der reellen Zahlen $(\mathbb{R}, +, 0)$ ist das $\{+, 0\}$-Redukt des Körpers der reellen Zahlen $(\mathbb{R}, +, \cdot, 0, 1)$.

2.3 Ein Zoo von Strukturen

(1) **Mengen.** Sei $\tau = \varnothing$. Die $\varnothing$-Struktur mit Universum A ist einfach die Menge A.

(2) **Graphen.** Die Signatur von Graphen ist $\tau_G = \{E\}$, E ein binäres Relationssymbol. Ein *ungerichteter Graph* ist eine τ_G-Struktur $G = (V, E^G)$ mit Punktmenge V (dem Universum von G) und einer Relation $E^G \subseteq V \times V$, welche folgende Bedingungen erfüllt:

keine Schlingen: Für alle $v \in V$ gilt: $(v, v) \notin E^G$.

Symmetrie: Für alle $u, v \in V$ gilt: wenn $(u, v) \in E^G$, dann auch $(v, u) \in E^G$.

Wenn nur die erste Bedingung gefordert wird, sprechen wir von *gerichteten Graphen.*

(3) **Lineare und partielle Ordnungen.** Eine partielle Ordnung ist eine $\{<\}$-Struktur $(A, <)$ welche folgende Bedingungen erfüllt:

Irreflexivität: Für kein $a \in A$ gilt $a < a$.

Transitivität: Wenn $a < b$ und $b < c$, dann auch $a < c$.

Daraus folgt insbesondere auch, dass $<$ *antisymmetrisch* ist: Wenn $a < b$, dann *nicht* $b < a$.

Eine *lineare* oder *totale* Ordnung erfüllt als zusätzliche Bedingung:

Vergleichbarkeit: Für alle a, b gilt entweder $a < b$ oder $a = b$ oder $b < a$.

Offensichtlich sind $(\mathbb{N},<)$ und $(\mathbb{R},<)$ (mit der üblichen Interpretation von $<$) lineare Ordnungen. Für jede Menge A ist $(\mathcal{P}(A),\subset)$ eine partielle Ordnung, für $|A|>1$ aber keine lineare Ordnung.

Eine lineare Ordnung ist *dicht*, wenn zu zwei beliebigen Elementen $a<b$ immer ein c existiert mit $a<c<b$. Eine *Wohlordnung* ist eine lineare Ordnung $(A,<)$ ohne unendliche absteigende Ketten: Es gibt keine unendliche Folge $a_0, a_1, a_2, \ldots$ in A so dass $a_{i+1} < a_i$ für alle $i \in \mathbb{N}$. Zum Beispiel ist $(\mathbb{N},<)$ eine Wohlordnung während $(\mathbb{Z},<)$ oder $(\mathbb{Q}^+,<)$ keine Wohlordnungen sind.

(4) **Wortstrukturen.** Sei Γ ein Alphabet (d.h. eine beliebige, in der Regel abzählbare, Menge von Symbolen). Ein *Wort* über Γ ist eine endliche Folge $w = w_0 \cdots w_{n-1}$ von Symbolen aus Γ. Jedem solchen Wort w ordnen wir eine Struktur $\mathfrak{B}(w)$ der Signatur $\{<\} \cup \{P_a : a \in \Gamma\}$ zu, mit einstelligen Relationssymbolen P_a. Das Universum von $\mathfrak{B}(w)$ ist die Menge $\{0, \ldots, n-1\}$ der Positionen an denen Symbole stehen, $<$ ist die übliche Ordnung auf dieser Menge und $P_a := \{i < n : w_i = a\}$ ist die Menge der Positionen an denen im Wort w das Symbol a steht. Das Wort $w = abbcab$ über dem Alphabet $\{a,b,c\}$ wird also durch die Wortstruktur

$$\mathfrak{B}(w) = (\{0,1,2,3,4,5\}, <, P_a, P_b, P_c)$$

repräsentiert, mit $P_a = \{0,4\}$, $P_b = \{1,2,5\}$ und $P_c = \{3\}$.

(5) **Transitionssysteme.** Ein Transitionssystem besteht aus einer Menge S von *Zuständen*, und aus einer Menge A von *Aktionen* oder *Programmen*, welche Zustände in neue Zustände überführen. Zusätzlich hat man in der Regel eine Menge B von Eigenschaften, welche die Zustände haben oder nicht haben können. Ein solches Transitionssystem wird beschrieben durch eine Struktur mit Universum S, einer Menge $\{P_b : b \in B\}$ von monadischen (d.h. einstelligen) Relationen und einer Menge $\{E_a : a \in A\}$ von binären Relationen auf S. Dabei soll P_b die Menge der Zustände mit der Eigenschaft b sein, und die Relation E_a soll auf ein Paar (s,t) von Zuständen zutreffen, genau dann, wenn das Programm a den Zustand s in den Zustand t überführt.

Eine wichtige Methode zur Verifikation paralleler Systeme besteht darin, diese als Transitionssysteme zu modellieren und Bedingungen wie Fairness, Sicherheit, Deadlock-Freiheit etc. in einer geeigneten logischen Sprache zu formulieren und auf dem Transitionssystem auszuwerten. Formale Spezifikation und Verifikation solcher Systeme ist eine der wichtigsten Anwendungen der Logik in der Informatik.

(6) **Relationale Datenbanken.** Eine relationale Datenbank ist, informell gesprochen, eine endliche Kollektion von endlichen Tabellen, welche sich zeitlich verändern. Jede Zeile in einer solchen Tabelle R ist ein Tupel $(a_1, \ldots, a_n) \in D_1 \times \cdots \times D_n$ wobei $D_1, \ldots, D_n$ die den einzelnen Spalten (im Datenbank-Jargon: den Attributen) zugeordneten Domains sind (z.B. Integers, Strings, ...). Sei D die Vereinigung aller in der Datenbank vorkommenden Domains. Die Tabelle R kann dann als eine n-stellige Relation über D aufgefasst werden: $R \subseteq D^n$.

Ein aktueller Zustand der Datenbank ist also eine endliche Kollektion von endlichen Relationen $R_1, \ldots, R_m$ über dem (in der Regel unendlichen) Universum D. Dies entspricht der Struktur $\mathfrak{D} = (D, R_1, \ldots, R_m)$.

Für viele Zwecke ist aber diese Formalisierung problematisch: Elementare Operationen wie die Bildung des Komplements einer Relation führen zu unendlichen Relationen. Daher ist eine Formalisierung durch eine *endliche* Struktur oft zweckmässiger. Anstelle des unendlichen Universums D betrachte man den *aktiven Domain* $\mathrm{ad}(\mathfrak{D})$, welcher aus all denjenigen Objekten besteht, die in einer der Relationen $R_1, \dots, R_m$ vorkommen, also

$$\begin{aligned}\mathrm{ad}(\mathfrak{D}) := \{a \in D :\ & \text{es gibt ein } R_i \text{ und ein Tupel } (b_1, \dots, b_r) \in R_i \\ & \text{so dass } b_j = a \text{ für ein } j \leq r\}.\end{aligned}$$

Da alle Relationen R_i endlich sind, ist auch $\mathrm{ad}(\mathfrak{D})$ endlich und die endliche Substruktur $(\mathrm{ad}(\mathfrak{D}), R_1, \dots, R_m)$ von $\mathfrak{D}$ ist eine adäquate endliche Formalisierung des Datenbank-Zustandes.

Anfragen an eine Datenbank entsprechen dem Auswerten logischer Formeln auf (endlichen) Strukturen. Es bestehen daher enge Verbindungen zwischen der Mathematischen Logik und der Theorie relationaler Datenbanken.

(7) **Arithmetische Strukturen.** Die Signatur der Arithmetik ist $\tau_{ar} = \{+, \cdot, 0, 1\}$, die Signatur der geordneten Arithmetik $\tau_{ar}^< = \tau_{ar} \cup \{<\}$, wobei wir annehmen, dass die Symbole $+, \cdot, 0, 1, <$ in der üblichen Weise interpretiert werden. Trotzdem gibt es natürlich ganz verschiedene arithmetische Strukturen, z.B.:

- $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$, die *Standard-Arithmetik* der natürlichen Zahlen. Die *geordnete Standard-Arithmetik* ist $\mathfrak{N}^< = (\mathbb{N}, +, \cdot, 0, 1, <)$. Sie ist eine Expansion von $\mathfrak{N}$.
- Beliebige *Ringe*, insbesondere der Ring $\mathfrak{Z} = (\mathbb{Z}, +, \cdot, 0, 1)$ der ganzen Zahlen. Offensichtlich ist $\mathfrak{Z}$ eine Erweiterung der Standard-Arithmetik $\mathfrak{N}$.
- Beliebige *Körper*, etwa den Körper $\mathfrak{R} = (\mathbb{R}, +, \cdot, 0, 1)$ der reellen Zahlen, den Körper $\mathfrak{Q} = (\mathbb{Q}, +, \cdot, 0, 1)$ der rationalen Zahlen oder endliche Körper.
- Die Standard-Arithmetik $\mathfrak{N}$ lässt sich durch Hinzunahme von 'unendlichen Elementen' zu neuen arithmetischen Strukturen erweitern. Die einfachste Variante ist $(\mathbb{N} \cup \{\infty\}, +, \cdot, 0, 1)$ mit

  $$a + \infty = \infty + a = a \cdot \infty = \infty \cdot a = \infty$$

  für alle $a \in \mathbb{N} \cup \{\infty\}$. Wir werden später sehen, dass es auch sogenannte *Nicht-Standard-Arithmetiken* gibt welche in gewissem Sinn äquivalent zur Standard-Arithmetik sind (weil sie genau die gleichen prädikatenlogischen Sätze erfüllen).

(8) **Boolsche Algebren.** Sei A eine beliebige Menge. Die boolsche Algebra über A ist $\mathrm{BA}(A) = (\mathcal{P}(A), \cup, \cap, ^-, \varnothing, A)$, wobei $\cup, \cap, ^-$ Vereinigung, Durchschnitt und Komplement in A bedeuten.

(9) **Gruppen.** Wie können Gruppen (im Sinne der Algebra) durch Strukturen gemäss Definition 2.4 formalisiert werden? Dafür gibt es mehrere Möglichkeiten, abhängig davon, welche in Gruppen vorkommenden Funktionen und Relationen explizit (d.h.

in der Signatur) vorkommen sollen. Mit den üblichen Bezeichnungen $\circ$ für die Gruppenoperation, e für das neutrale Element, g^{-1} für das zu g inverse Element ergeben sich sofort die Möglichkeiten

(i) $\mathfrak{G} = (G, \circ)$.

(ii) $\mathfrak{G} = (G, \circ, e)$.

(iii) $\mathfrak{G} = (G, \circ, e, \ ^{-1})$.

Die Wahl der Signatur ist abhängig von der jeweiligen Absicht: Will man eine möglichst minimale Formalisierung wird man *(i)* oder *(ii)* wählen, da die Gruppe dadurch bereits eindeutig festgelegt ist. Andererseits gibt es algebraische Überlegungen welche die dritte Möglichkeit nahelegen: Wenn die Funktion $^{-1}$ hinzugenommen wird, sind die Substrukturen von $\mathfrak{G}$ genau die Untergruppen. Dies ist nicht der Fall bei den beiden ersten Formalisierungen. So ist etwa $(\mathbb{N}, +, 0)$ eine Substruktur von $(\mathbb{Z}, +, 0)$ (der additiven Gruppe der ganzen Zahlen), aber offensichtlich keine Untergruppe.

In der Praxis sind oft noch ganz andere Operationen wesentlich, etwa die Multiplikation mit erzeugenden Elementen der Gruppe.

(10) **Vektorräume.** Zum Abschluss diskutieren wir das Problem der Formalisierung von Vektorräumen. Interessant ist dies deshalb, weil hier Objekte verschiedener Art auftreten: Vektoren und Skalare.

Sei etwa V ein Vektorraum über dem Körper K. Man kann eine Formalisierung wählen, in der das Universum ausschliesslich aus den Vektoren besteht, und die Elemente des Grundkörpers als Operationen auf dem Universum in Erscheinung treten. Dem Vektorraum entspricht dann die algebraische Struktur $(V, +, 0, (f_k)_{k \in K})$ mit $f_k(v) := kv$ (Multiplikation mit Skalar k). Für algebraische Überlegungen ist dies bei festem Grundkörper K die geeignete Formalisierung, da die Substrukturen genau den linearen Unterräumen entsprechen (Abgeschlossenheit unter Addition und unter Multiplikation mit Skalaren). Wenn wir im folgenden über Vektorräume sprechen, ist meistens diese Formalisierung gemeint. Eine andere Möglichkeit wird im nächsten Abschnitt diskutiert.

2.4* Mehrsortige Strukturen

Viele in der Praxis auftretende Strukturen beziehen sich auf Objekte verschiedener Art. Ein naheliegendes Beispiel aus der Mathematik sind Vektorräume, in welchen Vektoren und Skalare eine Rolle spielen. Ein für die Informatik wichtiges Beispiel sind Datenbanken, deren Relationen in der Regel Elemente verschiedenen Typs (z.B. natürliche Zahlen, Strings etc.) miteinander in Beziehung setzen. Oft werden solche Strukturen *mehrsortig* modelliert, unter Verwendung eines verallgemeinerten Strukturbegriffs bei dem das Universum aus verschiedenen Sorten bestehen kann, und die Funktionen 'getypt' sind.

Definition 2.7. Eine *mehrsortige Signatur* ist ein Tupel $\tau = (S, \mathcal{R}, \mathcal{F})$ bestehend aus

(1) einer nicht-leeren Menge S, deren Elemente *Sorten* genannt werden;

(2) einer Menge $\mathcal{R}$ von Relationssymbolen mit *Typdeklarationen* $R : (s_1 \times \cdots \times s_n)$ wobei $n \in \mathbb{N}$ und $s_1, \ldots, s_n \in S$;

(3) einer Menge $\mathcal{F}$ von Funktionssymbolen, mit *Typdeklarationen* $f : s_1 \times \cdots \times s_n \to s$ wobei $n \in \mathbb{N}$ und $s_1, \ldots, s_n, s \in S$.

Eine *mehrsortige Struktur* der Signatur $\tau = (S, \mathcal{R}, \mathcal{F})$ ist ein Tupel

$$\mathfrak{A} = ((A_s)_{s \in S}; (R^{\mathfrak{A}})_{R \in \mathcal{R}}; (f^{\mathfrak{A}})_{f \in \mathcal{F}})$$

mit folgenden Eigenschaften:

(a) Für jede Sorte $s \in S$ ist eine Menge A_s gegeben, genannt das *Universum der Sorte s*.

(b) Jedes Relationssymbol $r \in \mathcal{R}$ mit Typdeklaration $R : (s_1 \times \cdots \times s_n)$ ist interpretiert durch eine Relation $R^{\mathfrak{A}} \subseteq A_{s_1} \times \cdots \times A_{s_n}$.

(c) Jedes Funktionssymbol $f \in \mathcal{F}$ mit Typdeklaration $f : s_1 \times \cdots \times s_n \to s$ ist interpretiert durch eine Funktion $f^{\mathfrak{A}} : A_{s_1} \times \cdots \times A_{s_n} \to A_s$.

Beispiele. (1) **Vektorräume.** Man kann Vektorräume auch als zwei-sortige Strukturen

$$(V, K; +_V, 0_V, +_K, *_K, 0_K, 1_K, *_{KV})$$

formalisieren, mit den Sorten V und K, und den folgenden Typdeklarationen der Funktionen:

$$\begin{aligned}
+_V &: V \times V \to V \\
0_V &: \ \to V \\
+_K &: K \times K \to K \\
*_K &: K \times K \to K \\
0_K &: \ \to K \\
1_K &: \ \to K \\
*_{KV} &: K \times V \to V
\end{aligned}$$

Ein Vorteil dieser Formalisierung gegenüber der oben beschrieben ist, dass die Signatur hier endlich und unabhängig vom Grundkörper ist.

(2) **Graphen als Inzidenzstrukturen.** Sei G ein gerichteter Graph mit Knotenmenge V und Kantenmenge $E \subseteq V \times V$. Anstelle der üblichen Modellierung von G als Struktur mit Universum V und zweistelliger Relation E betrachtet man gelegentlich auch die zwei-sortige Struktur $(V, E; \mathit{Source}, \mathit{Sink})$ wobei das Universum aus den Knoten und den Kanten besteht, deren Zusammenhang durch die Inzidenzrelationen

$$\begin{aligned}
\mathit{Source} &:= \{(v, e) \in V \times E : v \text{ ist Anfangspunkt der Kante } e\} \\
\mathit{Sink} &:= \{(v, e) \in V \times E : v \text{ ist Endpunkt der Kante } e\}
\end{aligned}$$

gegeben ist.

(3) **Datenstrukturen: Stacks.** Stacks können durch algebraische zweisortige Strukturen beschrieben werden deren Signatur aus den Sorten s (Symbole) und w (Wörter) und den Funktionen mit den Typdeklarationen $\lambda :\to w$, $\mathit{push} : s \times w \to w$, $\mathit{pop} : w \to w$ und $\mathit{top} : w \to s$ besteht. Das einzige Problem ist die Definition der *top*-Funktion auf dem leeren Stack. Um

die Einführung nur partiell definierter Funktionen zu vermeiden, fügen wir zu den Universen eine spezielle Konstante *undef* hinzu. Stacks über einem Alphabet Σ entsprechen dann der Struktur mit Universen $A_s = \Sigma \cup \{undef\}$ und $A_w = \Sigma^* \cup \{undef\}$, der Konstante λ für das leere Wort und den folgenden Definitionen der Funktionen *push*, *pop* und *top*.

$$push(\sigma, x) := \begin{cases} \sigma x & \text{wenn } \sigma \in \Sigma, x \in \Sigma^* \\ undef & \text{wenn } \sigma = undef \text{ oder } x = undef \end{cases}$$

$$pop(x) := \begin{cases} x' & \text{wenn } x = \sigma x' \\ \lambda & \text{wenn } x = \lambda \\ undef & \text{wenn } x = undef \end{cases}$$

$$top(x) := \begin{cases} \sigma & \text{wenn } x = \sigma x' \\ undef & \text{sonst} \end{cases}$$

Mehrsortige Strukturen sind für praktische Modellierungsaufgaben nützlich. Für die Entwicklung der Logik als mathematische Disziplin spielen sie aber kaum eine Rolle, da eigentlich alle wesentlichen Fragestellungen unmittelbar auf einsortige (relationale) Strukturen zurückgespielt werden können. Zu diesem Zweck kann man zunächst jede Funktion $f : A_{s_1} \times \cdots \times A_{s_n} \to A_s$ durch ihren Graphen $G_f \subseteq A_{s_1} \times \cdots \times A_{s_n} \times A_s$ ersetzen und damit die Betrachtung auf mehrsortige relationale Strukturen $\mathfrak{A} = ((A_s)_{s\in S}; (R^{\mathfrak{A}})_{R\in\mathcal{R}})$ beschränken. Man geht dann zum Universum $A := \bigcup_{s\in S} A_s$ über und fasst das Universum A_s einer Sorte s als einstellige Relation auf A auf. Anstelle der gegebenen mehrsortigen Struktur arbeitet man dann mit der einsortigen Struktur $\mathfrak{A}' = (A, (A_s)_{s\in S}, (R^{\mathfrak{A}})_{R\in\mathcal{R}})$.

Übung 2.2. Modellieren Sie **Queues** als mehrsortige Struktur (analog zu Stacks).

Übung 2.3. Modellieren Sie eine beliebige relationale Struktur $\mathfrak{A} = (A, R_1, \ldots, R_k)$ durch eine mehrsortige Inzidenzstruktur.

2.5 Homomorphismen und Isomorphismen

Homomorphismen sind *strukturerhaltende Abbildungen*.

Definition 2.8. $\mathfrak{A}$ und $\mathfrak{B}$ seien τ-Strukturen. Eine Abbildung $\pi : A \to B$ ist ein *Homomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$, wenn folgende Bedingungen erfüllt sind:

(1) Für jedes Relationssymbol $R \in R^n(\tau)$ und alle $a_1, \ldots, a_n \in A$ gilt

$$(a_1, \ldots, a_n) \in R^{\mathfrak{A}} \;\Rightarrow\; (\pi a_1, \ldots, \pi a_n) \in R^{\mathfrak{B}}.$$

(2) Für jedes Funktionssymbol $f \in F^n(\tau)$ und alle $a_1, \ldots, a_n \in A$ gilt

$$\pi f^{\mathfrak{A}}(a_1, \ldots, a_n) = f^{\mathfrak{B}}(\pi a_1, \ldots, \pi a_n).$$

Bemerkung. Für jedes $n \in \mathbb{N}$ lässt sich π auf natürliche Weise zu einer Abbildung $\pi : A^n \to B^n$ erweitern, mit $\pi(a_1, \ldots, a_n) := (\pi a_1, \ldots, \pi a_n)$. Bedingung (1) können wir dann auch so formulieren: für alle Relationssymbole $R \in \tau$ ist $\pi(R^{\mathfrak{A}}) \subseteq R^{\mathfrak{B}}$. Bedingung (2) bedeutet, dass für alle Funktionssymbole $f \in \tau$ gilt: $\pi \circ f^{\mathfrak{A}} = f^{\mathfrak{B}} \circ \pi$.

$$\begin{tikzcd} A^n \arrow[r, "\pi"] \arrow[d, "f^{\mathfrak{A}}"] & B^n \arrow[d, "f^{\mathfrak{B}}"] \\ A \arrow[r, "\pi"] & B \end{tikzcd}$$

Für nullstellige Funktionssymbole c besagt Bedingung (2), dass $\pi c^{\mathfrak{A}} = c^{\mathfrak{B}}$.

Definition 2.9. Ein *starker Homomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ ist ein Homomorphismus $\pi : \mathfrak{A} \to \mathfrak{B}$, welcher die folgende, stärkere Version von (1) erfüllt:

(1)′ Für jedes Relationssymbol $R \in R^n(\tau)$ und alle $\bar{a} \in A^n$ gilt:

$$\bar{a} \in R^{\mathfrak{A}} \iff \pi\bar{a} \in R^{\mathfrak{B}}.$$

Bemerkung. Die Bedingung (1)′ ist äquivalent zur Forderung, dass für alle Relationssymbole $R \in \tau$ gilt: $\pi(R^{\mathfrak{A}}) = R^{\mathfrak{B}} \cap \pi(A^n)$.

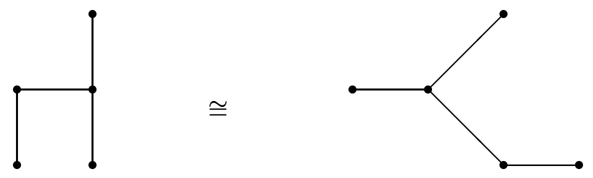
Definition 2.10. Eine *Einbettung* von $\mathfrak{A}$ in $\mathfrak{B}$ in ein injektiver starker Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$. Ein *Isomorphismus* ist ein bijektiver, starker Homomorphismus (also eine surjektive Einbettung). Zwei τ-Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ sind *isomorph* (kurz: $\mathfrak{A} \cong \mathfrak{B}$), wenn ein Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ existiert. Ein Isomorphismus $\pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{A}$ heisst *Automorphismus* von $\mathfrak{A}$.

Notation. Wir schreiben $\pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$ um anzudeuten, dass π ein Isomorphismus ist, und $\pi : \mathfrak{A} \hookrightarrow \mathfrak{B}$, wenn π eine Einbettung ist. Die Identitätsabbildung auf $\mathfrak{A}$ bezeichnen wir mit $1_{\mathfrak{A}}$.

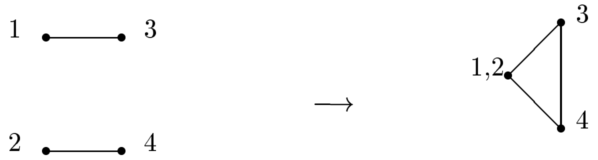
Die Menge aller Automorphismen einer Struktur $\mathfrak{A}$ bilden bzgl. Hintereinanderausführen eine Gruppe mit neutralem Element $1_{\mathfrak{A}}$. Wir nennen sie die *Automorphismengruppe* oder *Symmetriegruppe* von $\mathfrak{A}$ und bezeichnen sie mit $\mathrm{Aut}(\mathfrak{A})$. Eine Struktur $\mathfrak{A}$ ist *starr*, wenn $\mathrm{Aut}(\mathfrak{A}) = \{1_{\mathfrak{A}}\}$, d.h. wenn nur der triviale Automorphismus existiert.

Beispiele. (1) Unter der in Abschnitt 2.3 (10) zugrundegelegten Formalisierung von Vektorräumen sind die Homomorphismen zwischen Vektorräumen genau die linearen Abbildungen.

(2) $G = (V, E^G), H = (U, E^H)$ seien Graphen. $G \cong H$ falls es eine bijektive Abbildung $\pi : V \to U$ gibt, so dass $(v, v') \in E^G \Leftrightarrow (\pi v, \pi v') \in E^H$.



(3) Demgegenüber ist für einen Homorphismus $\pi : G \to H$ nicht gefordert, dass π bijektiv ist, und es muss nur die schwächere Bedingung $(v, v') \in E^G \implies (\pi v, \pi v') \in E^H$ erfüllt sein. Die folgende Abbildung ist ein Homomorphismus.



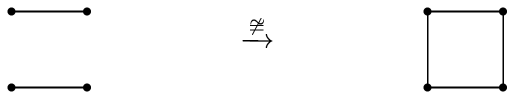
(4) Mit K_n bezeichnet man den vollständigen Graphen mit n Punkten, d.h. $K_n = (\{1, \dots, n\}, E)$ mit $E = \{(i, j) : i \neq j\}$. Offensichtlich ist jede Permutation von $\{1, \dots, n\}$ ein Automorphismus von K_n, d.h. $\mathrm{Aut}(K_n) = S_n$ (mit S_n bezeichnet man die Permutationsgruppe auf n Elementen).

Die Automorphismengruppe von $(\mathbb{Z}, <)$ ist $(\mathbb{Z}, +, 0)$, denn die Automorphismen von $(\mathbb{Z}, <)$ sind gerade die Translationen $x \mapsto x + a$ für $a \in \mathbb{Z}$. Hingegen ist $(\mathbb{N}, <)$ starr.

(5) Gemäss dem mittelalterlichen Scholastiker Thomas von Aquin (1225 – 1274) ist **Gott** eine Struktur mit drei Elementen *pater*, *filius* und *spiritus sanctus* und einer asymmetrischen binären Relation R^{Gott} (relatio originis). Thomas von Aquin schreibt zudem, dass die drei Elemente mit Hilfe von R^{Gott} eindeutig identifizierbar sind. Er folgert: Wenn (*pater*, *filius*) $\in R^{\text{Gott}}$ und (*pater*, *spiritus sanctus*) $\in R^{\text{Gott}}$, dann gehört genau eines der Paare (*filius*, *spiritus sanctus*) und (*spiritus sanctus*, *filius*) zu R^{Gott}.

Wieso? Da R^{Gott} asymmetrisch ist können nicht beide Paare in R^{Gott} sein. Aus dem selben Grund folgt, dass (*filius*, *pater*) $\notin R^{\text{Gott}}$ und (*spiritus sanctus*, *pater*) $\notin R^{\text{Gott}}$. Wenn jetzt keines der Paare (*filius*, *spiritus sanctus*) und (*spiritus sanctus*, *filius*) zu R^{Gott} gehören würde, dann wäre das Vertauschen von *filius* und *spiritus sanctus* ein Automorphismus von **Gott**, und daher nicht alle drei Elemente eindeutig identifizierbar.

(6) Für funktionale Signaturen ist Bedingung (1) der Homomorphismus-Definition leer. Daher ist jeder bijektive Algebren-Homomorphismus bereits ein Isomorphismus. Für Strukturen mit Relationssymbolen dagegen gilt dies nicht.



Übung 2.4. Zeigen Sie, dass ein ungerichteter Graph G genau dann m-färbbar ist (siehe Übung 1.18). wenn, ein Homomorphismus von G nach K_m (dem vollständigen Graphen mit m Knoten) existiert.

2.6* Kongruenzrelationen und Quotientenstrukturen

Definition 2.11. Eine binäre Relation $E \subseteq A \times A$ ist eine *Äquivalenzrelation* auf A, falls sie folgende Bedingungen erfüllt:

Reflexivität. Für alle $a \in A$ ist $(a, a) \in E$.

Symmetrie. Für alle $a, b \in A$ gilt: $(a, b) \in E \Rightarrow (b, a) \in E$.

Transitivität. Für alle $a, b, c \in A$ gilt: Wenn $(a, b) \in E$ und $(b, c) \in E$ dann auch $(a, c) \in E$.

Ist E eine Äquivalenzrelation auf A, so heisst (A, E) *Äquivalenzstruktur*.

Beispiele. (1) $(\mathbb{Z}, E_5)$ mit $E_5 := \{(a,b) : b - a$ ist durch 5 teilbar $\}$ ist eine Äquivalenzstruktur.

(2) $(\mathbb{N}, \mathrm{TF})$ mit $\mathrm{TF} := \{(a,b) : a, b$ sind teilerfremd$\}$ ist *keine* Äquivalenzrelation, da TF nicht transitiv ist (z.B. sind $(3,5)$ und $(5,9)$ teilerfremd, nicht aber $(3,9)$).

Sei E eine Äquivalenzrelation auf A. Dann ist

$$[a]_E := \{b : (a,b) \in E\}$$

die *Äquivalenzklasse* von a bezüglich E. Offensichtlich ist $[a]_E = [b]_E$ genau dann wenn $(a,b) \in E$. Wir sagen in diesem Fall, dass a und b *Repräsentanten* derselben Äquivalenzklasse sind. (Wenn E aus dem Kontext ersichtlich ist, lassen wir den Index E meist weg und schreiben $[a], [b], \ldots$, anstelle von $[a]_E, [b]_E, \ldots$) Eine Äquivalenzrelation auf A induziert also eine *Zerlegung* von A *in Äquivalenzklassen.*

Äquivalenzrelationen werden oft durch das Symbol $\sim$ (mit Infixnotation) bezeinet. Es ist eine weitverbreitete Technik in der Mathematik, in geeignetem Sinn äquivalente Objekte einer Menge A zu identifizieren, und zur Menge $A/_\sim$ überzugehen, deren Elemente die Äquivalenzklassen von A sind. So wird etwa $\mathbb{Z}$ durch die soeben beschriebene Äquivalenzrelation E_5 in fünf Äquivalenzklassen (Restklassen) zerlegt, und wir erhalten die Restklassenmenge $\mathbb{Z}_5 := \{[0], [1], [2], [3], [4]\}$.

Können wir auch auf einer allgemeinen τ-Struktur $\mathfrak{A}$ eine Äquivalenzrelation $\sim$ herausfaktorisieren und eine *Faktorstruktur* $\mathfrak{A}/_\sim$ (derselben Signatur) definieren? In der Tat ist dies möglich. Dazu reicht es aber nicht, dass $\sim$ eine Äquivalenzrelation auf A ist. Es ist zusätzlich erforderlich, dass $\sim$ mit den Funktionen und Relationen von $\mathfrak{A}$ *kompatibel* (verträglich) ist. Zum Beispiel ist E_5 auf $(\mathbb{Z}, +)$ mit der Addition verträglich, da folgendes gilt: Wenn $(a,b) \in E_5$ und $(c,d) \in E_5$, dann auch $(a+c, b+d) \in E_5$. Hingegen ist E_5 nicht kompatibel mit $<$ (da z.B. einerseits $2 < 7$, andererseits aber $[2] = [7]$).

Definition 2.12. Sei $\mathfrak{A}$ eine τ-Struktur. Eine *Kongruenzrelation* auf $\mathfrak{A}$ ist eine Äquivalenzrelation $\sim$ auf dem Universum A von $\mathfrak{A}$, welche in folgendem Sinn mit den Relationen und Funktionen von $\mathfrak{A}$ kompatibel ist.

(1) Für jede n-stellige Funktion $f^{\mathfrak{A}}$ von $\mathfrak{A}$ und alle Elemente $a_1, \ldots, a_n,\ b_1, \ldots, b_n \in A$ gilt: Wenn $a_1 \sim b_1, \ldots, a_n \sim b_n$, dann auch

$$f^{\mathfrak{A}}(a_1, \ldots, a_n) \sim f^{\mathfrak{A}}(b_1, \ldots, b_n).$$

Anders formuliert: Wenn $[a_1] = [b_1], \ldots, [a_n] = [b_n]$, dann auch $[f^{\mathfrak{A}}(a_1, \ldots, a_n)] = [f^{\mathfrak{B}}(b_1, \ldots, b_n)]$.

(2) Für jede n-stellige Relation $R^{\mathfrak{A}}$ von $\mathfrak{A}$ und alle $a_1, \ldots, a_n,\ b_1, \ldots, b_n \in A$ gilt: Wenn $a_1 \sim b_1, \ldots, a_n \sim b_n$, dann

$$(a_1, \ldots, a_n) \in R^{\mathfrak{A}} \iff (b_1, \ldots, b_n) \in R^{\mathfrak{A}}.$$

Die Äquivalenzklassen bzgl. einer Kongruenzrelation heissen auch *Kongruenzklassen.*

Definition 2.13. $\mathfrak{A}$ sei eine τ-Struktur und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Die *Quotienten-* oder *Faktor-Struktur* $\mathfrak{A}/_\sim$ ist die τ-Struktur welche wie folgt definiert ist:

(1) Das Universum von $\mathfrak{A}/_\sim$ ist die Menge $A/_\sim := \{[a] : a \in A\}$ der *Kongruenzklassen* von A.

(2) Für $f \in F^n(\tau)$ ist

$$f^{\mathfrak{A}/\sim}([a_0], \dots, [a_{n-1}]) := [f^{\mathfrak{A}}(a_0, \dots, a_{n-1})].$$

(3) Für $R \in R^n(\tau)$

$$([a_0], \dots, [a_{n-1}]) \in R^{\mathfrak{A}/\sim} \iff (a_0, \dots, a_{n-1}) \in R^{\mathfrak{A}}.$$

Man beachte, dass $f^{\mathfrak{A}/\sim}$ und $R^{\mathfrak{A}/\sim}$ wohldefiniert sind. In der Tat sind die in (2), (3) angegebenen Definitionen unabhängig von der Wahl der Repräsentanten, denn genau dies wird ja durch die Kompatibilitätsbedingungen für Kongruenzrelationen gefordert.

Beispiele. (1) Für jedes $n \in \mathbb{N} - \{0\}$ ist

$$E_n := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \text{ teilt } a - b\}$$

eine Kongruenzrelation auf $(\mathbb{Z}, +, \cdot, 0, 1)$. Für jedes n ist die zugehörige Faktorstruktur $\mathbb{Z}_n$ wieder ein Ring. (Für Primzahlen p ist $\mathbb{Z}_p$ sogar ein Körper.)

(2) Betrachte die τ_{ar}-Struktur $\mathfrak{A} = (\mathbb{Z} \times (\mathbb{Z} - \{0\}), +^{\mathfrak{A}}, \cdot^{\mathfrak{A}}, 0^{\mathfrak{A}}, 1^{\mathfrak{A}})$ mit

$$\begin{aligned} (a,b) +^{\mathfrak{A}} (c,d) &:= (ad + bc, bd), \\ (a,b) \cdot^{\mathfrak{A}} (c,d) &:= (ac, bd), \\ 0^{\mathfrak{A}} &:= (0,1), \\ 1^{\mathfrak{A}} &:= (1,1). \end{aligned}$$

Man zeige, dass $(a,b) \sim (c,d) \;:\Longleftrightarrow\; ad = bc$ eine Kongruenzrelation definiert ist und dass die Faktorstruktur $\mathfrak{A}/_\sim$ isomorph ist zum Körper der rationalen Zahlen.

Kongruenzrelationen und Homomorphismen. Wir diskutiern nun den Zusammenhang zwischen Faktorstrukturen und homomorphen Bildern.

Lemma 2.14. *Sei $\mathfrak{A}$ eine τ-Struktur und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Die Quotienten-Abbildung $\pi : A \to A/_\sim$ mit $a \mapsto [a]$ ist ein surjektiver Homomorphismus von $\mathfrak{A}$ auf $\mathfrak{A}/_\sim$.*

Der Beweis ist offensichtlich.

Satz 2.15. *Sei τ eine funktionale Signatur, und seien $\mathfrak{A}, \mathfrak{B}$ τ-Algebren. Für jeden Homomorphismus $\pi : \mathfrak{A} \to \mathfrak{B}$ ist die Relation*

$$E_\pi := \{(a, a') \in A \times A : \pi a = \pi a'\}$$

eine Kongruenzrelation über $\mathfrak{A}$.

Beweis. Offensichtlich ist E_π eine Äquivalenzrelation. Für $a_1, \dots, a_n$ und $a'_1, \dots, a'_n$ gelte nun $(a_i, a'_i) \in E_\pi$, also $\pi(a_i) = \pi(a'_i) = b_i$ für geeignete $b_1, \dots, b_n \in B$. Da π ein Homomorphismus ist, gilt für alle $f \in F^n(\tau)$, dass $\pi f^{\mathfrak{A}}(\bar{a}) = \pi f^{\mathfrak{A}}(\bar{a}') = f^{\mathfrak{B}}(\bar{b})$. Also sind auch $f^{\mathfrak{A}}(\bar{a})$ und $f^{\mathfrak{A}}(\bar{a}')$ äquivalent bzg. E_π. $\square$

Beispiel. Sei π eine lineare Abbildung von einem Vektorraum V in einen Vektorraum W. Dann ist $E_\pi = \{(v, v') : v - v' \in \mathrm{Kern}\pi\}$.

Bemerkung. Für nicht-funktionale Strukturen $\mathfrak{A}$, $\mathfrak{B}$ gilt dieser Satz nicht. Seien etwa $\mathfrak{A} = (\{a, b, c\}, R^{\mathfrak{A}})$, $\mathfrak{B} = (\{a, c\}, R^{\mathfrak{B}})$ mit $R^{\mathfrak{A}} = R^{\mathfrak{B}} = \{(a, c)\}$. Die Abbildung $\pi : \{a, b, c\} \to \{a, c\}$ mit $\pi(a) = \pi(b) = a$, $\pi(c) = c$ ist ein Homomorphismus, aber das zugehörige $E_\pi = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ ist keine Kongruenzrelation. Obwohl nämlich $(a, c) \in R^{\mathfrak{A}}$ und $(a, b) \in E_\pi$ sind ist $(b, c) \notin R^{\mathfrak{B}}$.

Sei $\pi : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus von τ-Strukturen. Da für jedes Funktionssymbol $f \in \tau$ gilt, dass $f^{\mathfrak{B}} \circ \pi = \pi \circ f^{\mathfrak{A}}$, ist das Bild $\pi(A) \subseteq B$ τ-abgeschlossen und daher Träger einer Substruktur $\pi(\mathfrak{A}) \subseteq \mathfrak{B}$.

Satz 2.16 (Homomorphie-Satz). *Für jeden Homomorphismus $\pi : \mathfrak{A} \to \mathfrak{B}$ zwischen τ-Algebren ist $\mathfrak{A}/_{E_\pi} \cong \pi(\mathfrak{A})$.*

Beweis. Man prüft leicht nach, dass die Abbildung $[a] \mapsto \pi a$ wohldefiniert ist und einen Isomorphismus von $\mathfrak{A}/_{E_\pi}$ nach $\pi(\mathfrak{A})$ definiert. □

Der aus der Linearen Algebra bekannte Homomorphiesatz für lineare Abbildungen auf Vektorräumen ist ein Spezialfall von Satz 2.16.

Kapitel 3

Syntax und Semantik der Prädikatenlogik

Die Aussagenlogik behandelt ausschliesslich Aussagen, welche aus atomaren Formeln mit Hilfe der aussagenlogischen Verknüpfungen $\wedge, \vee, \neg$ etc. zusammengesetzt werden. Eine aussagenlogische Interpretation ordnet den atomaren Formeln Wahrheitswerte 0 oder 1 zu, und dies setzt sich fort zu einer Interpretation beliebiger aussagenlogischer Formeln. Insbesondere haben die atomaren Aussagen selbst keine innere Struktur, ja wir abstrahieren vollständig vom mathematischen, umgangssprachlichen oder technischen Inhalt einer atomaren Aussage, nur ihr Wahrheitswert ist massgebend.

Für die meisten mathematischen Anwendungen ist die Aussagenlogik viel zu ausdrucksschwach. Bereits sehr einfache, alltägliche Argumente über konkrete Strukturen, z.B. "alle Quadratzahlen sind positiv, $25 = 5 \cdot 5$, also ist 25 positiv" widersetzen sich einer Formalisierung in der Aussagenlogik. Formal hat das Argument die Gestalt $\psi \wedge \varphi \rightarrow \theta$, aber ohne Zugriff auf die Struktur und den Zusammenhang der Teilaussagen ψ, φ, θ gibt es keinen Grund, warum eine solche Implikation wahr sein sollte.

Wir brauchen also ein ausdrucksstärkeres logisches System. Die Prädikatenlogik (abgekürzt FO für "first-order logic") macht Aussagen, welche durch Strukturen und Elemente von Strukturen (also nicht durch blosse Wahrheitswerte) interpretiert werden. Bereits die atomaren Formeln haben eine kompliziertere Struktur, sie sprechen über Relationen zwischen Elementen einer Struktur (z.B. $2x < y + 3$) oder über die Gleichheit von Elementen (z.B. $x^2 = y$). Ausserdem werden Aussagen nicht nur mit Hilfe der aussagenlogischen Junktoren miteinander verknüpft, es besteht auch die Möglichkeit, Existenz- oder Allaussagen über Elemente einer Struktur zu machen, der Art "es gibt eine reelle Zahl x, so dass $x^2 = 2$" oder "zu jeder Primzahl gibt es eine grössere". Was wir hingegen nicht zulassen, sind Existenz- oder Allaussagen über Mengen, Funktionen oder Relationen auf der zugrundegelegten Struktur.

3.1 Syntax der Prädikatenlogik

Wir fixieren eine Signatur τ, und definieren die Menge der τ-Terme und die Menge der τ-Formeln induktiv, als Wortmengen über einem Alphabet Alph(τ) welches aus folgenden Symbolen besteht:

- den Relations- und Funktionssymbolen in τ,
- einer festen, abzählbar unendlichen Menge VAR $= \{v_0, v_1, v_2, \dots\}$ von *Variablen*;
- dem *Gleichheitszeichen* $=$,
- den *aussagenlogischen Junktoren* $\neg, \wedge, \vee$ und $\rightarrow$,
- dem *Existenzquantor* $\exists$ und dem *Allquantor* $\forall$,
- den Klammersymbolen $($, $)$.

τ-Terme sind bestimmte Wörter über diesem Alphabet, welche aus Variablen und Funktionszeichen zusammengesetzt sind. Wir verwenden hier eine klammerfreie Notation.

Definition 3.1. Die Menge $T(\tau)$ der *τ-Terme* ist induktiv wie folgt definiert:

(1) VAR $\subseteq T(\tau)$, d.h. jede Variable ist ein τ-Term.

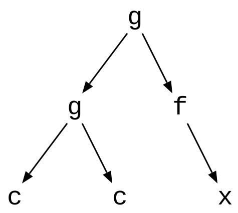
(2) Sind $t_1, \dots, t_n$ τ-Terme und $f \in F^n(\tau)$, so ist auch $ft_1 \cdots t_n$ ein τ-Term.

Wenn wir einen Term in der Form $t(x_1, \dots, x_n)$ schreiben, dann meinen wir, dass $x_1, \dots, x_n$ paarweise verschiedene Variablen sind und dass in t keine anderen Variablen als diese vorkommen. Man beachte, dass insbesondere jedes Konstantensymbol $c \in F^0(\tau)$ ein τ-Term ist. Ein *Grundterm* ist ein Term in dem keine Variablen auftreten.

Beispiel. Die Signatur τ enthalte die Funktionssymbole $f \in F^1(\tau)$, $g \in F^2(\tau)$ und $c \in F^0(\tau)$. Sei $x \in$ VAR eine Variable. Dann sind die folgenden Wörter τ-Terme.

$$x, \quad c, \quad fx, \quad fc, \quad gxx, \quad gfxc, \quad ggccfx.$$

Dabei sind c und fc Grundterme. Es ist oft nützlich, Terme als Bäume aufzufassen. Die Baumnotation des Terms $ggccfx$ ist



Eindeutige Lesbarkeit von Termen. Jedes Wort in Alph$(\tau)^*$ kann auf höchstens eine Weise als ein Term aufgefasst werden. Um dies nachzuweisen, zeigt man zunächst per Induktion über den Termaufbau, dass kein τ-Term ein echtes Anfangsstück eines andern τ-Terms sein kann. Daraus folgt, dass für jeden Term $ft_1 \cdots t_n$ die unmittelbaren Unterterme $t_1, \dots, t_n$ eindeutig bestimmt sind.

Definition 3.2. Die Menge FO(τ) der *τ-Formeln* der Prädikatenlogik ist induktiv definiert wie folgt:

(1) Sind t_1, t_2 τ-Terme dann ist $t_1 = t_2$ eine τ-Formel.

(2) Sind $t_1, \dots, t_n$ Terme aus $T(\tau)$ und ist $P \in \tau$ ein n-stelliges Relationssymbol, dann ist $Pt_1 \cdots t_n$ eine τ-Formel.

(3) Wenn ψ eine τ-Formel ist, dann auch $\neg\psi$.

(4) Wenn ψ und φ τ-Formeln sind, dann auch $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $(\psi \rightarrow \varphi)$.

(5) Wenn ψ eine τ-Formel ist und $x \in \mathrm{VAR}$ eine Variable, dann sind $\exists x\psi$ und $\forall x\psi$ τ-Formeln.

Eine Formel, die nur nach den Regeln (1) und (2) definiert ist, heisst *atomar* oder *Atom-Formel*, oder einfach *Atom. Literale* sind Atome und deren Negationen. Formeln, die nur nach den Regeln (1) – (4) definiert sind, heissen *quantorenfrei*.

Beispiel. Sei $\tau = \{E, f\}$, E ein zweistelliges Relationssymbol, f ein einstelliges Funktionssymbol. Hier sind einige Formeln aus $\mathrm{FO}(\{E, f\})$:

$$v_0 = v_1$$
$$((Ev_0v_0 \vee fv_0 = v_1) \wedge \neg Ev_1fv_0)$$
$$\forall v_0 \forall v_1(\neg v_0 = v_1 \rightarrow Ev_0v_1)$$
$$\forall v_0 \forall v_1(Ev_0v_1 \rightarrow \exists v_2(Ev_0v_2 \wedge Ev_2v_0)).$$

Konventionen zur Notation von Formeln. Wie bei der Aussagenlogik benutzen wir auch bei der Prädikatenlogik abkürzende oder vereinfachende Schreibweisen. Zum Beispiel bezeichnen wir in der Regel Variablen anstelle von $v_0, v_1, \ldots$ mit andern Symbolen, etwa $x, y, z, x_0, x_1, \ldots$. Für Terme, die aus Funktionssymbolen wie $+$, $\cdot$, $\circ$ etc. gebildet werden, verwenden wir in der Regel die Infix-Notation $x+y$ statt $+xy$; ähnliches gilt für Atome wie etwa $t_1 < t_2$ oder gelegentlich auch xEy. Anstelle von $\neg\, t_1 = t_2$ schreiben wir $t_1 \neq t_2$. Wo dies für die Lesbarkeit nützlich ist, werden wir von der klammerfreien Notation von Termen abweichen: So ist etwa $g(fx, g(x, ffy))$ als anschaulichere Beschreibung des Terms $gfxgxffy$ zu verstehen. Zum Beispiel schreiben wir $x + (y + z) = (x + y) + z$ anstelle von $+x + yz = ++xyz$. Andererseits werden wir in Formeln oft Klammern weglassen, welche für das Verständnis überflüssig sind.

Man beachte, dass diese anschaulichen Mitteilungsweisen keine Terme und Formeln im eigentlichen Sinn mehr sind sondern metasprachliche Umschreibungen solcher Objekte. Die präsize formale Definition der syntaktischen Objekte ist notwendig für die Präzisierung des Begriffs einer logischen Aussage, für die Analyse des Beweisbegriffs, und insbesondere für die maschinelle Verarbeitung mathematischer Aussagen. Für die metasprachliche Kommunikation ist eine allzu formale Notation hingegen eher hinderlich als hilfreich. Dies gilt nicht nur für logische Formeln; auch in der Kommunikation über andere syntaktische Objekte, etwa Computer-Programme (für die eine präzise Syntax natürlich zwingend erforderlich ist), wird man, etwa bei der Konzeption und Analyse informellere Beschreibungen vorziehen.

Wir weisen ausserdem darauf hin, dass ein Ausdruck $t_1 = t_2$ je nach Kontext entweder eine Formel aus $\mathrm{FO}(\tau)$ oder aber eine metasprachliche Aussage sein kann, welche die Gleichheit der beiden Terme t_1, t_2 als syntaktische Objekte ausdrückt. Um diese mögliche Quelle von Konfusionen zu vermeiden, kann man entweder zwei verschiedene Gleichheitszeichen einführen oder einfach versuchen, sorgfältig zu sein. Wir wählen hier die zweite Möglichkeit.

Freie und gebundene Variablen. Ein *Vorkommen* einer Variablen x in einer Formel ψ kann *frei* oder *gebunden* sein. Es ist gebunden, wenn es in einer Unterformel der Form $\exists x\psi$ oder $\forall x\psi$ stattfindet, andernfalls ist es frei.

Beispiel. In der folgenden Formel sind unterstrichene Vorkommen von Variablen gebunden, nicht unterstrichene Vorkommen sind frei.

$$\exists \underline{x}(Eyz \wedge \forall \underline{z}(\underline{z} = \underline{x} \vee Ey\underline{z})).$$

Beachte, dass z in dieser Formel sowohl frei als auch gebunden vorkommt.

Formal ist die Menge der in einer Formel frei auftretenden Variablen wie folgt definiert.

Definition 3.3. Sei $t \in T(\tau)$ ein Term und $\psi \in \mathrm{FO}(\tau)$ eine Formel. Mit $\mathrm{Var}(t)$ bzw. $\mathrm{Var}(\psi)$ bezeichnen wir die Menge aller in t bzw. ψ auftretenden Variablen. Die Menge $\mathrm{Frei}(\psi)$ der freien Variablen von ψ ist induktiv wie folgt definiert:

(1) Für atomare Formeln ψ ist $\mathrm{Frei}(\psi) = \mathrm{Var}(\psi)$.

(2) $\mathrm{Frei}(\neg\psi) = \mathrm{Frei}(\psi)$.

(3) $\mathrm{Frei}(\psi \circ \varphi) = \mathrm{Frei}(\psi) \cup \mathrm{Frei}(\varphi)$, für $\circ \in \{\wedge, \vee, \rightarrow\}$.

(4) $\mathrm{Frei}(\exists x\psi) = \mathrm{Frei}(\forall x\psi) = \mathrm{Frei}(\psi) - \{x\}$.

Oft bezeichnen wir eine Formel in der Form $\psi(x_1, \ldots, x_k)$, um anzudeuten, dass höchstens die Variablen $x_1, \ldots, x_k$ in ψ frei vorkommen. Ein *τ-Satz* ist eine τ-Formel ohne freie Variablen.

Mächtigkeit von $\mathbf{T}(\tau)$ und $\mathbf{FO}(\tau)$. Wenn τ abzählbar ist, dann auch das Alphabet $\mathrm{Alph}(\tau)$. Nach Übung 2.1 folgt dann, dass auch $\mathrm{Alph}(\tau)^*$, und damit inbesondere $T(\tau)$ und $\mathrm{FO}(\tau)$ abzählbar sind. Andererseits sind $T(\tau)$ und $\mathrm{FO}(\tau)$ auch bei endlicher Signatur τ (sogar bei $\tau = \varnothing$) unendlich. In der Tat enthält $T(\tau)$ alle Variablen und $\mathrm{FO}(\tau)$ alle Formeln $x = y$ für $x, y \in \mathrm{VAR}$.

3.2 Semantik der Prädikatenlogik

Die Modellbeziehung.

Definition 3.4. Sei τ eine Signatur. Eine *τ-Interpretation* ist ein Paar $\mathfrak{I} = (\mathfrak{A}, \beta)$ wobei $\mathfrak{A}$ eine τ-Struktur und $\beta : X \rightarrow A$ eine Belegung von Variablen durch Elemente von A ist. Dabei ist $X = \mathrm{Def}(\beta) \subseteq \mathrm{VAR}$. Eine τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ ordnet

- jedem Term $t \in T(\tau)$ mit $\mathrm{Var}(t) \subseteq \mathrm{Def}(\beta)$ einen Wert $[\![t]\!]^{\mathfrak{I}} \in A$ zu, und
- jeder Formel $\psi \in \mathrm{FO}(\tau)$ mit $\mathrm{Frei}(\psi) \subseteq \mathrm{Def}(\beta)$ einen Wahrheitswert $[\![\psi]\!]^{\mathfrak{I}} \in \{0, 1\}$. (Wie üblich steht 0 für *falsch* und 1 für *wahr*.)

Die Zuordnung dieser Werte erfolgt induktiv gemäss dem Aufbau der Terme und Formeln wie folgt:

Interpretation von Termen.

(1) Für $x \in \mathrm{Def}(\beta)$ ist $[\![x]\!]^{\mathfrak{I}} := \beta(x)$.

(2) Für $t = ft_1 \cdots t_n$ ist $[\![t]\!]^{\mathfrak{I}} := f^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{I}}, \ldots, [\![t_n]\!]^{\mathfrak{I}})$.

Interpretation von Formeln.

(3) $[\![t_1 = t_2]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{wenn } [\![t_1]\!]^{\mathfrak{I}} = [\![t_2]\!]^{\mathfrak{I}} \\ 0 & \text{sonst.} \end{cases}$

(4) $[\![Pt_1 \cdots t_n]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{wenn } ([\![t_1]\!]^{\mathfrak{I}}, \dots, [\![t_n]\!]^{\mathfrak{I}}) \in P^{\mathfrak{A}} \\ 0 & \text{sonst.} \end{cases}$

Die Bedeutung der Junktoren $\neg, \wedge, \vee$ und $\rightarrow$ ist genau gleich wie in der Aussagenlogik.

(5) $[\![\neg\psi]\!]^{\mathfrak{I}} := 1 - [\![\psi]\!]^{\mathfrak{I}} = \begin{cases} 1 & \text{wenn } [\![\psi]\!]^{\mathfrak{I}} = 0 \\ 0 & \text{wenn } [\![\psi]\!]^{\mathfrak{I}} = 1 \end{cases}$

(6) $[\![\psi \vee \varphi]\!]^{\mathfrak{I}} := \max([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}}) = \begin{cases} 1 & \text{wenn } [\![\psi]\!]^{\mathfrak{I}} = 1 \text{ oder } [\![\varphi]\!]^{\mathfrak{I}} = 1 \\ 0 & \text{sonst.} \end{cases}$

(7) $[\![\psi \wedge \varphi]\!]^{\mathfrak{I}} := \min([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}}) = \begin{cases} 1 & \text{wenn } [\![\psi]\!]^{\mathfrak{I}} = 1 \text{ und } [\![\varphi]\!]^{\mathfrak{I}} = 1 \\ 0 & \text{sonst.} \end{cases}$

(8) $[\![\psi \rightarrow \varphi]\!]^{\mathfrak{I}} := [\![\neg\psi \vee \varphi]\!]^{\mathfrak{I}} = \begin{cases} 0 & \text{wenn } [\![\psi]\!]^{\mathfrak{I}} = 1 \text{ und } [\![\varphi]\!]^{\mathfrak{I}} = 0 \\ 1 & \text{sonst.} \end{cases}$

Um $[\![\exists x\psi]\!]^{\mathfrak{I}}$ und $[\![\forall x\psi]\!]^{\mathfrak{I}}$ zu definieren, verwenden wir folgende Notation: Sei $\beta : X \rightarrow A$ eine Belegung, x eine Variable und a ein Element von A. Wir definieren eine neue Belegung $\beta[x/a] : X \cup \{x\} \rightarrow A$ mit $\beta[x/a](y) := \beta(y)$ für $y \neq x$ und $\beta[x/a](x) := a$. Für $\mathfrak{I} = (\mathfrak{A}, \beta)$ setzen wir $\mathfrak{I}[x/a] := (\mathfrak{A}, \beta[x/a])$. Wir definieren nun

(10) $[\![\exists x\psi]\!]^{\mathfrak{I}} := \max_{a\in A} [\![\psi]\!]^{\mathfrak{I}[x/a]} = \begin{cases} 1 & \text{wenn ein } a \in A \text{ existiert, so dass } [\![\psi]\!]^{\mathfrak{I}[x/a]} = 1 \\ 0 & \text{sonst.} \end{cases}$

(11) $[\![\forall x\psi]\!]^{\mathfrak{I}} := \min_{a\in A} [\![\psi]\!]^{\mathfrak{I}[x/a]} = \begin{cases} 1 & \text{wenn für alle } a \in A \text{ gilt, dass } [\![\psi]\!]^{\mathfrak{I}[x/a]} = 1 \\ 0 & \text{sonst.} \end{cases}$

Ein *Modell* einer Formel ψ ist eine Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$, so dass $\mathrm{Frei}(\psi) \subseteq \mathrm{Def}(\beta)$ und $[\![\psi]\!]^{\mathfrak{I}} = 1$. Wir schreiben dann: $(\mathfrak{A}, \beta) \models \psi$ oder auch $\mathfrak{A} \models \psi[\beta]$ und sagen *ψ gilt in $\mathfrak{A}$ unter der Belegung β*.

Man beachte, dass eine Formel $\psi \in \mathrm{FO}(\sigma)$ auch zu $\mathrm{FO}(\tau)$ gehört, wenn $\sigma \subseteq \tau$. Eine Interpretation $(\mathfrak{A}, \beta)$ ist also *passend* für eine Formel ψ wenn alle Funktions- und Relationssymbole von ψ in der Signatur von $\mathfrak{A}$ enthalten sind, und alle freien Variablen von ψ zum Definitionsbereich von β gehören. Offensichtlich ist für die Modellbeziehung die Interpretation der Relations- und Funktionssymbole, welche in ψ gar nicht vorkommen, sowie die Belegung der in ψ nicht frei auftretenden Variablen unerheblich. Dieser Sachverhalt, den man durch eine einfache, aber langweilige Induktion über den Formelaufbau nachweisen kann, wird durch das Koinzidenzlemma ausgedrückt.

Lemma 3.5 (Koinzidenzlemma). *Sei $\psi \in \mathrm{FO}(\sigma \cap \tau)$, $(\mathfrak{A}, \beta)$ eine σ-Interpretation und $(\mathfrak{A}', \beta')$ eine τ-Interpretation, so dass folgendes gilt:*

(i) $\mathfrak{A}$ *und* $\mathfrak{A}'$ *haben dasselbe* $(\sigma \cap \tau)$*-Redukt:* $\mathfrak{A} \restriction \sigma \cap \tau = \mathfrak{A}' \restriction \sigma \cap \tau$.

(ii) $\mathrm{Frei}(\psi) \subseteq \mathrm{Def}(\beta) \cap \mathrm{Def}(\beta')$ *und* $\beta(x) = \beta'(x)$ *für alle* $x \in \mathrm{Frei}(\psi)$.

Dann gilt: $\mathfrak{A} \models \psi[\beta] \iff \mathfrak{A}' \models \psi[\beta']$.

Notation. Wie erwähnt, deuten wir mit der Notation $\psi(x_1, \dots, x_k)$ an, dass $\mathrm{Frei}(\psi) \subseteq \{x_1, \dots, x_k\}$. Sei nun $(\mathfrak{A}, \beta)$ eine Interpretation welche die Variablen $x_1, \dots, x_k$ durch die Elemente $a_1 = \beta(x_1), \dots, a_k = \beta(x_k)$ bewertet. Wir schreiben dann anstelle von $\mathfrak{A} \models \psi[\beta]$ meistens $\mathfrak{A} \models \psi(a_1, \dots, a_k)$. (Diese Notation ist durch das Koinzidenzlemma gerechtfertigt, denn es gilt dann $\mathfrak{A} \models \psi[\beta']$ für *alle* Belegungen β' welche $x_1, \dots, x_k$ auf $a_1, \dots a_k$ abbilden.) Ist ψ ein Satz (also $\mathrm{Frei}(\psi) = \varnothing$) so schreiben wir $\mathfrak{A} \models \psi$ und nennen $\mathfrak{A}$ ein Modell von ψ.

Beispiel. Sei $\psi := \exists z(Exz \wedge Ezy)$ und $\varphi := \forall x \forall y(Exy \rightarrow \psi)$. Offensichtlich ist ψ eine $\{E\}$-Formel mit $\mathrm{Frei}(\psi) = \{x, y\}$ und φ ein $\{E\}$-Satz.

Die Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ mit $\mathfrak{A} = (\mathbb{N}, E^{\mathfrak{A}})$, $E^{\mathfrak{A}} = \{(m, n) : m$ ist ein echter Teiler von $n\}$ und $\beta(x) = 2$, $\beta(y) = 36$ ist ein Modell von $\psi(x, y)$, d.h. $\mathfrak{A} \models \psi(2, 36)$. In der Tat existiert ein $m \in \mathbb{N}$ (z.B. $m = 6$), so dass unter der Belegung $\beta[z/m]$ die Formel $(Exz \wedge Ezy)$ in $\mathfrak{A}$ gilt. Jedoch gilt *nicht* $\mathfrak{A} \models \varphi$, denn unter der Belegung $x \mapsto 2, y \mapsto 4$ ist $(Exy \rightarrow \psi)$ falsch in $\mathfrak{A}$ (2 ist echter Teiler von 4, aber es gibt keine Zahl, welche echt von 2 geteilt wird und ihrerseits 4 echt teilt). Hingegen ist $(\mathbb{Q}, <)$ ein Modell von φ, da $\mathbb{Q}$ dicht geordnet ist.

Ein *Modell einer Formelmenge* $\Phi \subseteq \mathrm{FO}(\tau)$ ist eine τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$, so dass $\mathfrak{A} \models \varphi[\beta]$ für alle $\varphi \in \Phi$ gilt. Ein Modell einer Formelmenge erfüllt also alle Formeln in dieser Menge gleichzeitig.

Definition 3.6. Sei Φ eine Menge von τ-Sätzen. Die *Modellklasse von* Φ (kurz: $\mathrm{Mod}(\Phi)$) besteht aus aus allen τ-Strukturen $\mathfrak{A}$ mit $\mathfrak{A} \models \Phi$. Eine Klasse $\mathcal{K}$ von τ-Strukturen ist *axiomatisiert durch* Φ, wenn $\mathcal{K} = \mathrm{Mod}(\Phi)$. Wir nennen Φ dann ein *Axiomensystem* für $\mathcal{K}$.

Beispiele. (1) Die Klasse aller *ungerichteten Graphen* ist die Modellklasse von

$$\Phi_{\mathrm{Graph}} = \{\forall x \neg Exx,\ \forall x \forall y(Exy \rightarrow Eyx)\}.$$

(2) Die Klasse aller *Gruppen* $(G, \circ, e, {}^{-1})$ ist axiomatisiert durch

$$\Phi_{\mathrm{Gruppe}} = \{\forall x \forall y \forall z(x \circ (y \circ z) = (x \circ y) \circ z), \forall x(x \circ e = x), \forall x(x \circ x^{-1} = e)\}.$$

(3) Ein Axiomensystem für die Klasse aller linearen Ordnungen ist

$$\Phi_{<} = \{\forall x \neg x < x, \forall x \forall y \forall z(x < y \wedge y < z \rightarrow x < z), \forall x \forall y(x < y \vee x = y \vee y < x)\}.$$

(4) Für eine beliebige Signatur τ und $n \in \mathbb{N}$ sei $\mathcal{K}_{\geqslant n}$ die Klasse der τ-Strukturen mit mindestens n Elementen. $\mathcal{K}_{\geqslant n}$ (für $n \geq 2$) ist axiomatisiert durch den Satz

$$\varphi_{\geqslant n} := \exists x_1 \cdots \exists x_n \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j.$$

Die Klasse $\mathcal{K}_{\infty}$ aller unendlichen τ-Strukturen ist axiomatisiert durch das unendliche Axiomensystem $\Phi_{\infty} = \{\varphi_{\geqslant n} : n \in \mathbb{N}\}$.

Die semantische Folgerungsbeziehung ("ψ folgt aus Φ"), sowie die Begriffe "erfüllbar", "allgemeingültig" und "logisch äquivalent" sind wie für die Aussagenlogik definiert.

Definition 3.7. (Semantische Folgerungsbeziehung) Sei $\Phi \subseteq \mathrm{FO}(\tau)$ eine Formelmenge, $\psi \in \mathrm{FO}(\tau)$ eine Formel. Wir sagen, ψ *folgt aus* Φ (kurz: $\Phi \models \psi$) genau dann, wenn jede zu $\Phi \cup \{\psi\}$ passende Interpretation, welche Modell von Φ ist, auch Modell von ψ ist. Wenn $\Phi = \{\varphi\}$ schreiben wir auch $\varphi \models \psi$ anstelle von $\{\varphi\} \models \psi$.

Beispiele. (1) $\Phi_{\text{Gruppe}} \models \psi$ bedeutet, dass ψ in jeder Gruppe gilt. Man beachte, dass Φ_{Gruppe} eine Menge von Sätzen ist, dass aber in ψ durchaus freie Variabeln vorkommen dürfen. Da jedes Modell von Φ_{Gruppe} auch ein Modell von ψ sein muss, bedeutet $\Phi_{\text{Gruppe}} \models \psi$, dass $(\mathfrak{G}, \beta) \models \psi$ für jede Gruppe $\mathfrak{G}$ und jede Belegung β. Zum Beispiel gilt $\Phi_{\text{Gruppe}} \models x^{-1} \circ x = e$ (da in jeder Gruppe das (Rechts-)Inverse jedes Elements auch Linksinverses ist.) Hingegen ist $\Phi_{\text{Gruppe}} \not\models x \circ y = y \circ x$, da nicht jede Gruppe kommutativ ist.

(2) $\Phi_\infty \models \psi$ bedeutet, dass ψ in allen unendlichen Strukturen gilt.

Definition 3.8. Hat eine Formel ψ (bzw. eine Formelmenge Φ) ein Modell, so heisst ψ (bzw. Φ) *erfüllbar*, andernfalls *unerfüllbar*. Eine Formel ψ heisst *allgemeingültig* (kurz: $\models \psi$), wenn jede zu ψ passende Interpretation ein Modell von ψ ist. Dies ist äquivalent zur Aussage, dass ψ aus der leeren Formelmenge folgt. Zwei Formeln ψ und φ heissen *logisch äquivalent* (kurz: $\psi \equiv \varphi$), wenn $\psi \models \varphi$ und $\varphi \models \psi$.

Definition 3.9. Sei ψ eine Formel mit freien Variablen $x_1, \dots, x_k$. Dann nennen wir die Sätze $\exists x_1 \cdots \exists x_k \psi$ und $\forall x_1 \cdots \forall x_k \psi$ den *existentiellen* bzw. *universellen Abschluss* von ψ.

Lemma 3.10. *(i) Eine Formel ist erfüllbar genau dann, wenn ihr existentieller Abschluss erfüllbar ist.*

(ii) Eine Formel ist eine allgemeingültig genau dann, wenn ihr universeller Abschluss allgemeingültig ist.

3.3 Substitutionen

In der Prädikatenlogik haben wir Substitutionsoperatoren für Terme und Formeln. Der einfachste Fall ist die Substitution einer einzelnen Variablen x durch einen Term $s \in T(\tau)$. Wenn wir jedes Vorkommen von x in einem Term t durch s ersetzten, erhalten wir einen neuen Term $t[x/s]$. Für die Baumnotation von Termen bedeutet dies, dass jedes mit x beschriftete Blatt von t durch eine Kopie des Baumes s ersetzt wird. Man beachte, dass x in s und damit auch im Term $t[x/s]$ vorkommen kann. Auch in einer Formel ψ möchten wir die freien Vorkommen von x durch einen Term t ersetzen können, um eine neue Formel $\psi[x/t]$ zu erhalten, welche dasselbe über t aussagen soll wie ψ über x.

Beispiel. Mit Hilfe einer Substitution lässt sich eine Aussage "es gibt genau ein x, so dass ψ" auf bequeme Weise formalisieren, etwa durch $\exists x(\psi \land \forall y(\psi[x/y] \to x = y))$.

Bei der präzisen Definition muss man etwas aufpassen, um Konflikte zwischen freien und gebundenen Variablen zu vermeiden. Man betrachte etwa die Formel $\psi = \exists z(x + z = y)$. Interpretiert in der Struktur $(\mathbb{N}, +)$ sagt ψ aus, dass $x \leq y$. Eine Ersetzung von x durch eine Variable u oder auch durch einen Term $u + u$ ist unproblematisch, wenn u von x und y verschieden ist: die Formel $\psi[x/u + u] = \exists z(u + u + z = y)$ drückt dann eben aus, dass $2u \leq y$. Man betrachte jedoch die Formel $\exists z(z + z + z = y)$, welche durch 'naive' Ersetzung von x durch $z + z$ gewonnen wird. In $(\mathbb{N}, +)$ drückt diese Formel einen ganz anderen Sachverhalt als $2z \leq y$ aus (nämlich dass y durch 3 teilbar ist). Der Grund für diese Bedeutungsänderung liegt darin, dass der eingesetzte Term $z + z$ eine Variable enthält, die in ψ gebunden auftritt. Dieser Konflikt kann allerdings auf einfache Weise aufgelöst werden, indem die gebundene Variable z in ψ zunächst durch eine neue Variable u ersetzt wird, und erst dann die Substitution von x durch $z + z$ durchgeführt wird. Wir erhalten so die Formel $\exists u(z + z + u = y)$, welche in der Tat den gewünschten Sachverhalt ausdrückt.

Ausserdem möchte man gerne einen etwas allgemeineren Begriff einer Substitution zur Vefügung haben, welcher die gleichzeitige Ersetzung von mehreren Variablen erlaubt. Substitutionen werden als eigenständige Objekte betrachtet und studiert; sie spielen eine wesentliche Rolle in Gebieten wie der Unifikationstheorie, dem automatischen Beweisen und der Logik-Programmierung.

Definition 3.11. Eine Substitution ist eine Funktion $\rho : \mathrm{VAR} \to T(\tau)$. In der Regel wird voraussgesetzt, dass ρ *endlichen Support* hat, d.h. dass ρ alle bis auf endlich viele $x \in \mathrm{VAR}$ fest lässt. Wir bezeichnen eine Substitution, welche die Variablen $x_1, \ldots, x_k$ auf die Terme $t_1, \ldots, t_k$ abbildet und alle andern Variablen fest lässt, auch in der Form $x_1/t_1, \ldots, x_k/t_k$.

Operation auf Termen. Eine Substitution kann auf eindeutige Weise zu einer Funktion $\overline{\rho} : T(\tau) \to T(\tau)$ fortgesetzt werden. Man ersetzt einfach alle Vorkommen von x in t durch $\rho(x)$. Wir bezeichnen das Resultat der Anwendung von $\overline{\rho}$ auf t mit $t[\rho]$. Offensichtlich ist $ft_1 \cdots t_n[\rho] = ft_1[\rho] \cdots t_n[\rho]$.

Operation auf Formeln. Die Anwendung einer Substitution $\rho = [x_1/t_1, \ldots, x_k/t_k]$ auf eine Formel ψ führt zu einer neuen Formel $\psi[\rho]$, welche wir dadurch erhalten, dass wir *simultan* alle *freien* Vorkommen von $x_1, \ldots, x_k$ durch die Terme $t_1, \ldots, t_k$ ersetzen, sofern keine Kollisionen auftreten. Gebundene Variablen werden nicht ersetzt. Eine Kollision tritt dann auf, wenn eines der freien Vorkommen einer zu ersetzenden Variablen x_i in einer Unterformel $\exists y\varphi$ oder $\forall y\varphi$ stattfindet und der Term t_i die Variable y enthält. Um eine solche Kollision aufzulösen ersetzen wir in $\exists y\varphi$ zunächst die gebundene Variable y durch eine neue, nicht in ψ und $t_1, \ldots, t_k$ vorkommende Variable, und führen dann die Substitution durch.

Beispiel. Sei $\psi := Rx_0x_2 \wedge \exists x_0(Rx_0x_1 \wedge Rx_0x_2)$ und sei ρ die Substitution $(x_0/x_4, x_1/c, x_2/gx_0x_0)$. Hier tritt eine Kollision auf, da eines der freien Vorkommen von x_2 in der Teilformel $\exists x_0(Rx_0x_1 \wedge Rx_0x_2)$ stattfindet und x_2 durch den Term gx_0x_0 ersetzt werden soll. Wir müssen daher zuerst die gebundenen Vorkommen von x_0 durch eine neue Variable x_3 ersetzen, bevor wir die Substitution durchführen können.

$$\begin{aligned}(\psi)[\rho] &= (Rx_0x_2 \wedge \exists x_0(Rx_0x_1 \wedge Rx_0x_2))[\rho] \\ &= (Rx_0x_2 \wedge \exists x_3(Rx_3x_1 \wedge Rx_3x_2))[\rho] \\ &= Rx_4gx_0x_0 \wedge \exists x_3(Rx_3c \wedge Rx_3gx_0x_0).\end{aligned}$$

Zu beachten ist der Unterschied zwischen der soeben beschriebenen simultanen Substitution und dem Hintereinanderausführen von Substitutionen einzelner Variablen. So ist etwa das Vertauschen zweier Variablen x und y in einer Formel $\varphi(x, y)$ eine simultane Substitution: wir gehen von φ zu der Formel $\varphi[x/y, y/x]$ über (für die wir üblicherweise einfach $\varphi(y, x)$ schreiben). Führen wir aber die beiden Ersetzungen x/y und y/x hintereinander aus, dann erhalten wir die Formel $\varphi[x/y][y/x] = \varphi[y/x]$. Angewandt auf die Formel $\varphi := Rxy$ ist $\varphi[x/y, y/x] = Ryx$ während $\varphi[x/y][y/x] := Rxx$.

Man kann aber durch Einführen neuer Variablen simultane Substitutionen durch Komposition von einzelnen Substituionen simulieren. So ist etwa $\varphi[x/y, y/x] = \varphi[y/z][x/y][z/x]$, falls z verschieden ist von den freien Variablen in φ.

Übung 3.1. Zeigen Sie:

(a) $\varphi[x_1/t_1, \ldots, x_n/t_n] = \varphi[x_1/t_1] \cdots [x_n/t_n]$ falls für alle $i \neq j$ x_i nicht in t_j vorkommt;

(b) $\varphi[x_1/t_1, \ldots, x_n/t_n] = \varphi[x_n/y][x_1/t_1, \ldots, x_{n-1}/t_{n-1}][y/t_n]$ falls y nicht in φ und den Termen $t_1, \ldots, t_n$ vorkommt.

(c) Verallgemeinern Sie (b) so, dass $\varphi[x_1/t_1, \ldots, x_n/t_n]$ aus φ mittels einer Komposition einfacher Substitutionen gewonnen werden kann.

Notation. Wenn klar ist (oder unerheblich), welche Variablen durch welche Terme ersetzt werden, benutzt man oft vereinfachende Schreibweisen, wie etwa $\psi(t_1, \ldots, t_n)$ anstelle von $\psi[x_1/t_1, \ldots, x_n/t_n]$.

Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine τ-Interpretation und $\rho = (x_1/t_1, \ldots, x_k/t_k)$ eine Substitution so dass $[\![t_1]\!]^{\mathfrak{I}}, \ldots, [\![t_k]\!]^{\mathfrak{I}}$ definiert sind. (Dies ist dann der Fall, wenn alle Variablen von $t_1, \ldots, t_k$ im Definitionsbereich von β sind.) Dann ist $\mathfrak{I} \circ \rho = (\mathfrak{A}, \beta[x_1/[\![t_1]\!]^{\mathfrak{I}}, \ldots, x_k/[\![t_k]\!]^{\mathfrak{I}}])$ eine neue Interpretation über der Struktur $\mathfrak{A}$, welche Variablen $y \in \mathrm{Def}(\beta) \cup \{x_1, \ldots, x_k\}$ durch $[\![\rho(y)]\!]^{\mathfrak{I}}$ bewertet. Das Substitutionslemma besagt, dass es zum selben Resultat führt, wenn wir einen Term t oder eine Formel ψ mittels $\mathfrak{I} \circ \rho$ interpretieren, wie wenn wir zuerst die Substition ρ anwenden und dann den Term $t[\rho]$ bzw. die Formel $\psi[\rho]$ via $\mathfrak{I}$ interpretieren.

Lemma 3.12 (Substitutionslemma). *Für jeden Term $t \in T(\tau)$, jede Formel $\psi \in \mathrm{FO}(\tau)$, jede Substitution $\rho : \mathrm{VAR} \to T(\tau)$ und jede zu $t[\rho]$ bzw. $\psi[\rho]$ passende Interpretation $\mathfrak{I}$ gilt:*

(i) $[\![t[\rho]]\!]^{\mathfrak{I}} = [\![t]\!]^{\mathfrak{I} \circ \rho}$.

(ii) $\mathfrak{I} \models \psi[\rho] \iff (\mathfrak{I} \circ \rho) \models \psi$.

Beweis. Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine zu $t[\rho]$ passende Interpretation. Für jede Variable y (auf der $\mathfrak{I} \circ \rho$ definiert ist) gilt $[\![y]\!]^{\mathfrak{I} \circ \rho} = [\![\rho(y)]\!]^{\mathfrak{I}}$ nach Definition.

Per Induktion über den Termaufbau gilt

$$\begin{aligned} [\![ft_1 \cdots t_n]\!]^{\mathfrak{I} \circ \rho} &= f^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{I} \circ \rho}, \ldots, [\![t_n]\!]^{\mathfrak{I} \circ \rho}) \\ &= f^{\mathfrak{A}}([\![t_1[\rho]]\!]^{\mathfrak{I}}, \ldots, [\![t_n[\rho]]\!]^{\mathfrak{I}}) = [\![ft_1 \cdots t_n[\rho]]\!]^{\mathfrak{I}}. \end{aligned}$$

Die Behauptung für Formeln ergibt sich auf einfache Weise per Induktion über den Formelaufbau. □

3.4 Normalformen

Der Begriff einer Normalform taucht in vielen Gebieten der Mathematik auf. Die allgemeine Situation ist die, dass auf einer Menge M von mathematischen Objekten (hier: von Formeln) eine Äquivalenzrelation $\sim$ gegeben ist. Angestrebt wird eine Aussage der Art, dass für eine bestimmte Teilmenge $N \subseteq M$ (von Objekten 'in Normalform') jede $\sim$-Äquivalenzklasse einen Repräsentanten in N besitzt. Oft sind auch stärkere Aussagen erwünscht, etwa über die effiziente Konstruierbarkeit solcher Repräsentanten. Ein bekanntes Beispiel aus der Linearen Algebra sind die Sätze über Normalformen von Matrizen.

Wir sind hier interessiert an Normalformen für Formeln der Prädikatenlogik. Die zugrunde gelegte Äquivalenzrelation ist in der Regel die logische Äquivalenz; wir werden aber am Ende dieses Abschnitts auch eine Normalform für eine schwächere Äquivalenzrelation betrachten, nämlich die Skolem-Normalform.

Wir beginnen mit einer einfachen Beobachtung, welche die Technik begründet, Transformationen in äquivalente Formeln per Induktion über den Formelaufbau durchzuführen.

Lemma 3.13 (Ersetzungslemma). *Für beliebige Formeln $\psi, \psi', \varphi, \varphi'$ gilt:*

(i) *Wenn $\psi \equiv \varphi$, dann auch $\neg\psi \equiv \neg\varphi$.*

(ii) *Wenn $\psi \equiv \psi'$ und $\varphi \equiv \varphi'$, dann auch $(\psi \circ \varphi) \equiv (\psi' \circ \varphi')$ für $\circ \in \{\wedge, \vee, \rightarrow\}$.*

(iii) *Wenn $\psi \equiv \varphi$, dann auch $\exists x\psi \equiv \exists x\varphi$ und $\forall x\psi \equiv \forall x\varphi$.*

(iv) *Sei ϑ eine Teilformel von ψ und sei $\vartheta \equiv \varphi$. Sei weiter $\psi[\vartheta/\varphi]$ diejenige Formel, die man aus ψ erhält, indem man ϑ durch φ ersetzt. Dann ist $\psi \equiv \psi[\vartheta/\varphi]$.*

Beweis. Die Aussagen *(i)* – *(iii)* sind trivial; *(iv)* ergibt sich durch Induktion über den Formelaufbau mittels *(i)* – *(iii)*. □

Reduzierte Formeln. Aus der Definition der Modellbeziehung ergibt sich sofort, dass für beliebige Formeln ψ, φ folgende Äquivalenzen gelten. (1) und (2) kennnen wir bereits aus der Aussagenlogik.

(1) $\psi \wedge \varphi \equiv \neg(\neg\psi \vee \neg\varphi)$

(2) $\psi \rightarrow \varphi \equiv \neg\psi \vee \varphi$

(3) $\forall x\psi \equiv \neg\exists x\neg\psi$

Daraus folgt, dass wir uns ohne Verlust an Ausdrucksstärke etwa auf die Junktoren $\vee, \neg$ und den Quantor $\exists$ beschränken können. Wir nennen Formeln, in denen die Symbole $\wedge, \rightarrow, \leftrightarrow$ und $\forall$ nicht vorkommen, *reduziert*.

Lemma 3.14. *Zu jeder Formel $\psi \in \mathrm{FO}(\tau)$ kann man effektiv eine logisch äquivalente reduzierte Formel konstruieren.*

Wir können daher in vielen Fällen die Betrachtung auf reduzierte Formeln beschränken. Der Vorteil der Verwendung reduzierter Formeln liegt darin, dass sie aus weniger Symbolen aufgebaut sind, und daher konzisere Definitionen und kürzere Induktionsbeweise erlauben.[1] Ein Nachteil reduzierter Formeln ist, dass sie länger und schlechter lesbar werden.

Negationsnormalform. In manchen Situationen (z.B. für Auswertungsalgorithmen oder für die spieltheoretische Deutung der Semantik, siehe Kapitel 3.5) ist es praktisch, den nicht-monotonen Junktor $\rightarrow$ auszuschliessen und die Anwendung der Negation auf atomare Formeln einzuschränken.

[1] Aus diesem Grund wird in einigen Lehrbüchern die Prädikatenlogik nur mit den Junktoren $\vee, \neg$ und dem Existenquantor eingeführt. Formeln mit $\wedge, \vee, \rightarrow$ und $\forall$ werden als abkürzende, informelle Schreibweisen für die eigentlichen, reduzierten Formeln verstanden.

Definition 3.15. Eine Formel ist in *Negationsnormalform*, wenn sie aus Literalen (d.h. atomaren Formeln und Negationen atomarer Formeln) nur mit Hilfe der Junktoren $\vee$, $\wedge$ und der Quantoren $\exists$ und $\forall$ aufgebaut ist.

Satz 3.16. *Jede Formel aus* FO *ist logisch äquivalent zu einer Formel in Negationsnormalform.*

Beweis. Wir haben bereits gesehen, dass $\rightarrow$ eliminiert werden kann. Durch wiederholte Anwendung der de Morganschen Regeln

$$\neg(\psi \wedge \varphi) \equiv (\neg\psi \vee \neg\varphi) \qquad \neg(\psi \vee \varphi) \equiv (\neg\psi \wedge \neg\varphi)$$

und der Quantorenregeln

$$\neg\exists x\psi \equiv \forall x\neg\psi \qquad \neg\forall x\psi \equiv \exists x\neg\psi$$

kann jede FO-Formel in eine äquivalente Formel transformiert werden, in der Negationen nur noch auf atomare Formeln angewandt werden. $\square$

Beispiel. Um die Formel $\neg\exists x(Rxy \wedge \forall z(Sxz \rightarrow Ryy))$ in Negationsnormalform zu überführen, zieht man die Negationen schrittweise 'nach innen' und eliminiert $\rightarrow$:

$$\begin{aligned}\neg\exists x(Rxy \wedge \forall z(Sxz \rightarrow Ryy)) &\equiv \forall x\neg(Rxy \wedge \forall z(Sxz \rightarrow Ryy))\\ &\equiv \forall x(\neg Rxy \vee \neg\forall z(Sxz \rightarrow Ryy))\\ &\equiv \forall x(\neg Rxy \vee \exists z\neg(Sxz \rightarrow Ryy))\\ &\equiv \forall x(\neg Rxy \vee \exists z(Sxz \wedge \neg Ryy))\end{aligned}$$

Termreduzierte Formeln. Eine weitere Normalform, welche insbesondere für die Elimination von Funktionen nützlich ist, betrifft die Komplexität der darin auftretenden Terme. Eine Formel heisst *termreduziert* , wenn sie nur Atome der Form $R\bar{x}$, $f\bar{x} = y$ und $x = y$ enthält (also insbesondere keine Terme der Tiefe ≥ 2).

Lemma 3.17. *Zu jeder Formel gibt es eine logisch äquivalente termreduzierte Formel.*

Beweis. Wenn ψ nicht termreduziert ist, dann enthält ψ einen Term t der Form $t = f\bar{x}$, der in ψ an einer 'verbotenen' Stelle auftritt (z.B. als Argument in einem Atom $R \cdots t \cdots$, oder $t = t'$, oder als Subterm eines komplizierteren Terms). Führe eine neue Variable x_t ein und ersetze jedes Atom α, das t an einer verbotenen Stelle enthält, durch $\exists x_t(x_t = t \wedge \alpha[t/x_t])$ wobei $\alpha[t/x_t]$ die Formel sein soll, die man durch Ersetzten von t durch x_t gewinnt. Offensichtlich ist die modifizierte Formel logisch äquivalent zu ψ. Dieser Eliminationsschritt wird solange ausgeführt, bis ψ termreduziert ist. $\square$

Die Pränex-Normalform. Wir betrachten zunächst einige logische Äquivalenzen für einfache Quantorenanwendungen.

Lemma 3.18.

(i) $\exists x(\psi \vee \varphi) \equiv \exists x\psi \vee \exists x\varphi$
$\forall x(\psi \wedge \varphi) \equiv \forall x\psi \wedge \forall x\varphi$

(ii) Falls x nicht frei in ψ vorkommt, gilt:
$\psi \vee \exists x\varphi \equiv \exists x(\psi \vee \varphi)$
$\psi \wedge \exists x\varphi \equiv \exists x(\psi \wedge \varphi)$
$\psi \vee \forall x\varphi \equiv \forall x(\psi \vee \varphi)$
$\psi \wedge \forall x\varphi \equiv \exists x(\psi \wedge \varphi)$

(iii) $\neg\exists x\psi \equiv \forall x\neg\psi$
$\neg\forall x\psi \equiv \forall x\neg\psi$

(iv) $\exists x\exists y\psi \equiv \exists y\exists x\psi$
$\forall x\forall y\psi \equiv \forall y\forall x\psi.$

Wir führen exemplarisch den Beweis für die erste Behauptung in *(ii)* vor. Für jede zu beiden Seiten der Äquivalenz passende Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ gilt:

$$
\begin{aligned}
& \mathfrak{I} \models \psi \vee \exists x\varphi \\
\Longleftrightarrow\quad & \mathfrak{I} \models \psi \text{ oder es gibt ein } a \in A, \text{ so dass } \mathfrak{I}[x/a] \models \varphi \\
\Longleftrightarrow\quad & \text{es gibt ein } a \in A, \text{ so dass } \mathfrak{I}[x/a] \models \psi \text{ oder } \mathfrak{I}[x/a] \models \varphi \\
& (\text{da } x \notin \mathrm{Frei}(\psi) \text{ gilt nach dem Koinzidenzlemma, dass } \mathfrak{I} \models \psi \text{ gdw. } \mathfrak{I}[x/a] \models \psi) \\
\Longleftrightarrow\quad & \text{es gibt ein } a \in A, \text{ so dass } \mathfrak{I}[x/a] \models \psi \vee \varphi \\
\Longleftrightarrow\quad & \mathfrak{I} \models \exists x(\psi \vee \varphi).
\end{aligned}
$$

Man beachte, dass einige zu *(i)* ganz ähnlich aussehende Formelpaare *nicht* äquivalent sind:

$$\exists x(\psi \wedge \varphi) \not\equiv \exists x\psi \wedge \exists x\varphi$$
$$\forall x(\psi \vee \varphi) \not\equiv \forall x\psi \vee \forall x\varphi$$

Weiter ist zu beachten, dass die Äquivalenzen in *(ii)* ohne die Bedingung $x \notin \mathrm{Frei}(\psi)$ im allgemeinen nicht gelten.

Beispiel. Die Formel $\forall x(Px \vee Qx)$ ist weder zu $\forall xPx \vee \forall xQx$ noch zu $Px \vee \forall xQx$ äquivalent.

Wie schon bei Substitutionen sehen wir also, dass wir auf Konflikte zwischen freien und gebundenen Variablen achten müssen. Offensichtlich können wir aber gebundene Variablen umbenennen. Wenn die Variable y in $\exists x\psi$ nicht vorkommt, dann ist nämlich $\exists x\psi \equiv \exists y\psi[x/y]$ Wir nennen eine Formel ψ *bereinigt*, wenn keine Variable in ψ sowohl frei wie gebunden auftritt, und wenn keine Variable mehr als einmal quantifiziert wird. Per Induktion über den Formelaufbau folgt, dass man durch systematisches Umbenennen gebundener Variabeln zu jeder Formel eine äquivalente bereinigte Formel konstruieren kann.

Definition 3.19. Eine Formel ist in *Pränex-Normalform* (PNF), wenn sie bereinigt ist und die Form $Q_1x_1 \cdots Q_rx_r\varphi$ hat, wobei φ quantorenfrei ist und $Q_i \in \{\exists, \forall\}$. Das Anfangsstück $Q_1x_1 \cdots Q_rx_r$ nennt man das *Präfix* der Formel.

Satz 3.20 (Satz über die Pränex-Normalform). *Jede Formel $\psi \in \mathrm{FO}(\tau)$ lässt sich in eine logisch äquivalente Formel in Pränex-Normalform transformieren.*

Beweis. Der Beweis wird per Induktion über den Aufbau von ψ geführt. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass ψ die Junktoren $\rightarrow$ und $\leftrightarrow$ nicht enthält.

(1) Quantorenfreie Formeln sind bereits in PNF.

(2) Sei $\psi = \neg\varphi$. Nach Induktionsvoraussetzung kann φ in eine logisch äquivalente Formel $\varphi' = Q_1x_1 \cdots Q_rx_r\vartheta'$ transformiert werden. Durch wiederholte Anwendung von Lemma 3.18 *(iii)* folgt, dass

$$\psi \equiv \overline{Q_1}x_1 \cdots \overline{Q_r}x_r\neg\vartheta'$$

wobei $\overline{\exists} := \forall$ und $\overline{\forall} := \exists$. Diese Formel hat die gewünschte Form.

(3) Sei $\psi = \varphi_1 \circ \varphi_2$ für $\circ \in \{\vee, \wedge\}$. Nach Induktionsvoraussetzung lassen sich φ_1 und φ_2 in logisch äquivalente Formeln in PNF umformen. Durch Umbennung gebundener Variablen erreichen wir, dass diese Formeln die Form $\varphi_1' = Q_1x_1 \cdots Q_rx_r\vartheta_1$ und $\varphi_2' = Q_1'y_1 \ldots Q_s'y_s\vartheta_2$, wobei $x_1, \ldots, x_r, y_1, \ldots, y_s$ paarweise verschieden und verschieden von allen freien Variablen in φ_1 und φ_2 sind. Sei nun

$$\psi' := Q_1x_1 \cdots Q_rx_rQ_1'y_1 \cdots Q_s'y_s(\vartheta_1' \circ \vartheta_2').$$

Diese Formel hat die gewünschte Form, und da die Variablen $y_1, \ldots, y_s$ nicht in φ_1' und $x_1, \ldots, x_r$ nicht in φ_2' vorkommen, folgt mit Lemma 3.18 *(ii)*, dass $\psi \equiv \psi'$.

(4) Sei $\psi = Qx\varphi$ für $Q \in \{\exists, \forall\}$ und sei $\varphi' := Q_1x_1 \cdots Q_rx_r\vartheta'$ eine zu φ äquivalente Formel in PNF. Durch Umbenennen kann erreicht werden, dass die gebundenen Variablen von φ' von x verschieden sind. Dann ist $Qx\varphi'$ eine zu ψ äquivalente Formel in PNF.

□

Beispiel. Sei $\psi := \neg\forall x\neg Rxx \wedge \forall x\exists y(Rxy \wedge (\neg Ryy \wedge \exists xRyx))$. Die Transformation in eine äquivalente Formel in PNF, gemäss dem im Beweis beschriebenen Verfahren, ergibt

$$\begin{aligned}\psi &\equiv \exists xRxx \wedge \forall x\exists y(Rxy \wedge \exists x(\neg Ryy \wedge Ryx))\\ &\equiv \exists uRuu \wedge \forall x\exists y\exists z(Rxy \wedge (\neg Ryy \wedge Ryz))\\ &\equiv \exists u\forall x\exists y\exists z(Ruu \wedge Rxy \wedge \neg Ryy \wedge Ryz)\end{aligned}$$

Übung 3.2. Geben Sie zu den folgenden Formeln äquivalente Formeln in PNF an:

(a) $\forall x\exists yPxy \vee (\neg Qz \wedge \neg\exists xRxy)$

(b) $\exists yRxy \leftrightarrow \forall xRxx$

Satz 3.21 (Satz über die Skolem-Normalform). *Zu jeder Formel $\psi \in \mathrm{FO}(\sigma)$ lässt sich eine Formel $\varphi \in \mathrm{FO}(\tau)$ mit $\sigma \subseteq \tau$ konstruieren, so dass gilt:*

(i) $\varphi = \forall y_1 \cdots \forall y_s\varphi'$, *wobei φ' quantorenfrei ist;*

(ii) $\mathrm{Frei}(\psi) = \mathrm{Frei}(\varphi)$*;*

(iii) $\varphi \models \psi$*;*

(iv) Zu jedem Modell von ψ existiert eine Expansion, welche Modell von φ ist.

Die letzten beiden Punkte implizieren insbesondere, dass ψ und φ über den selben Universen erfüllbar sind.

Beweis. Nach dem Satz über die Pränex-Normalform können wir ohne Beschränkung der Allgemeinheit annehmen, dass $\psi = Q_1 x_1 \dots Q_r x_r \vartheta$ mit ϑ quantorenfrei. Wir eliminieren Existenzquantoren schrittweise von aussen nach innen durch folgenden Algorithmus. Sei Q_{k+1} der vorderste Existenzquantor. Die gegebene Formel hat also die Form

$$\psi = \forall x_1 \dots \forall x_k \exists x_{k+1} \eta.$$

Sei f ein neues, d.h. nicht in ψ vorkommendes, k-stelliges Funktionssymbol (für $k = 0$ also ein Konstantensymbol). Setze

$$\psi' := \forall x_1 \cdots \forall x_k \eta[x_{k+1}/f x_1 \cdots x_k].$$

Offensichtlich liefert die Iteration dieses Eliminationsschrittes schliesslich eine Formel der gewünschten syntaktischen Gestalt. Zu zeigen bleibt, dass $\psi' \models \psi$ und dass jedes Modell von ψ zu einem Modell von ψ' expandiert werden kann.

Zur ersten Behauptung nehmen wir an, dass

$$\mathfrak{I} = (\mathfrak{A}, \beta) \models \psi' := \forall x_1 \cdots \forall x_k \eta[x_{k+1}/f x_1 \cdots x_k].$$

Also folgt, dass für alle $a_1, \dots, a_k \in A$,

$$\mathfrak{I}[x_1/a_1, \dots, x_k/a_k] \models \eta[x_{k+1}/f x_1 \cdots x_k].$$

Nach dem Substitutionslemma bedeutet dies, für $b := f^{\mathfrak{A}}(a_1, \dots, a_k)$, dass

$$\mathfrak{I}[x_1/a_1, \dots, x_k/a_k, x_{k+1}/b] \models \eta.$$

Damit ist gezeigt, dass $\mathfrak{I} \models \forall x_1 \cdots \forall x_k \exists x_{k+1} \eta$, also $\mathfrak{I} \models \psi$.

Zur zweiten Behauptung nehmen wir an, dass $(\mathfrak{A}, \beta) \models \psi$. Da f in ψ nicht vorkommt, können wir annehmen, dass f nicht in der Signatur von $\mathfrak{A}$ enthalten ist. Wir definieren eine Expansion $\mathfrak{B} = (\mathfrak{A}, f^{\mathfrak{B}})$ von $\mathfrak{A}$, so dass $(\mathfrak{B}, \beta) \models \psi'$.

Da $(\mathfrak{A}, \beta) \models \forall x_1 \cdots \forall x_k \exists x_{k+1} \eta$ gibt es für alle $a_1, \dots, a_k$ ein b, so dass

$$(\mathfrak{A}, \beta)[x_1/a_1, \dots, x_k/a_k, x_{k+1}/b] \models \eta.$$

Wir wählen nun für jedes Tupel $(a_1, \dots, a_k)$ ein solches b und setzen $f^{\mathfrak{B}}(a_1, \dots, a_k) := b$. Offensichtlich gilt also für alle $a_1, \dots, a_k$, dass

$$(\mathfrak{B}, \beta)[x_1/a_1, \dots, x_k/a_k, x_{k+1}/f^{\mathfrak{B}}(a_1, \dots, a_k)] \models \eta,$$

also nach dem Substitutionslemma auch

$$(\mathfrak{B}, \beta)[x_1/a_1, \dots, x_k/a_k] \models \eta[x_{k+1}/f x_1 \cdots x_k].$$

Damit ist gezeigt, dass $(\mathfrak{B}, \beta) \models \forall x_1 \cdots \forall x_k \eta[x_{k+1}/f x_1 \cdots x_k]$ und daher ψ' erfüllbar ist.
□

Übung 3.3. (Relationale Skolem-Normalform) Zeigen Sie, dass zu jeder Formel $\psi \in \mathrm{FO}(\sigma)$ eine *relationale* Formel $\varphi \in \mathrm{FO}(\tau)$ der Gestalt $\forall x_1 \cdots \forall x_r \exists y_1 \cdots \exists y_s \eta$ mit quantorenfreiem η existiert, so dass ψ und φ über den selben Universen erfüllbar sind.

3.5 Spieltheoretische Semantik

> Der Mensch spielt nur,
> wo er in voller Bedeutung des Wortes Mensch ist,
> und er ist nur da ganz Mensch, wo er spielt.
>
> Friedrich Schiller, Über die ästhetische Erziehung des Menschen

> Nessuno ha mai sostenuto seriamente che i giochi siano inutili.
>
> Umberto Eco

Die Semantik der Prädikatenlogik kann man auch spieltheoretisch formulieren. Eine FO-Formel ψ und eine dazu passende Interpretation $\mathfrak{I}$ definieren ein *Auswertungsspiel* $\mathrm{MC}(\mathfrak{I}, \psi)$ zwischen zwei Spielern, der *Verifiziererin* V und dem *Falsifizierer* F. Die Verifiziererin möchte zeigen, dass $\mathfrak{I}$ ein Modell für ψ ist, der Falsifizierer möchte nachweisen, dass dies nicht der Fall ist.

Der Einfachheit halber nehmen wir hier an, dass ψ in Negationsnormalform ist. Die gegebene Interpretation sei $\mathfrak{I} = (\mathfrak{A}, \beta_0)$. Die Struktur $\mathfrak{A}$ bleibt während der gesamten Partie gleich, die Bewertung und die Formel werden verändert. Die Positionen des Spiels sind also Paare (φ, β) bestehend aus einer Unterformel φ von ψ und einer Bewertung $\beta : \mathrm{Frei}(\varphi) \to A$.

Das Spiel beginnt bei der Position (ψ, β_0). Sei (φ, β) die aktuelle Position. Dann geht das Spiel, abhängig von der Gestalt von φ, wie folgt weiter:

- Wenn φ ein Literal ist, dann ist das Spiel beendet. Die Verifiziererin hat gewonnen, falls $\mathfrak{A} \models \varphi[\beta]$, andernfalls hat der Falsifizierer gewonnen.
- An einer Position $(\vartheta \vee \eta, \beta)$ ist die Verifiziererin am Zug und kann entweder zu (ϑ, β) oder zu (η, β) ziehen.
- Analog zieht von einer Position $(\vartheta \wedge \eta, \beta)$ der Falsifizierer entweder zu (ϑ, β) oder zu (η, β).
- An einer Position der Form $(\exists x \vartheta, \beta)$ wählt die Verifiziererin ein Element $a \in A$ und zieht zu $(\vartheta, \beta[x/a])$.
- Entsprechend darf an einer Position der Form $(\forall x \vartheta, \beta)$ der Falsifizierer ein Element $a \in A$ auswählen und zur Position $(\vartheta, \beta[x/a])$ ziehen.

Etwas allgemeiner ist ein solches Spiel beschrieben durch einen Spielgraphen

$$G = (P, Z, p_0),$$

bestehend aus folgenden Objekten.

- $P = P_V \cup P_F \cup W_V \cup W_F$ ist die Menge der Positionen, welche disjunkt zerlegt ist in die Mengen P_V bzw. P_F der Positionen, an denen V bzw. F am Zug ist, und in die Mengen der Gewinnpositionen W_V und W_F für die Spieler V und F.
- Die Menge der möglichen Züge ist $Z \subseteq (P_V \cup P_F) \times P$ wobei vorausgesetzt wird, dass für jede Position $p \in P_V \cup P_F$ mindestens ein Zug $(p, p') \in Z$ existiert.
- p_0 ist die Anfangsposition.

Eine *Partie* ist ein endlicher oder unendlicher Pfad $(p_0, p_1, \ldots, p_m)$ bzw. $(p_0, p_1, \ldots)$ so dass $(p_{i-1}, p_i) \in Z$ für alle $i > 0$ und $p_m \in W_V \cup W_F$. Die Positionen in $W_V \cup W_F$ heissen Endpositionen.

In unserem Fall ist das Spiel *fundiert*, d.h. alle Partien sind endlich (da jeder Zug die Komplexität der Formel reduziert). Eine Strategie für Spielerin V von Position p aus ist beschrieben durch einen Untergraphen $S = (P_S, Z_S)$ von (P, Z) wobei $P_S \subseteq P$ die Menge der S-erreichbaren Positionen und $Z_S \subseteq Z \cap (P_S \times P_S)$ die Menge der mit S verträglichen Züge beschreibt. Die folgenden Bedingungen müssen dabei erfüllt sein:

(1) $p \in P_S$

(2) Wenn $p' \in P_S \cap P_V$, dann existiert mindestens ein Zug $(p', p'') \in Z_S$.

(3) Wenn $p' \in P_S \cap P_F$, dann gilt für alle Züge $(p', p'') \in Z$, dass $(p', p'') \in Z_S$ (und daher auch $p'' \in P_S$).

Eine Gewinnstrategie für V von p ist eine Strategie S, so dass alle erreichbaren Endpositionen in W_V liegen. (Gewinn-)Strategien für F werden analog definiert.

Übung 3.4. Zeigen Sie, dass in einem fundierten Spiel dieser Art von jeder Position aus genau einer der beiden Spieler eine Gewinnstrategie besitzt.

Satz 3.22. *Für jede* FO*-Formel ψ und jede dazu passende Interpretation $\mathfrak{I}$ gilt: $\mathfrak{I} \models \psi$ genau dann, wenn die Verifiziererin eine Gewinnstrategie für das Spiel* $\mathrm{MC}(\mathfrak{I}, \psi)$ *hat,*

Beweis. Sei $\mathfrak{I} = (\mathfrak{A}, \beta_0)$ Wir zeigen, dass in dem Spiel $\mathrm{MC}(\mathfrak{I}, \psi)$ die Verifiziererin eine Gewinnstrategie von Position (φ, β) hat, wenn $(\mathfrak{A}, \beta) \models \varphi$, und dass der Falsifizierer eine Gewinnstrategie von Position (φ, β) hat, wenn $(\mathfrak{A}, \beta) \models \neg\varphi$.

Definiere in dem Spiel die Strategien $S^+ = (P^+, Z^+)$ und $S^- = (P^-, Z^-)$ wie folgt:

$$P^+ := \{(\varphi, \beta) : (\mathfrak{A}, \beta) \models \varphi\} \qquad Z^+ := Z \cap (P^+ \times P^+)$$
$$P^- := \{(\varphi, \beta) : (\mathfrak{A}, \beta) \models \neg\varphi\} \qquad Z^- := Z \cap (P^- \times P^-).$$

Es reicht zu überprüfen, dass S^+ tatsächlich eine Strategie für V und S^- eine Strategie für F ist. Da offensichtlich $W_V \subseteq P^+$, $W_F \subseteq P^-$ und P die disjunkte Vereinigung von P^+ und P^- ist, sind S^+ und S^- dann Gewinnstrategien für V bzw. F.

Wir zeigen, dass S^+ eine Strategie für V ist.

- Sei (φ, β) eine Position in P^+ an der V am Zug ist. Dann gilt $(\mathfrak{A}, \beta) \models \varphi$ und entweder $\varphi = (\vartheta \vee \eta)$ oder $\varphi = \exists x \vartheta$. Zu zeigen ist, dass V einen Zug (gemäss Strategie S^+) zu einer Position in P^+ machen kann. Wenn $\varphi = \vartheta \vee \eta$, dann gilt entweder $(\mathfrak{A}, \beta) \models \vartheta$ oder $(\mathfrak{A}, \beta) \models \eta$, also kann V zu (mindestens) einer der Positionen (ϑ, β) oder (η, β) ziehen. Wenn $\varphi = \exists x \vartheta$, dann existiert ein $a \in A$, so dass $(\mathfrak{A}, \beta[x/a]) \models \vartheta$. Also kann V zu der Position $(\vartheta, \beta[x/a])$ ziehen.

- Sei (φ, β) eine Position in P^+ an der F am Zug ist. Dann gilt $(\mathfrak{A}, \beta) \models \varphi$ und entweder $\varphi = (\vartheta \wedge \eta)$ oder $\varphi = \forall x \vartheta$. Zu zeigen ist, dass jeder Zug von (φ, β) wieder zu einer Position in P^+ führt. Wenn $\varphi = \vartheta \wedge \eta$, dann gilt $(\mathfrak{A}, \beta) \models \vartheta$ und $(\mathfrak{A}, \beta) \models \eta$, also führt jeder der beiden möglichen Züge von F zu einer Position in P^+. Wenn $\varphi = \forall x \vartheta$, dann gilt $(\mathfrak{A}, \beta[x/a]) \models \vartheta$ für alle $a \in A$. Also ist jede Position $(\vartheta, \beta[x/a])$ zu der F ziehen kann, wieder eine Position in P^+.

Die Argumente, dass S^- eine Strategie für F ist, sind völlig analog. □

Übung 3.5. Geben sie einen Algorithmus an, der zu jedem endlichen Spielgraphen $G = (P, Z, p_0)$ in Zeit $O(|P| + |Z|)$ berechnet, ob Spieler V für das Spiel G eine Gewinnstrategie hat.

Übung 3.6. (Auswertung von FO **auf endlichen Strukturen)** Konstruieren Sie (auf der Basis des Auswertungsspiels) einen möglichst effizienten Auswertungsalgorithmus für FO-Sätze auf endlichen Strukturen. Schätzen Sie die Laufzeit und den Speicherbedarf des Algorithmus ab, abhängig von der Grösse der gegebenen Struktur und der Länge (oder Komplexität) des gegebenen Satzes.

Übung 3.7. Formulieren Sie ein Auswertungsspiel für FO-Formeln, welche nicht notwendigerweise in Negationsnormalform sind. Welcher spieltheoretischen Operation entspricht die Negation?

Kapitel 4

Modallogik

Modale und temporale Logiken sind geeignete logische Systeme, um Aussagen über Transitionssysteme zu formalisieren. Sie bieten ein gutes Gleichgewicht zwischen vernünftiger Ausdrucksstärke und günstigen algorithmischen Eigenschaften. Dies macht sie für Anwendungen in der Informatik sehr interessant.

Modallogiken formalisieren Aussagen über Transitionssysteme von einer internen, lokalen Perspektive her.

4.1 Syntax und Semantik der Modallogik

Die Modallogik erweitert die Aussagenlogik um einstellige Modaloperatoren, mit welchen man aus einer Formel ψ neue Formeln der Form $\langle a\rangle\psi$ bzw. $[a]\psi$ bildet, für all a aus einer Menge von *Aktionen*.

Definition 4.1. Die Menge ML der modallogischen Formeln (mit Aktionen aus A und atomaren Eigenschaften P_i (für $i \in I$) ist induktiv definiert wie folgt:

- Alle aussagenlogischen Formeln mit Aussagenvariablen P_i gehören zu ML.
- Wenn $\psi, \varphi \in$ ML, dann auch $\neg\psi$, $(\psi \vee \varphi)$, $(\psi \wedge \varphi)$ und $(\psi \rightarrow \varphi)$.
- Wenn $\psi \in$ ML und $a \in A$, dann gehören auch $\langle a\rangle\psi$ und $[a]\psi$ zu ML.

Bemerkung. Wenn nur eine Aktion a vorhanden ist, also $|A| = 1$, dann schreiben wir $\Diamond\psi$ (sprich "Diamond ψ" oder "möglicherweise ψ") und $\Box\psi$ (sprich "Box ψ" oder notwendigerweise ψ") anstelle von $\langle a\rangle\psi$ und $[a]\psi$.

Definition 4.2. Ein *Transitionssystem* oder eine *Kripkestruktur* mit Aktionen aus A und atomaren Eigenschaften $\{P_i : i \in I\}$ ist eine Struktur

$$\mathcal{K} = (V, (E_a)_{a\in A}, (P_i)_{i\in I})$$

mit Universum V (dessen Elemente Zustände oder Welten genannt werden), zweistelligen Relationen $E_a \subseteq V \times V$ $(a \in A)$ (welche Transitionen zwischen Zuständen beschreiben) und einstelligen Relationen (Eigenschaften der Zustände) $P_i \subseteq V$ $(i \in I)$. Statt $(u, v) \in E_a$ schreiben wir oft auch $u \xrightarrow{a} v$.

Man kann sich ein Transitionssystem als einen Graphen mit beschrifteten Knoten und Kanten vorstellen. Die Elemente des Universums sind Knoten, die einstelligen Relationen entsprechen den Beschriftungen der Knoten und die zweistelligen Relationen den beschrifteten Kanten.

Definition 4.3. Sei $\mathcal{K} = (V, (E_a)_{a \in A}, (P_i)_{i \in I})$ ein Transitionssystem, $\psi \in$ ML eine Formel und v ein Zustand von $\mathcal{K}$. Die *Modellbeziehung* $\mathcal{K}, v \models \psi$ (d.h. ψ gilt im Zustand v von $\mathcal{K}$) ist induktiv wie folgt definiert:

(1) $\mathcal{K}, v \models P_i$ genau dann, wenn $v \in P_i$.

(2) Die Bedeutungen von $\neg\psi$, $(\psi \wedge \varphi), (\psi \vee \varphi)$ und $(\psi \rightarrow \varphi)$ sind wie üblich.

(3) $\mathcal{K}, v \models \langle a \rangle \psi$, wenn ein w existiert mit $(v, w) \in E_a$ und $\mathcal{K}, w \models \psi$.

(4) $\mathcal{K}, v \models [a]\psi$ genau dann, wenn für alle w mit $(v, w) \in E_a$ gilt, dass $\mathcal{K}, w \models \psi$.

Wie schon eingangs erwähnt, haben wir hier im Gegensatz zu FO eine lokale Sichtweise der Modellbeziehung. Von einem bestimmten Zustand v ausgehend, wird eine Formel ψ an diesem v evaluiert. Die Modaloperatoren $\langle a \rangle$ und $[a]$ können als eingeschränkte Varianten der Quantoren $\exists$ und $\forall$ (Quantifizierung entlang von Transitionen) gesehen werden.

Wir können auch jeder Formel ψ und jedem Transitionssystem $\mathcal{K}$ die Extension

$$[\![\psi]\!]^{\mathcal{K}} := \{v : \mathcal{K}, v \models \psi\}$$

zuordnen, also die Menge der Zustände v, an denen ψ in $\mathcal{K}$ gilt. Die Modellbeziehung ist dann durch folgende Regeln gegeben (welche natürlich zu den in Definition 4.3 gegeben Regeln äquivalent sind):

(1) $[\![P_i]\!]^{\mathcal{K}} = P_i$.

(2) $[\![\neg\psi]\!]^{\mathcal{K}} := V - [\![\psi]\!]^{\mathcal{K}}$
$[\![\psi \wedge \varphi]\!]^{\mathcal{K}} := [\![\psi]\!]^{\mathcal{K}} \cap [\![\varphi]\!]^{\mathcal{K}}$
$[\![\psi \vee \varphi]\!]^{\mathcal{K}} := [\![\psi]\!]^{\mathcal{K}} \cup [\![\varphi]\!]^{\mathcal{K}}$
$[\![\psi \rightarrow \varphi]\!]^{\mathcal{K}} := (V - [\![\psi]\!]^{\mathcal{K}}) \cup [\![\varphi]\!]^{\mathcal{K}}$.

(3) $[\![\langle a \rangle \psi]\!]^{\mathcal{K}} := \{v : vE_a \cap [\![\psi]\!]^{\mathcal{K}} \neq \varnothing\}$.

(4) $[\![[a]\psi]\!]^{\mathcal{K}} := \{v : vE_a \subseteq [\![\psi]\!]^{\mathcal{K}}\}$.

Dabei ist $vE_a := \{w : (v, w) \in E_a\}$ die Menge aller a-Nachfolger von v.

Einbettung der Modallogik in die Prädikatenlogik. Formal ist die Modallogik eine Erweiterung der Aussagenlogik. Oft ist es aber weitaus zweckmässiger, ML in die Prädikatenlogik zu übersetzen und sie damit als Fragment von FO aufzufassen. Dies liegt schon deshalb nahe, weil die Modallogik über Transitionssysteme, also Strukturen, spricht.

Die folgende Übersetzung zeigt, dass man dabei mit FO-Formeln auskommt, die nur zwei Variablen x und y (diese allerdings mehrfach quantifiziert) verwenden.

Definition 4.4. FO^2, das *Zwei-Variablen-Fragment* von FO, ist die Menge aller relationalen FO-Formeln, welche nur zwei Variablen x und y enthalten.

Beispiel. Wir wollen ausdrücken, dass es (in einem gegebenen Transitionsystem) vom aktuellen Zustand x aus einen a-Pfad der Länge 5 zu einem Zustand gibt, der in der Menge P liegt. In ML wird dies durch die Formel $\langle a\rangle\langle a\rangle\langle a\rangle\langle a\rangle\langle a\rangle P$ formalisiert. Die naheliegendste Weise, dieselbe Aussage in FO auszudrücken, führt zu der Formel

$$\psi(x) := \exists y_1 \cdots \exists y_5 (E_a x y_1 \wedge \bigwedge_{i=1}^{5} E_a y_i y_{i+1} \wedge P y_5),$$

welche sechs Variabeln vewendet. Wir können aber denselben Sachverhalt auch mit nur zwei Variablen ausdrücken, durch die Formel

$$\psi'(x) := \exists y(Exy \wedge \exists x(Eyx \wedge \exists y(Exy \wedge \exists x(Eyx \wedge \exists y(Exy \wedge Py))))).$$

Satz 4.5. *Zu jeder Formel $\psi \in$ ML gibt es eine Formel $\psi^*(x)$ in FO^2, so dass für alle Transitionssysteme $\mathcal{K}$ und alle Zustände v von $\mathcal{K}$ gilt:*

$$\mathcal{K}, v \models \psi \iff \mathcal{K} \models \psi^*(v).$$

Beweis. Wir geben eine Tabelle an, nach der jede Formel $\psi \in$ ML induktiv in eine Formel $\psi^*(x) \in \mathrm{FO}^2$ übersetzt werden kann. Mit $\psi^*(y)$ sei hier die Formel bezeichent, die man aus $\psi^*(x)$ erhält indem man alle (freien und gebundenen) Vorkommen von x durch y ersetzt, und umgekehrt.

$\psi \in$ ML	$\longmapsto$	$\psi^*(x) \in \mathrm{FO}^2$
P_i	$\longmapsto$	$P_i x$
$\neg\psi$	$\longmapsto$	$\neg\psi^*(x)$
$(\psi \circ \varphi)$	$\longmapsto$	$(\psi^*(x) \circ \varphi^*(x))$ für $\circ \in \{\wedge, \vee, \rightarrow\}$
$\langle a\rangle\psi$	$\longmapsto$	$\exists y(E_a xy \wedge \psi^*(y))$
$[a]\psi$	$\longmapsto$	$\forall y(E_a xy \rightarrow \psi^*(y))$.

$\square$

Erfüllbarkeit, Gültigkeit, Äquivalenz. Analog zu Aussagenlogik und Prädikatenlogik definieren wir: Eine Formel $\psi \in$ ML ist *erfüllbar*, wenn ein Transitionssystem $\mathcal{K}$ und ein Zustand v von $\mathcal{K}$ existiert, so dass $\mathcal{K}, v \models \psi$. Sie ist *gültig*, wenn $\mathcal{K}, v \models \psi$ für alle $\mathcal{K}$ und alle v. Zwei Formeln ψ, φ sind *äquivalent*, kurz $\psi \equiv \varphi$, wenn $[\![\psi]\!]^{\mathcal{K}} = [\![\varphi]\!]^{\mathcal{K}}$ für alle zu ψ und φ passenden Transitionssysteme $\mathcal{K}$.

Beispiel. Für alle Formeln $\psi \in$ ML und alle Aktionen a gilt:

(1) $\langle a\rangle\psi \rightarrow [a]\psi$ ist erfüllbar, aber nicht gültig.

(2) $[a](\psi \rightarrow \varphi) \rightarrow ([a]\psi \rightarrow [a]\varphi)$ ist gültig.

(3) $[a]\psi \equiv \neg\langle a\rangle\neg\psi$ (Dualität von $\langle a\rangle$ und $[a]$).

Negationsnormalform. Wie für Aussagenlogik und Prädikatenlogik gibt es auch für die Modallogik Normalformen. Nützlich ist insbesondere die Negationsnormalform. Jede Formel $\psi \in$ ML ist äquivalent zu einer Formel, in der die Negation nur auf atomare Eigenschaften P_i angewandt wird. Dies folgt unmittelbar aus den de Morganschen Gesetzen und der Dualität von $\langle a\rangle$ und $[a]$.

Übung 4.1. Gilt für ML das Analogon des Satzes über die Pränex-Normalform?

4.2 Bisimulation

Einer der wichtigsten Begriffe bei der Analyse von Modallogiken ist die Bisimulation. Mit ihr wollen wir die Ununterscheidbarkeit von Kripkestrukturen bezüglich Formeln aus ML untersuchen.

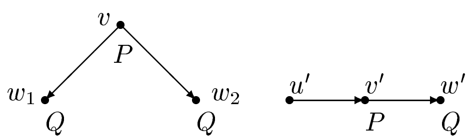
Definition 4.6. Seien $\mathcal{K} = (V, (E_a)_{a\in A}, (P_i)_{i\in I})$ und $\mathcal{K}' = (V', (E'_a)_{a\in A}, (P'_i)_{i\in I})$ Transitionssysteme. Eine *Bisimulation* zwischen $\mathcal{K}$ und $\mathcal{K}'$ ist eine Relation $Z \subseteq V \times V'$, so dass für alle $(v, v') \in Z$ gilt:

(1) $v \in P_i \Longleftrightarrow v' \in P'_i$ für alle $i \in I$.

(2) **Hin:** Für alle $a \in A$, $w \in V$ mit $v \xrightarrow{a} w$ existiert ein $w' \in V'$ mit $v' \xrightarrow{a} w'$ und es ist $(w, w') \in Z$.

Her: Für alle $a \in A$, $w' \in V'$ mit $v' \xrightarrow{a} w'$ existiert ein $w \in V$ mit $v \xrightarrow{a} w$ und es ist $(w, w') \in Z$.

Beispiel.



$Z = \{(v, v'), (w_1, w'), (w_2, w')\}$ ist eine Bisimulation.

Definition 4.7. Seien $\mathcal{K}, \mathcal{K}'$ Kripkestrukturen und $u \in V$, $u' \in V'$. $(\mathcal{K}, u)$ und $(\mathcal{K}', u')$ sind *bisimilar* (kurz: $\mathcal{K}, u \sim \mathcal{K}', u'$), wenn eine Bisimulation Z zwischen $\mathcal{K}$ und $\mathcal{K}'$ existiert, so dass $(u, u') \in Z$.

Das Bisimulationsspiel. Die Bisimililarität zweier Transitionssysteme kann auch auf spieltheoretische Weise, durch ein Bisimulationsspiel, beschrieben werden. Das Spiel wird von zwei Spielern auf zwei Kripkestrukturen $\mathcal{K}$ und $\mathcal{K}'$, auf denen sich je ein Spielstein befindet, gespielt. In der Anfangsposition liegen die Steine auf u bzw. u'. Die Spieler ziehen nun abwechselnd nach folgenden Regeln:

Spieler I bewegt den Stein in $\mathcal{K}$ oder $\mathcal{K}'$ entlang einer Transition zu einem neuem Zustand: von v entlang $v \xrightarrow{a} w$ zu w oder von v' entlang $v' \xrightarrow{a} w'$ zu w'. Spielerin II antwortet mit einer entsprechenden Bewegung in der anderen Struktur: $v' \xrightarrow{a} w'$ oder $v \xrightarrow{a} w$. Wenn ein Spieler nicht ziehen kann, verliert er. D.h. Spieler I verliert, wenn er zu einem Knoten kommt, von dem keine Transitionen mehr wegführen und Spielerin II verliert, wenn sie nicht mehr mit der entsprechenden Aktion antworten kann. Am Anfang und nach jedem Zug wird überprüft, ob für die aktuelle Position v, v' gilt: $v \in P_i \leftrightarrow v' \in P'_i$ für alle $i \in I$. Wenn nicht, dann hat I gewonnen, ansonsten geht das Spiel weiter. II gewinnt, wenn sie nie verliert.

Uns interessieren nicht primär einzelne Partien, sondern ob einer der Spieler eine Gewinnstrategie hat. Wir sagen, II gewinnt das Bisimulationsspiel auf $(\mathcal{K}, \mathcal{K}')$ von (u, u') aus, wenn es eine Strategie für II gibt mit der sie nie verliert, was auch immer I zieht. Eine derartige Strategie entspricht genau einer Bisimulation. Also gilt:

Lemma 4.8. *II gewinnt das Bisimulationsspiel auf $\mathcal{K}, \mathcal{K}'$ von (u, u') aus genau dann, wenn $\mathcal{K}, u \sim \mathcal{K}', u'$.*

Wir können die Analyse noch etwas verfeinern, wenn wir die Anzahl der Züge in einem Bisimulationsspiel in Betracht ziehen. Wir sagen, II gewinnt das n-Züge-Bisimulationsspiel, wenn sie eine Strategie hat, um n Züge lang zu spielen ohne zu verlieren. Analog dazu betrachten wir den Begriff der *n-Bisimilarität*, kurz $\sim_n$. Es seien $\mathcal{K}$ und $\mathcal{K}'$ zwei Kripkestrukturen mit Zuständen v bzw. v'.

- $\mathcal{K}, v \sim_0 \mathcal{K}', v'$ genau dann, wenn für alle $i \in I$ gilt: $v \in P_i \leftrightarrow v' \in P_i'$.
- $\mathcal{K}, v \sim_{n+1} \mathcal{K}', v'$ genau dann, wenn
  - $\mathcal{K}, v \sim_n \mathcal{K}', v'$
  - für alle w mit $v \xrightarrow{a} w$ existiert ein w' mit $v' \xrightarrow{a} w'$ mit $\mathcal{K}, w \sim_n \mathcal{K}', w'$
  - für alle w' mit $v' \xrightarrow{a} w'$ existiert ein w mit $v \xrightarrow{a} w$ mit $\mathcal{K}, w \sim_n \mathcal{K}', w'$.

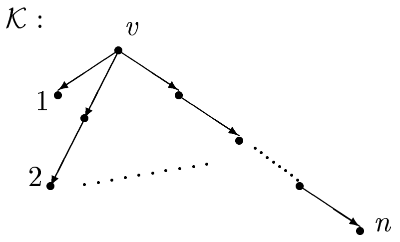
Für alle $n \in \mathbb{N}$ sind nun folgende Aussagen äquivalent:

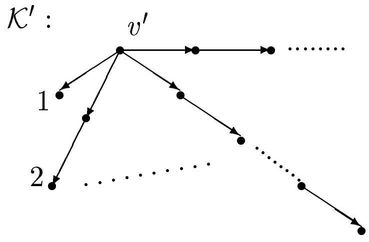
(i) II gewinnt das n-Züge-Bisimulationsspiel von (v, v') aus

(ii) $\mathcal{K}, v \sim_n \mathcal{K}', v'$

Satz 4.9. *Für alle Kripkestrukturen $\mathcal{K}, \mathcal{K}'$ mit Zuständen v bzw. v' gilt: Wenn $\mathcal{K}, v \sim \mathcal{K}, v$, dann ist $\mathcal{K}, v \sim_n \mathcal{K}', v'$ für alle n. Die Umkehrung gilt jedoch nicht: es gibt $\mathcal{K}, v$ und $\mathcal{K}, v'$ so dass $\mathcal{K}, v \sim_n \mathcal{K}', v'$, aber $\mathcal{K}, v \not\sim \mathcal{K}', v'$.*

Beweis. Die erste Behauptung folgt unmittelbar aus den Definitionen. Für die zweite Behauptung betrachten wir folgende Kripkestrukturen:





$\mathcal{K}$ besitzt von v aus für jedes $n \in \mathbb{N}$ einen Pfad der Länge n. $\mathcal{K}'$ setzt sich aus $\mathcal{K}$ und einem unendlichen Pfad, der von v' ausgeht, zusammen. Es ist $\mathcal{K}, v \sim_n \mathcal{K}', v'$ für alle $n \in \mathbb{N}$, aber $\mathcal{K}, v \not\sim \mathcal{K}', v'$. Spielt nämlich I entlang des unendlichen Pfades von $\mathcal{K}'$, dann muß II einen endlichen Pfad in $\mathcal{K}$ auswählen und auf diesem ziehen. Ist eine bestimmte Anzahl n von Zügen vor dem Spiel festgelegt worden, so kann II immer einen Pfad finden, der länger ist als n und somit n-Züge spielen ohne zu verlieren. Ist keine feste Zugzahl ausgemacht worden, so verliert II nach endlich vielen Zügen. □

Bisimulationsinvarianz von modallogischen Formeln. Die grundlegende Bedeutung von Bisimilationen kommt daher, dass modallogische Formeln bisimilare Zustände nicht unterscheiden können. Eine verfeinerte Analyse zieht auch die Modaltiefe, d.h. die maximale Schachtelungstiefe von Modaloperatoren in einer Formel, in Betracht.

Definition 4.10. Die *Modaltiefe* einer Formel $\psi \in \mathrm{ML}$ ist induktiv definiert definiert durch

(1) $\mathrm{md}(\psi) = 0$ für ussagenlogische Formeln ψ,

(2) $\mathrm{md}(\neg\psi) = md(\psi)$,

(3) $\mathrm{md}(\psi \circ \varphi) = \max(\mathrm{md}(\psi), \mathrm{md}(\varphi))$ für $\circ \in \{\wedge, \vee, \rightarrow\}$,

(4) $\mathrm{md}(\langle a\rangle\psi) = \mathrm{md}([a]\psi) = \mathrm{md}(\psi) + 1$.

Definition 4.11. Seien $\mathcal{K}$ und $\mathcal{K}'$ zwei Kripkestrukturen und $v \in \mathcal{K}$, $v' \in \mathcal{K}'$.

(1) $\mathcal{K}, v \equiv_{\mathrm{ML}} \mathcal{K}', v'$, wenn für alle $\psi \in \mathrm{ML}$ gilt: $\mathcal{K}, v \models \psi \iff \mathcal{K}', v' \models \psi$.

(2) $\mathcal{K}, v \equiv^n_{\mathrm{ML}} \mathcal{K}', v'$, wenn für alle $\psi \in \mathrm{ML}$ mit $\mathrm{md}(\psi) \leq n$ gilt: $\mathcal{K}, v \models \psi \iff \mathcal{K}', v' \models \psi$.

Satz 4.12. *Für Kripkestrukturen $\mathcal{K}$, $\mathcal{K}'$ und $u \in \mathcal{K}$, $u' \in \mathcal{K}'$ gilt:*

(1) $\mathcal{K}, u \sim \mathcal{K}', u' \implies \mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'$.

(2) $\mathcal{K}, u \sim_n \mathcal{K}', u' \implies \mathcal{K}, u \equiv^n_{\mathrm{ML}} \mathcal{K}', u'$.

Beweis. Wir beweisen nur die erste Aussage, der Beweis der zweiten ist analog (per Induktion nach n).

Sei Z eine Bisimulation zwischen $\mathcal{K}$ und $\mathcal{K}'$. Wir behaupten, dass für alle $\psi \in \mathrm{ML}$ gilt:

$$\mathcal{K}, v \models \psi \iff \mathcal{K}', v' \models \psi \text{ für alle } (v, v') \in Z.$$

Wir beweisen dies per Induktion über den Formelaufbau von ψ. Für $\psi = P_i$ ist die Behauptung nach Definition einer Bisimulation erfüllt. Für die Fälle $\psi = \neg\varphi$, $\psi = (\varphi \vee \vartheta)$ und $\psi = (\varphi \wedge \vartheta)$ ist der Induktionsschritt offensichtlich: Wenn die Teilformeln von ψ auf $(\mathcal{K}, v)$ und $(\mathcal{K}, v')$ denselben Wahrheitswert haben, dann auch ψ selbst. Sei $\psi = \langle a\rangle\varphi$. Aus $\mathcal{K}, v \models \langle a\rangle\varphi$ folgt $\mathcal{K}, w \models \varphi$ für ein $w \in \mathcal{K}$ mit $v \xrightarrow{a} w$. Nach der Hin-Eigenschaft von Z existiert ein $w' \in \mathcal{K}'$ mit $v' \xrightarrow{a} w'$ und $(w, w') \in Z$. Nach Induktionsvoraussetzung gilt $\mathcal{K}', w' \models \varphi$, also $\mathcal{K}', v' \models \langle a\rangle\varphi$. Die Umkehrung folgt analog mit der Her-Eigenschaft. $\psi = [a]\varphi$ brauchen wir wegen der Dualität $\langle a\rangle\varphi \equiv \neg[a]\neg\varphi$ nicht zu betrachten. ☐

Die Aussage (1) nennt man die *Bisimulationsinvarianz der Modallogik*:

$$\text{Wenn } \mathcal{K}, v \models \psi \text{ und } \mathcal{K}, v \sim \mathcal{K}', v', \text{ dann auch } \mathcal{K}', v' \models \psi.$$

Die Umkehrung von (1) gilt im Allgemeinen **nicht**. Um dies einzusehen, betrachten wir wieder die Kripkestrukturen $\mathcal{K}, \mathcal{K}'$ aus dem Beweise von Satz 4.9. Da $\mathcal{K}, v \sim_n \mathcal{K}'v'$ gilt $\mathcal{K}, v \equiv^n_{\mathrm{ML}} \mathcal{K}', v'$ für alle $n \in \mathbb{N}$ und daher $\mathcal{K}, v \equiv_{\mathrm{ML}} \mathcal{K}', v'$, obwohl $\mathcal{K}, v \not\sim \mathcal{K}', v'$.

Es gibt jedoch wichtige Spezialfälle, in denen die Umkehrung doch gilt.

Definition 4.13. Ein Transitionssystem ist *endlich verzweigt*, wenn für alle Zustände v und alle Aktionen a die Menge $vE_a := \{w : (v, w) \in E_a\}$ der a-Nachfolger von v endlich ist. Insbesondere ist natürlich jedes endliche Transitionssystem endlich verzweigt.

Satz 4.14. *Seien $\mathcal{K}, \mathcal{K}'$ endlich verzweigte Transitionssysteme. Dann ist*

$$\mathcal{K}, u' \sim \mathcal{K}', u' \iff \mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'.$$

Beweis. Sei $\mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'$. Wir setzen $Z := \{(v, v') : \mathcal{K}, v \equiv_{\mathrm{ML}} \mathcal{K}', v'\}$. Dabei folgt sofort aus der Voraussetzung $\mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'$, dass $(u, u') \in Z$. Wir zeigen, dass Z eine Bisimulation zwischen $\mathcal{K}$ und $\mathcal{K}'$ ist. Dann ist $\mathcal{K}, u \sim \mathcal{K}', u'$.

- Wenn $(v, v') \in Z$, dann gilt $v \in P_i \iff v' \in P_i'$, denn sonst wäre $\mathcal{K}, v \models P_i$ und $\mathcal{K}', v' \models \neg P_i$ (oder umgekehrt).

- **Hin**: Sei $(v, v') \in Z$, d.h. $\mathcal{K}, v \equiv_{\mathrm{ML}} \mathcal{K}', v'$, und $v \xrightarrow{a} w$. Wir setzen

  $$\begin{aligned} v'E_a &:= \{z' : v' \xrightarrow{a} z'\} \text{ und} \\ X_w &:= \{z' \in v'E_a : \mathcal{K}, w \not\equiv_{\mathrm{ML}} \mathcal{K}', z'\}. \end{aligned}$$

  Es reicht zu zeigen, dass ein $w' \in v'E_a - X_w$ existiert, denn dann ist $(w, w') \in Z$ und die Hin-Eigenschaft erfüllt. Dazu wählen wir für jedes $z' \in X_w$ eine Formel $\varphi_{z'} \in \mathrm{ML}$, so dass $\mathcal{K}, w \models \varphi_{z'}$ aber $\mathcal{K}', z' \models \neg\varphi_{z'}$ und setzen $\varphi := \bigwedge\{\varphi_{z'} : z' \in X_w\}$. Da $\mathcal{K}'$ endlich verzweigt ist, gibt es nur endlich viele $z' \in X_w$, es ist also $\varphi \in \mathrm{ML}$. Es gilt $\mathcal{K}, w \models \varphi$, also $\mathcal{K}, v \models \langle a \rangle\varphi$. Da $\mathcal{K}, v \equiv_{\mathrm{ML}} \mathcal{K}', v'$, ist auch $\mathcal{K}', v' \models \langle a \rangle\varphi$, d.h. es existiert ein $w' \in v'E_a$ mit $\mathcal{K}', w' \models \varphi$. Dann kann aber w' nicht Element von X_w sein, denn dann wäre $\mathcal{K}', w' \models \neg\varphi_{w'}$ und daher $\mathcal{K}', w' \models \neg\varphi$.

- Der Beweis der **Her**-Eigenschaft läuft analog, mit vertauschten Rollen von $\mathcal{K}, v$ und $\mathcal{K}', v'$.

□

4.3 Abwicklungen, Baummodell-Eigenschaft und Endliche-Modell-Eigenschaft

Definition 4.15. Ein Transitionssystem $\mathcal{K} = (V, (E_a)_{a \in A}, (P_i)_{i \in I})$ mit einem ausgezeichneten Knoten w ist ein *Baum*, wenn

(1) $E_a \cap E_b = \varnothing$ für alle Aktionen $a \neq b$,

(2) für $E = \bigcup_{a \in A} E_a$ ist (V, E) ein (gerichteter) Baum mit Wurzel w im Sinn der Graphentheorie (siehe auch Kapitel 1.4, Lemma von König).

Definition 4.16. Sei Φ eine Menge von Formeln (irgendeiner Logik, etwa der Modallogik oder der Prädikatenlogik).

(1) Φ hat die *Endliche-Modell-Eigenschaft* (EME), wenn jede erfüllbare Formel $\varphi \in \Phi$ ein endliches Modell besitzt.

(2) Angenommen Φ spricht über Transitionssysteme (d.h. nur über ein- und zweistellige Relationen). Φ hat die *Baummodell-Eigenschaft* (BME), wenn jede erfüllbare Formel in Φ ein Modell hat, welches ein Baum ist.

(3) Analog definieren wir die *Endliche-Baummodell-Eigenschaft*.

Bemerkung. FO hat weder die Endliche-Modell-Eigenschaft noch die Baummodell-Eigenschaft. Die Formel $\exists y Exy \wedge \forall y Eyx$ ist erfüllbar, hat aber kein Baummodell. Die Formel

$$\forall y \neg Eyx \wedge \forall x \exists y Exy \wedge \forall x \forall y \forall z (Exz \wedge Eyz \rightarrow x = y)$$

andererseits hat ein Modell, mit $(\mathbb{N}, E, 0)$ und $E = \{(n, n+1) : n \in \mathbb{N}\}$ sogar ein Baummodell, aber kein endliches Modell. (Übung: Beweisen Sie dies.) Erfüllbare Formeln mit ausschliesslich unendlichen Modellen heissen *Unendlichkeitsaxiome.* Wir sehen also, dass es in FO Unendlichkeitsaxiome mit nur drei Variablen gibt. Es ist andererseits bekannt, dass FO^2 die Endliche-Modell-Eigenschaft besitzt, wir werden das aber im Rahmen dieser Vorlesung nicht beweisen. Wir werden aber zeigen, dass modallogische Formeln sowohl die Endliche-Modell-Eigenschaft wie auch die Baummodell-Eigenschaft haben.

Dazu betrachten wir *Abwicklungen* von Transitionssystemen. Die Abwicklung von $\mathcal{K}$ vom Zustand v aus besteht aus allen Pfaden in $\mathcal{K}$ die bei v beginnen. Dabei wird jeder Pfad als ein separates Objekt angesehen, d.h. selbst wenn sich zwei Pfade überschneiden, wird jeder zu einem neuen Zustand in der abgewickelten Struktur $\mathcal{T}$, und jeder Zustand aus $\mathcal{K}$, der auf einem Pfad von v aus erreicht wird, wird neu zu der Abwicklung hinzugefügt, unabhängig davon ob er schon einmal erreicht wurde. Schleifen in $\mathcal{K}$ entsprechen also unendlichen Wegen in der Abwicklung. Formal werden Abwicklungen wie folgt definiert.

Definition 4.17. Sei $\mathcal{K} = (V^{\mathcal{K}}, (E_a^{\mathcal{K}})_{a \in A}, (P_i^{\mathcal{K}})_{i \in I})$ eine Kripkestruktur und $v \in V^{\mathcal{K}}$. Die *Abwicklung* von $\mathcal{K}$ von v aus ist die Kripkestruktur $\mathcal{T}_{\mathcal{K},v} = (V^{\mathcal{T}}, (E_a^{\mathcal{T}})_{a \in A}, (P_i^{\mathcal{T}})_{i \in I})$ mit

$$\begin{aligned}
V^{\mathcal{T}} &= \{\bar{v} = v_0 a_0 v_1 a_1 v_2 \dots v_{m-1} a_{m-1} v_m : m \in \mathbb{N}, \\
&\qquad v_0 = v,\ v_i \in V^{\mathcal{K}},\ a_i \in A,\ (v_i, v_{i+1}) \in E_{a_i}^{\mathcal{K}} \text{ für alle } i < m\} \\
E_a^{\mathcal{T}} &= \{(\bar{v}, \bar{w}) \in V^{\mathcal{T}} \times V^{\mathcal{T}} : \bar{w} = \bar{v} a w \text{ für ein } w \in V^{\mathcal{K}}\} \\
P_i^{\mathcal{T}} &= \{\bar{v} = v_0 a_0 \dots v_m \in V^{\mathcal{T}} : v_m \in P_i^{\mathcal{K}}\}.
\end{aligned}$$

Mit $\text{end}(\bar{v})$ bezeichnen wir den letzten Knoten auf dem Pfad $\bar{v}$. Damit ist $\bar{v} \in P_i^{\mathcal{T}} \iff \text{end}(\bar{v}) \in P_i^{\mathcal{K}}$.

Lemma 4.18. *Es gilt* $\mathcal{K}, v \sim \mathcal{T}_{K,v}, v$.

Beweis. $Z := \{(w, \bar{w}) \in V^{\mathcal{K}} \times V^{\mathcal{T}} : \text{end}(\bar{w}) = w\}$ ist eine Bisimulation von $\mathcal{K}$ nach $\mathcal{T}_{\mathcal{K},v}$ mit $(v, v) \in Z$. ☐

Satz 4.19. ML *hat die Baummodell-Eigenschaft.*

Beweis. Sei ψ eine beliebige erfüllbare Formel aus ML. Es gibt also ein Modell $\mathcal{K}, v \models \psi$. Sei $\mathcal{T} := \mathcal{T}_{\mathcal{K},v}$ die Abwicklung von $\mathcal{K}, v$. Da $\mathcal{K}, v \sim \mathcal{T}, v$ gilt nach der Bisimulationsinvarianz der Modallogik auch $\mathcal{T}, v \models \psi$. Also hat ψ ein Baummodell. ☐

Dasselbe Argument zeigt, dass *jede* Klasse von bisimulations-invarianten Formeln die Baummodell-Eigenschaft besitzt. Für ML können wir ein wesentlich stärkeres Resultat beweisen. Wir benutzen dazu den Begriff des Abschlusses $C(\psi)$ einer Formel ψ.

Definition 4.20. Für jede Formel $\psi \in$ ML definieren wir induktiv für alle $n \in \mathbb{N}$ die Formelmengen $C_n(\psi)$ wie folgt:

(1) $\psi \in C_0(\psi)$.

(2) Wenn $\neg\varphi \in C_n(\psi)$, dann auch $\varphi \in C_n(\psi)$.

(3) Wenn $(\varphi \wedge \vartheta) \in C_n(\psi)$ oder $(\varphi \vee \vartheta) \in C_n(\psi)$, dann sind auch φ und ϑ in $C_n(\psi)$.

(4) Wenn $\langle a\rangle\varphi \in C_n(\psi)$ oder $[a]\varphi \in C_n(\varphi)$, dann ist $\varphi \in C_{n+1}(\varphi)$.

Schliesslich sei $C(\psi) := \bigcup_{n\in\mathbb{N}} C_j(\psi)$.

Der Abschluss $C_j(\psi)$ enthält diejenigen Formeln aus ML die für die Auswertung von ψ wesentlich sind; $C_j(\psi)$ sind dabei diejenigen Formeln die in ψ innerhalb von j verschachtelten Modaloperatoren vorkommen. Man beachte, dass $|C(\psi)| \leq |\psi|$ und dass $C_n(\psi) = \varnothing$ für alle $n > \mathrm{md}(\psi)$.

Satz 4.21. *Zu jeder erfüllbaren Formel $\psi \in$ ML existiert eine endliche Baumstruktur $\mathcal{T}, v$ mit Tiefe $\leq \mathrm{md}(\psi)$ und Verzweigungsgrad $\leq |C(\psi)|$, so dass $\mathcal{T}, v \models \psi$. Insbesondere hat* ML *also die endliche Baummodell-Eigenschaft.*

Beweis. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass ψ in Negationsnormalform ist. Da ψ erfüllbar ist, existiert ein Baummodell $\mathcal{T}, u \models \psi$. Die Tiefe eines Knotens von $\mathcal{T}$ ist seine Distanz von der Wurzel. Wir definieren nun eine Beschriftung S, welche jedem Knoten v von $\mathcal{T}$ mit Tiefe m eine Teilmenge von $C_m(\psi)$ zuordnet, nämlich

$$S(v) := \{\varphi \in C_m(\psi) : \mathcal{T}, v \models \varphi\}.$$

Wir transformieren $\mathcal{T}$ in eine endliche Baumstruktur, indem wir sukzessive überflüssige Teilbäume rausschneiden.

Sei $\mathcal{T}' \subseteq \mathcal{T}$ irgendein Teilbaum von $\mathcal{T}$ und v ein Knoten von $\mathcal{T}'$. Beachte dass $\mathcal{T}, v \models S(v)$. Das folgende Lemma gibt uns ein hinreichendes Kriterium dafür, dass auch $\mathcal{T}', v \models S(v)$.

Lemma 4.22. *Der Teilbaum $\mathcal{T}' \subseteq \mathcal{T}$ sei so konstruiert, dass folgende Bedingungen erfüllt sind.*

(1) Für jeden Nachfolger w von v in $\mathcal{T}'$ gilt $\mathcal{T}', w \models S(w)$.

(2) Für jede Formel der Form $\langle a\rangle\varphi \in S(v)$ existiert im Baum $\mathcal{T}'$ ein a-Nachfolger $w_{\langle a\rangle\varphi}$ von v, so dass $\mathcal{T}', w_{\langle a\rangle\varphi} \models \varphi$.

Dann gilt $\mathcal{T}', v \models S(v)$.

Beweis. Jede Formel in $S(v)$ ist eine mit $\wedge$ und $\vee$ zusammengesetzte Kombination von Formeln der Form $P_i, \neg P_i$, $\langle a\rangle\varphi$ und $[a]\varphi$. Es genügt also, für jede Formel ϑ dieser Form zu zeigen, dass $\mathcal{T}, v \models \vartheta$ auch $\mathcal{T}', v \models \vartheta$ impliziert. Für $\vartheta = P_i$ und $\vartheta = \neg P_i$ ist dies klar, da die atomaren Eigenschaften am Knoten v in $\mathcal{T}$ und $\mathcal{T}'$ dieselben sind. Für Formeln $[a]\varphi$ folgt dies aus Bedingung (1) und für Formeln $\langle a\rangle\varphi$ aus Bedingung (2). $\square$

Zur Konstruktion eines endlichen Teilbaumes $\mathcal{T}'$ können wir demnach wie folgt vorgehen. Sei v zuerst die Wurzel von $\mathcal{T}$. Für jede Formel der Form $\langle a\rangle\varphi \in S(v)$ wählen wir einen a-Nachfolger $w_{\langle a\rangle\varphi} \in vE_a$ so dass $\mathcal{T}, w_{\langle a\rangle\varphi} \models \varphi$ und schneiden aus $\mathcal{T}$ alle nicht-ausgewählten

Nachfolgeknoten von v und die daran hängenden Unterbäume heraus. Wir wiederholen diesen Prozess für alle verbleibenden Knoten der Tiefe 1,2, ... Da die Beschriftung $S(v)$ von Knoten der Tiefe $m = \mathrm{md}(\psi)$ nur noch aus Formeln P_i und $\neg P_i$ besteht, hat der resultierende Baum höchstens die Tiefe m. Von jedem Knoten v bleiben höchstens $|S(v)| \leq C(\psi)$ Nachfolger übrig, so dass der Verzweigungsgrad von $\mathcal{T}'$ durch $|C(\psi|$ beschränkt ist.

Per Induktion von den Blättern von $\mathcal{T}'$ zur Wurzel folgt mit Hilfe des Lemmas, dass $\mathcal{T}', v \models S(v)$, insbesondere also $\mathcal{T}', v \models \psi$. □

4.4 Algorithmische Probleme: Model-Checking und Erfüllbarkeit

Die wichtigsten algorithmischen Probleme für eine Logik sind (1) das *Auswertungs-* oder *Model-Checking-Problem* und (2) das Erfüllbarkeitsproblem. Wir präzisieren diese beiden Probleme für den Fall der Modallogik ML.

Model-Checking: Gegeben sei eine Formel $\psi \in \mathrm{ML}$, ein endliches Transitionssystem $\mathcal{K}$ und ein Zustand v von $\mathcal{K}$. Man enscheide, ob $\mathcal{K}, v \models \psi$.

Erfüllbarkeit: Gegeben sei eine Formel $\psi \in \mathrm{ML}$. Man entscheide, ob es ein Modell für ψ gibt.

Natürlich gibt es noch viele andere wichtige algorithmische Probleme. Die meisten sind aber entweder Varianten oder lassen sich relativ leicht auf eines der beiden Probleme reduzieren. Eine wichtige Variante des Erfüllbarkeitsproblems ist etwa das Problem der endlichen Erfüllbarkeit: Gegeben eine Formel ψ, entscheide man, ob ψ ein endliches Modell zulässt. Für Logiken mit der EME (wie z.B. ML) ist Erfüllbarkeit und endliche Erfüllbarkeit natürlich dasselbe Problem. Ein Variante des Model-Checking-Problems ist das *Auswertungsproblem:* Gegeben eine Formel ψ und ein endliches Transitionssystem $\mathcal{K}$ berechne man die Extension $[\![\psi]\!]^{\mathcal{K}}$. Natürlich sind das Auswertungs- und das Model-Checking-Problem effizient aufeinander reduzierbar. Ein Beispiel für ein Problem, das sich auf das Erfüllbarkeitsproblem reduzieren lässt, ist das *Subsumtionsproblem*: Gegeben zwei Formeln ψ und φ, entscheide man, ob jedes Modell von ψ auch Modell von φ ist. Dies ist genau dann *nicht* der Fall, wenn die Formel $\psi \wedge \neg\varphi$ erfüllbar ist.

Das Auswertungsproblem (und damit auch das Model-Checking-Problem) für ML ist effizient lösbar, nämlich in linearer Zeit sowohl bzgl. der Länge der Formel, wie bzgl. der Grösse des Transitionssystems. Die "Grösse des Transitionssystems" $\mathcal{K} = (V, (E_a)_{a\in A}, (P_i)_{i\in I})$ sei dabei $\|\mathcal{K}\| := |V| + \sum_{a\in A} |E_a|$.

Satz 4.23. *Es gibt einen Algorithmus, welcher zu einem gegebenen endlichen Transitionssystem $\mathcal{K}$ und einer Formel $\psi \in \mathrm{ML}$ in Zeit $O(\|\mathcal{K}\| \cdot |\psi|)$ die Extension $[\![\psi]\!]^{\mathcal{K}}$ berechnet.*

Beweis. Seien $\psi_1, \ldots, \psi_m$ die Unterformeln von ψ, geordnet so, dass $|\psi_i| \leq |\psi_j|$ für $i < j$. Insbesondere ist $\psi_m = \psi$. Wir berechnen für $i = 1, \ldots, m$ die Extension $[\![\varphi_i]\!]^{\mathcal{K}}$. Wenn die Extensionen $[\![\varphi_j]\!]$ für $j < i$ bereits berechnet sind erfordert dies höchstens Zeit $O(\|\mathcal{K}\|)$, insgesamt also Zeit $O(\|\mathcal{K}\| \cdot |\psi|)$. □

Ein andere Methode, um das Model-Checking-Problem zu lösen ist in der folgenden Übung beschrieben.

Übung 4.2. Beschreiben Sie das Auswertungsspiel für die Modallogik (vgl. Kapitel 3.5). Zeigen sie, dass man jedem endlichen Transitionssystem $\mathcal{K}$, jedem Zustand v und jeder Formel $\psi \in \mathrm{ML}$ ein Spiel $\mathrm{MC}(\mathcal{K}, v, \psi)$ der Grösse $\|\mathcal{K}\| \cdot |\psi|$ zuordnen kann, welches eine Gewinnstrategie für den Verifizierer zulässt genau dann, wenn $\mathcal{K}, v \models \psi$. Da gemäss Übung 3.5 das Strategieproblem für solche Spiel in linearer Zeit lösbar ist, folgt Satz 4.23.

Das Erfüllbarkeitsproblem ist in der Regel wesentlich komplizierter als das Model-Checking-Problem. Schon für die Aussagenlogik ist es NP-vollständig, lässt also vermutlich keinen effizienten Algorithmus zu (vgl. Kapitel 1). Für die Prädikatenlogik ist es, wie wir später sehen werden, unentscheidbar. Für die Modallogik folgt die Entscheidbarkeit des Erfüllbarkeitsproblems unmittelbar aus Satz 4.21.

Eine gegebene Formel $\psi \in \mathrm{ML}$ ist erfüllbar genau dann, wenn für ψ ein Baummodell mit Tiefe $\leq \mathrm{md}(\psi)$ und Verzweigungsgrad $\leq |\psi|$. Da in ψ nur endlich viele Aktionen und atomare Eigenschaften vorkommen können, gibt es nur endlich viele Baumstukturen mit diesen Eigenschaften. Wir können also einfach alle diese Baumstrukturen der Reihe nach konstruieren und (mit dem Algorithmus aus Satz 4.23) prüfen, ob eine davon ein Modell von ψ ist.

Wir haben damit gezeigt:

Satz 4.24. *Das Erfüllbarkeitsproblem für* ML *ist entscheidbar.*

Allerdings ist das angegebene, naive Entscheidungsverfahren sehr ineffizient. Da ML eine Erweiterung der Aussagenlogik ist, ist nicht zu erwarten, dass man einen Polynomzeit-Algorithmus finden kann. Es gibt aber deutlich bessere Algorithmen, welche zwar (im schlimmsten Fall) exponentielle Laufzeit benötigen, dafür aber mit linearem Speicherplatz auskommen. Das Erfüllbarkeitsproblem für ML ist PSPACE-vollständig.

4.5 CTL

Der wesentlichste Mangel von ML ist das Fehlen eines Rekursionsmechanismus. Zu den wichtigsten Aussagen in einer Reihe von Anwendungen (insbeondere in der Verifikation) gehören *Erreichbarkeitsaussagen*, wie etwa *Lebendigkeitsbedingungen* (ein 'guter' Zustand wird auf jeden Fall irgendwann erreicht) oder *Fairnessbedingungen* (kein schlechter Zustand ist erreichbar). Erreichbarkeit ist aber nicht in ML formalisierbar, da jede ML-Formel ψ vom Zustand an dem sie ausgewertet wird höchstens $\mathrm{md}(\psi)$ viele Schritte weit in das Transitionssytem 'hineinsehen' kann. Wir werden später sehen, dass Erreichbarkeitsaussagen in Transitionssystemen auch in FO nicht formalisierbar sind.

Es gibt verschiedene Möglichkeiten, solche Mängel von Logiken zu beseitigen, indem Rekursionsmechanismen hinzugefügt werden. Die eleganteste Lösung sind sogenannte *Fixpunktlogiken*, welche so definiert sind, dass kleinste und grösste Fixpunkte von definierbaren monotonen Operationen wieder definierbar sind. Fixpunktlogiken sind allerdings relativ kompliziert und sprengen den Rahmen dieser Vorlesung. Wir behandeln stattdessen CTL ("computation tree logic" oder auch "branching time temporal logic"), eine einfache Erweiterung von ML welche in der Hardware-Verifikation sehr populär ist. Die Idee von CTL ist, ML um Pfadquantoren und temporale Operatoren (wie "next" und " until") auf Pfaden zu erweitern.

CTL operiert auf Transitionssystemen mit nur einer Transitionsrelation, d.h. Strukturen der Form $\mathcal{K} = (V, E, (P_i)_{i \in I})$. Der Einfachheit halber wird dabei vorausgesetzt, dass E nicht terminiert, d.h. zu jedem $u \in V$ existiert ein v, so dass $(u, v) \in E$.

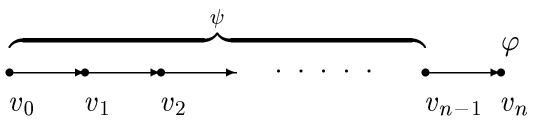
Definition 4.25 (Syntax von CTL). Die Formeln von CTL sind induktiv definiert wie folgt.

- Alle aussagenlogischen Formeln über $\{P_i : i \in I\}$ gehören zu CTL.
- CTL ist abgeschlossen unter den Boolschen Operatoren $\wedge$, $\vee, \rightarrow$ und $\neg$.
- Wenn ψ, $\varphi \in$ CTL, dann sind auch die Ausdrücke

  $$\mathrm{EX}\psi,\ \mathrm{AX}\psi,\ \mathrm{E}(\psi \mathrm{U} \varphi) \text{ und } \mathrm{A}(\psi \mathrm{U} \varphi)$$

  Formeln von CTL.

Die Intuition bei der Modellbeziehung ist folgende: Sei $\mathcal{K}$ ein Transitionssystem, v ein Zustand von $\mathcal{K}$. Dann quantifizieren E und A über unendliche Pfade $v = v_0 v_2 v_3 \cdots$ in $\mathcal{K}$, welche bei v beginnen. Der Ausdruck Xψ ("next ψ") bedeutet, dass am nächsten Zustand auf dem Pfad ψ gilt und der Ausdruck $\psi \mathrm{U} \varphi$ ("ψ until φ") besagt, dass es ein $n \geq 0$ gibt, so dass an allen Zuständen v_i mit $i < n$ ψ und an Zustand v_n φ gilt:



Definition 4.26 (Semantik von CTL). Sei $\mathcal{K} = (V, E, (P_i)_{i \in I})$ eine Kripkestruktur und $v \in V$. Dann gilt:

- $\mathrm{EX}\psi :\equiv \Diamond\psi$.
- $\mathrm{AX}\psi :\equiv \Box\psi$.
- Es ist $\mathcal{K}, v \models \mathrm{E}(\psi \mathrm{U} \varphi)$, wenn es eine Folge $v = v_0 v_1 v_2 \cdots$ gibt (mit $(v_i, v_{i+1}) \in E$ für alle i) und ein $n \geq 0$ existiert, so dass $\mathcal{K}, v_n \models \varphi$ und $\mathcal{K}, v_m \models \psi$ für alle m mit $0 \leq m < n$.
- Es ist $\mathcal{K}, v \models \mathrm{A}(\psi \mathrm{U} \varphi)$, wenn für alle unendlichen Pfade $v = v_0 v_1 v_2 \cdots$ (mit $(v_i, v_{i+1}) \in E$ für alle i) ein $n \geq 0$ existiert mit $\mathcal{K}, v_n \models \varphi$ und $\mathcal{K}, v_m \models \psi$ für alle m mit $0 \leq m < n$.

Notation. Zwei wichtige Abkürzungen sind:

$$\mathrm{F}\psi := (1\ \mathrm{U}\psi) : \text{ irgendwann gilt } \psi \text{ (auf dem Pfad)}$$
$$\mathrm{G}\psi := \neg\mathrm{F}\neg\psi : \text{ es gilt immer } \psi \text{ (auf dem Pfad).}$$

Beispiele. (1) In CTL ist Erreichbarkeit definierbar: EFφ bedeutet, dass ein Zustand erreicht werden kann, an dem φ gilt.

(2) AG$\neg(P \wedge Q)$ drückt aus, dass sich P und Q in allen erreichbaren Zuständen ausschließen.

(3) AFψ besagt, dass auf allen Pfaden irgendwann ψ gilt.

(4) AGAFψ besagt, dass ψ unendlich oft auf allen Pfaden gilt.

Diese Beispiele zeigen, dass viele für die Verifikation wichtige Aussagen in CTL formalisierbar sind. Dies allein macht aber noch nicht die Bedeutung von CTL aus. Wichtig ist, dass CTL andererseits günstige modelltheoretische und algorithmische Eigenschaften besitzt.

Zunächst ist CTL (wie ML) invariant unter Bisimulation.

Übung 4.3. Zeigen Sie, per Induktion über den Aufbau von CTL-Formeln, dass für alle $\psi \in \mathrm{CTL}$ gilt: Wenn $\mathcal{K}, v \models \psi$ und $\mathcal{K}, v \sim \mathcal{K}', v'$, dann auch $\mathcal{K}', v' \models \psi$. Es folgt, dass CTL die Baummodell-Eigenschaft hat.

CTL-Formeln können effizient ausgewertet werden (in linearer Zeit sowohl bzgl. der Länge der Formel wie der Grösse des Transitionssystems).

Satz 4.27. *Es gibt einen Algorithmus, welcher zu einem gegebenen endlichen Transitionssystem $\mathcal{K}$ und einer Formel $\psi \in \mathrm{CTL}$ in Zeit $O(\|\mathcal{K}\| \cdot |\psi|)$ die Extension $[\![\psi]\!]^{\mathcal{K}}$ berechnet.*

Dieser Satz erweitert Satz 4.23. Der Beweis beruht auf darauf, dass Formeln der Form $\mathrm{E}(\psi \mathrm{U} \varphi)$ und $\mathrm{A}(\psi \mathrm{U} \varphi)$ mit Hilfe von graphentheoretischen Algorithmen mit linearer Laufzeit ausgewertet werden können.

Weitere wichtige Eigenschaften von CTL sind:

- CTL hat die Endliche-Modell-Eigenschaft.
- das Erfüllbarkeitsproblem für CTL ist entscheidbar (in exponentieller Zeit).

Dies kann hier nicht bewiesen werden. Für die Behandlung von CTL und anderen modalen und temporalen Logiken sind insbesondere automatentheoretische Methoden wichtig.

Im Gegensatz zu ML kann CTL *nicht* in FO eingebettet werden (z.B. da Erreichbarkeit nicht FO-definierbar ist). Eine hinreichende Erweiterung von FO ist MSO, die *monadische Logik zweiter Stufe*, welche FO um Quantoren über einstellige Relationssymbole (d.h. Mengenvariablen) erweitert. Aus einer Formel ψ können neue Formeln der Form $\exists X \psi$ bzw. $\forall X \psi$ gebildet werden, mit der Bedeutung "es gibt eine Teilmenge X des Universums, so dass ψ" bzw. "für alle Teilmengen X des Universums gilt ψ". So drückt z.B. die Formel

$$\forall X((Xs \land \forall y \forall z(Xy \land Eyz \to Xz) \to Xt)$$

aus, dass im Graphen (V, E) ein Pfad von s nach t existiert.

Übung 4.4. Zeigen Sie, dass jede CTL-Formel in eine äquivalente Formel in MSO übersetzt werden kann.

Kapitel 5

Definierbarkeit in der Prädikatenlogik

5.1 Definierbarkeit

Axiomatisierbare Strukturklassen. Wir haben bereits in Kapitel 3 den Begriff der durch eine Satzmenge Φ axiomatisierten Strukturklasse $\mathrm{Mod}(\Phi)$ eingeführt und Axiomensysteme für einige wichtige Klassen angegeben, etwa für Graphen, Gruppen, lineare Ordnungen sowie für die Klasse aller unendlichen Strukturen.

Definition 5.1. Sei $\mathrm{Str}(\tau)$ die Klasse aller τ-Strukturen. Eine Strukturklasse $\mathcal{K} \subseteq \mathrm{Str}(\tau)$ ist FO-*axiomatisierbar* (oder einfach: axiomatisierbar), wenn eine Satzmenge $\Phi \subseteq \mathrm{FO}(\tau)$ existiert, so dass $\mathcal{K} = \mathrm{Mod}(\Phi)$. Wenn das Axiomensystem Φ für $\mathcal{K}$ endlich ist, dann können wir die Konjunktion $\psi = \bigwedge\{\varphi : \varphi \in \Phi\}$ bilden und damit $\mathcal{K}$ durch einen einzigen Satz axiomatisieren. Wir sagen in diesem Fall, $\mathcal{K}$ ist *elementar* oder *endlich axiomatisierbar*.

Wir beginnen in diesem Kapitel mit der Untersuchung der Ausdrucksstärke der Prädikatenlogik. Ein wichtiger Aspekt ist dabei die Frage, welche Strukturklassen FO-axiomatisierbar, welche sogar endlich axiomatisierbar sind.

Wir wissen bereits, dass Graphen, Gruppen und lineare Ordnungen endlich axiomatisierbar sind. Weiter ist offensichtlich, dass dasselbe auch für Äquivalenzstrukturen, partielle Ordnungen, dichte lineare Ordnungen, diskrete lineare Ordnungen, Ringe und Körper gilt. Die Klasse aller unendlichen Strukturen ist zwar FO-axiomatisierbar, aber das Axiomensystem Φ_∞, das wir in Kapitel 3.2 dafür angegeben haben, besteht aus unendlich vielen Formeln. (Wir werden später sehen, dass kein endliches Axiomensystem für diese Klasse existiert.)

Hier sind noch einige weitere Beispiele für axiomatisierbare Strukturklassen.

Beispiele. (1) Die Klasse aller Körper ist axiomatisiert durch $\psi_{\text{Körper}} \in \mathrm{FO}(\tau_{ar})$, die Konjunktion aller Körperaxiome. Für jede Primzahl p ist auch die Klasse der Körper mit Charakteristik p endlich axiomatisierbar, durch $\psi_{\text{Körper}} \wedge \chi_p$ wobei χ_p der Satz $\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$ ist. Für Körper der Charakteristik 0 können wir zumindest ein unendliches Axiomensystem angeben, nämlich

$$\Phi = \{\psi_{\text{Körper}}\} \cup \{\neg\chi_p : p \text{ Primzahl}\}.$$

(2) Auch die Klasse ACF der algebraisch abgeschlossenen Körper ist FO-axiomatisierbar. Der Satz

$$\psi_n := \forall u_0 \cdots \forall u_n (u_n \neq 0 \to \exists x (u_0 + u_1 x + \cdots u_n x^n = 0))$$

besagt, dass jedes Polynom n-ten Grades mit Koeffizienten aus dem Körper auch eine Nullstelle im Körper hat. (Hier ist x^n als abkürzende Schreibweise für den Term $\underbrace{x \cdot x \ldots x}_{n \text{ mal}}$ aufzufassen.)

Also ist $\Phi_{\text{ACF}} = \{\psi_{\text{Körper}}\} \cup \{\psi_n : n \geq 1\}$ ein Axiomensystem für algebraisch abgeschlossene Körper.

Übung 5.1. Sei $\mathfrak{A}$ eine endliche Struktur mit endlicher Signatur. Zeigen Sie, dass $\{\mathfrak{B} : \mathfrak{B} \cong \mathfrak{A}\}$ endlich axiomatisierbar ist.

Der Nachweis, dass eine Strukturklasse (endlich) axiomatisierbar ist, wird in der Regel durch explizite Angabe eines Axiomensystems geführt. Um nachzuweisen, dass eine Strukturklasse gar kein oder mindestens kein endliches Axiomensystem zulässt, sind andere Methoden erforderlich, welche in diesem und dem folgenden Kapitel entwickelt werden sollen.

Zunächst aber diskutieren wir noch einen anderen Aspekt der Ausdrucksstärke einer Logik.

Definierbarkeit in einer Struktur. Neben der Frage, welche Strukturklassen durch Sätze oder Satzmengen der Prädikatenlogik axiomatisierbar sind, können wir die Ausdrucksstärke von FO auch innerhalb einer festen Struktur untersuchen.

Sei $\psi(x_1, \ldots, x_r) \in \text{FO}(\tau)$ und $\mathfrak{A}$ eine τ-Struktur. Dann definiert ψ in $\mathfrak{A}$ die r-stellige Relation

$$\psi^{\mathfrak{A}} := \{(a_1, \ldots, a_r) : \mathfrak{A} \models \psi(a_1, \ldots, a_r)\} \subseteq A^r.$$

Definition 5.2. Eine Relation $R \subseteq A^r$ auf dem Universum einer τ-Struktur $\mathfrak{A}$ ist *(elementar) definierbar* in $\mathfrak{A}$, wenn $R = \psi^{\mathfrak{A}}$ für eine Formel $\psi \in \text{FO}(\tau)$. Eine Funktion $f : A^r \to A$ heisst elementar definierbar, wenn ihr Graph R_f elementar definierbar ist.

Insbesondere ist also eine Konstante a elementar definierbar, wenn eine Formel $\varphi(x) \in \text{FO}(\tau)$ existiert, so dass $\mathfrak{A} \models \varphi(a)$ und $\mathfrak{A} \models \neg\varphi(b)$ für alle $b \neq a$. Wir sagen, a ist *termdefinierbar* in $\mathfrak{A}$, wenn ein Grundterm $t \in T(\tau)$ existiert, so dass $t^{\mathfrak{A}} = a$. Jede termdefinierbare Konstante ist insbesondere elementar definierbar durch eine Formel der Form $x = t$.

Beispiele. (1) Die Ordnungsrelation $<$ auf $\mathbb{R}$ ist elementar definierbar in $(\mathbb{R}, +, \cdot, 0, 1)$, denn für die Formel $\varphi(x, y) := \exists z (z \neq 0 \land x + z \cdot z = y)$ gilt

$$a < b \iff (\mathbb{R}, +, \cdot, 0, 1) \models \varphi(a, b).$$

(2) In $(\mathbb{Z}, <)$ ist die Nachfolgerfunktion $z \mapsto z+1$ elementar definierbar durch die Formel $\varphi(x, y) := x < y \land \forall z (x < z \land y \neq z \to y < z)$.

(3) In $(\mathbb{N}, +, 0, 1)$ ist jedes n termdefinierbar, durch den Term $\boldsymbol{n} = \underbrace{1 + \cdots + 1}_{n \text{ mal}}$ (für $n \geq 1$).

(4) Im Körper $(\mathbb{Q}, +, \cdot, 0, 1)$ der rationalen Zahlen sind die termdefinierbaren Konstanten genau die natürlichen Zahlen $n \in \mathbb{N}$. Alle anderen Elemente sind elementar definierbar durch Formeln der Form $\boldsymbol{p} \cdot x = \boldsymbol{q}$ oder $\boldsymbol{p} \cdot x + \boldsymbol{q} = 0$, nicht aber termdefinierbar.

(5) Im Körper der reellen Zahlen können schon aus Mächtigkeitsgründen nicht alle Elemente elementar definierbar sein: es gibt überabzählbar viele reelle Zahlen, aber nur abzählbar viele Formeln $\varphi(x) \in \mathrm{FO}(\tau_{ar})$.

Als nächstes beobachten wir, dass das Hinzunehmen definierbarer Relationen zu einer Struktur keinen Gewinn an Ausdruckstärke bringt.

Lemma 5.3. *Sei $\mathfrak{A}$ eine σ-Struktur und $\mathfrak{B}$ eine Expansion von $\mathfrak{A}$ durch beliebig viele, in $\mathfrak{A}$ elementar definierbare Relationen und Funktionen. Dann ist jede in $\mathfrak{B}$ elementar definierbare Relation oder Funktion bereits in $\mathfrak{A}$ elementar definierbar.*

Beweis. Sei τ die Signatur von $\mathfrak{B}$. In jeder Formel $\psi(\bar{x}) \in \mathrm{FO}(\tau)$ kommen nur endlich viele Relations- und Funktionssymbole $R_1, \dots, R_s, f_1, \dots, f_t$ aus $\tau - \sigma$ vor. Zu jedem dieser R_i bzw. f_j gibt es eine σ-Formel $\vartheta_i(\bar{y})$ bzw. $\chi_j(\bar{y}, z)$, welche in $\mathfrak{A}$ die entsprechende Relation bzw. Funktion von $\mathfrak{B}$ definiert.

Weiter können wir nach Lemma 3.17 annehmen, dass ψ termreduziert ist, d.h., dass Funktionssymbole aus $\tau - \sigma$ nur in Atomen der Form $f_j\bar{y} = z$ auftreten. Indem wir in $\psi(\bar{x})$ die Relations- und Funktionssymbole aus $\tau - \sigma$ durch die definierenden Formeln ersetzen (d.h. jedes Atom $R_i\bar{u}$ durch $\vartheta_i(\bar{u})$ und jedes Atom $f_j\bar{u} = v$ durch $\chi_j(\bar{u}, v)$), erhalten wir eine Formel $\varphi(\bar{x}) \in \mathrm{FO}(\sigma)$ so, dass $\mathfrak{B} \models \forall\bar{x}(\psi \leftrightarrow \varphi)$. Da φ eine σ-Formel ist, folgt insbesondere $\psi^{\mathfrak{B}} = \varphi^{\mathfrak{A}}$. □

Relativierte Quantoren. An zwei Beispielen illustrieren wir die Verwendung relativierter Quantoren.

Stetigkeit. Sei $f : \mathbb{R} \to \mathbb{R}$ eine Funktion auf den reellen Zahlen. Ist die Menge $\{a \in \mathbb{R} : f \text{ stetig im Punkt } a\}$ in der Struktur $(\mathbb{R}, +, \cdot, 0, 1, <, f)$ elementar definierbar?

Wir betrachten dazu die Stetigkeitsdefinition aus der Analysis: Sei $U_\varepsilon(x)$ die ε-Umgebung von x. Die Funktion f ist stetig in x, wenn für alle $\varepsilon > 0$ ein $\delta > 0$ existiert, so dass für alle $y \in U_\delta(x)$ gilt: $f(y) \in U_\varepsilon(f(x))$.

Die Existenz- und Allaussagen für δ, ε und y sind hier *relativiert*: es werden nur Elemente betrachtet, die gewisse Eigenschaften erfüllen. Man beachte, dass relativierte Aussagen der Form "es gibt ein x mit α, so dass $\cdots$" bzw. "für alle x mit α gilt $\cdots$" durch $\exists x(\alpha \wedge \cdots)$ bzw. $\forall x(\alpha \to \cdots)$ formalisiert werden können Wir benutzen gelegentlich die Schreibweise $(\exists x \,.\, \alpha)\psi$ als Umschreibung für $\exists x(\alpha \wedge \psi)$ und $(\forall x \,.\, \alpha)\psi$ für $\forall x(\alpha \to \psi)$.

Um Stetigkeit zu formalisieren gehen wir nun wie folgt vor. (Wir verwenden die Relation $\leq$, was aufgrund ihrer elementaren Definierbarkeit unproblematisch ist.) Zunächst ist leicht einzusehen, dass die Relation $\{(a, b, \varepsilon) \in \mathbb{R}^3 : \varepsilon \geq 0 \text{ und } b \in U_\varepsilon(a)\}$ durch die Formel

$$\varphi(x, y, z) := 0 \leq z \wedge (\exists u \,.\, 0 \leq u \leq z)(x + u = y \vee y + u = x)$$

definiert wird. Die Stetigkeit von f im Punkt x ist nun ausgedrückt durch die Formel

$$\psi(x) := (\forall u \,.\, 0 < u)(\exists z \,.\, 0 < z)\forall y(\varphi(x, y, z) \to \varphi(fx, fy, u)).$$

Modallogik. Auch bei der Übersetzung der Modallogik in die Prädikatenlogik (siehe Satz 4.5) haben wir relativierte Quantoren verwendet. Die Modaloperatoren $\langle a \rangle$ und $[a]$ entsprechen relativierten Existenz- bzw. Allquantoren 'entlang a-Transitionen":

$$\langle a \rangle\psi \longmapsto (\exists y \,.\, E_a xy)\psi^*(y) = \exists y(E_a xy \wedge \psi^*(y))$$
$$[a]\psi \longmapsto (\forall y \,.\, E_a xy)\psi^*(y) = \forall y(E_a xy \to \psi^*(y))$$

5.2 Das Isomorphielemma

Isomorphe Strukturen betrachten wir als gleich. Insbesondere können FO-Formeln nicht zwischen isomorphen Strukturen unterscheiden.

Lemma 5.4 (Isomorphielemma). *Sei $\pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$ ein Isomorphismus von τ-Strukturen. Dann gilt für alle $\psi(x_1, \dots, x_n) \in \mathrm{FO}(\tau)$ und alle $a_1, \dots, a_n \in A$*

$$\mathfrak{A} \models \psi(a_1, \dots, a_n) \iff \mathfrak{B} \models \psi(\pi a_1, \dots, \pi a_n)$$

Beweis. Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine Interpretation mit $\beta(x_1) = a_1, \dots, \beta(x_n) = a_n$, und sei $\mathfrak{I}^\pi$ die Interpretation $(\mathfrak{B}, \pi \circ \beta)$.

Per Induktion über den Termaufbau zeigt man sofort, dass für jeden Term $t \in T(\tau)$

$$[\![t]\!]^{\mathfrak{I}^\pi} = \pi[\![t]\!]^{\mathfrak{I}}, \qquad (*)$$

sogar wenn nur vorausgesetzt ist, dass $\pi : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus ist.

Es ist zu zeigen, dass $\mathfrak{I} \models \psi$ genau dann, wenn $\mathfrak{I}^\pi \models \psi$. Wir führen den Beweis per Induktion über den Formelaufbau; nach Lemma 3.14 können wir dabei annehmen, dass ψ reduziert ist.

(1) Für Formeln der Form $t_1 = t_2$ gilt

$$\begin{aligned}
\mathfrak{I} \models t_1 = t_2 &\iff [\![t_1]\!]^{\mathfrak{I}} = [\![t_2]\!]^{\mathfrak{I}} \\
&\iff \pi[\![t_1]\!]^{\mathfrak{I}} = \pi[\![t_2]\!]^{\mathfrak{I}} \quad \text{(da π injektiv ist)} \\
&\iff [\![t_1]\!]^{\mathfrak{I}^\pi} = [\![t_2]\!]^{\mathfrak{I}^\pi} \quad \text{(nach (*))} \\
&\iff \mathfrak{I}^\pi \models t_1 = t_2
\end{aligned}$$

(2) Für Atome $Pt_1 \cdots t_n$ gilt

$$\begin{aligned}
\mathfrak{I} \models Pt_1 \cdots t_n &\iff ([\![t_1]\!]^{\mathfrak{I}}, \dots, [\![t_n]\!]^{\mathfrak{I}}) \in P^{\mathfrak{A}} \\
&\iff (\pi[\![t_1]\!]^{\mathfrak{I}}, \dots, \pi[\![t_n]\!]^{\mathfrak{I}}) \in P^{\mathfrak{B}} \quad \text{(da π ein starker Homomorphismus ist)} \\
&\iff ([\![t_1]\!]^{\mathfrak{I}^\pi}, \dots, [\![t_n]\!]^{\mathfrak{I}^\pi}) \in P^{\mathfrak{B}} \quad \text{(nach (*))} \\
&\iff \mathfrak{I}^\pi \models Pt_1 \cdots t_n
\end{aligned}$$

(3) Für Formeln der Form $\neg\psi$ oder $\psi \vee \varphi$ ist der Induktionsschluss trivial.

(4) Für Formeln $\exists x \psi$ gilt

$$\begin{aligned}
\mathfrak{I} \models \exists x \psi &\iff \mathfrak{I}[x/a] \models \psi \quad \text{für ein } a \in A \\
&\iff \mathfrak{I}[x/a]^\pi \models \psi \quad \text{für ein } a \in A \text{ (nach Induktionsvoraussetzung)} \\
&\iff \mathfrak{I}^\pi[x/\pi a] \models \psi \quad \text{für ein } a \in A \text{ (da } \mathfrak{I}[x/a]^\pi = \mathfrak{I}^\pi[x/\pi a]) \\
&\iff \mathfrak{I}^\pi[x/b] \models \psi \quad \text{für ein } b \in B \text{ (da π bijektiv ist)} \\
&\iff \mathfrak{I}^\pi \models \exists x \psi.
\end{aligned}$$

□

Insbesondere lassen sich isomorphe τ-Strukturen durch Sätze der Prädikatenlogik nicht unterscheiden. Sind $\mathfrak{A}$ und $\mathfrak{B}$ isomorphe τ-Strukturen, so gilt für alle τ-Sätze ψ:

$$\mathfrak{A} \models \psi \iff \mathfrak{B} \models \psi.$$

Also sind axiomatisierbare Modellklassen immer isomorphie-abgeschlossen. Dies bedeutet, dass für jede Klasse $\mathcal{K} = \text{Mod}(\psi)$ und alle Strukturen $\mathfrak{A}, \mathfrak{B}$ gilt

$$\mathfrak{A} \in \mathcal{K},\ \mathfrak{A} \cong \mathfrak{B} \implies \mathfrak{B} \in \mathcal{K}.$$

In manchen Fällen liefert das Isomorphielemma ein einfaches Kriterium, um nachzuweisen, dass eine Relation in einer Struktur *nicht* elementar definierbar ist

Lemma 5.5. *Sei π ein Automorphismus einer τ-Struktur $\mathfrak{A}$ und sei $\psi \in \text{FO}(\tau)$. Dann ist π auch ein Automorphismus der expandierten Struktur $(\mathfrak{A}, \psi^{\mathfrak{A}})$.*

Beweis. Da π ein Automorphisus ist, gilt für alle Tupel $\bar{a}$ aus A: $\mathfrak{A} \models \psi(\bar{a}) \iff \mathfrak{A} \models \psi(\pi\bar{a})$. Also ist $\pi(\psi^{\mathfrak{A}}) = \psi^{\mathfrak{A}}$. □

Beispiel. Wir haben gesehen, dass $<$ definierbar ist in $(\mathbb{R}, +, \cdot, 0, 1)$. Aus dem soeben bewiesenen Lemma folgt dagegen, dass $<$ in $(\mathbb{R}, +, 0)$ *nicht* elementar definierbar ist. Die Abbildung $\pi : x \mapsto -x$ ist nämlich ein Automorphismus von $(\mathbb{R}, +, 0)$, nicht aber von $(\mathbb{R}, +, 0, <)$, denn aus $a < b$ folgt eben gerade *nicht* $-a < -b$.

Übung 5.2. Sei $\tau = \varnothing$ und A unendlich. Beschreiben Sie alle in A elementar definierbaren Relationen $R \subseteq A^n$.

Übung 5.3. Zeigen Sie, dass in $(\mathbb{N}, \cdot, 1)$ die Addition nicht elementar definierbar ist.

5.3 Relationale Algebra

Kann man mit (definierbaren) Relationen 'algebraisch' rechnen, ähnlich wie etwa mit Polynomen, ohne Variablen und Quantoren explizit zu verwenden? Die relationale Algebra ist ein solcher algebraischer Kalkül auf Relationen, welcher im wesentlichen auf den Logiker Alfred Tarski zurückgeht. Zu Beginn der 70er Jahre wurde die relationale Algebra von Codd in seinen grundlegenden Arbeiten zum relationalen Datenbankmodell wiederentdeckt. Die relationale Algebra spielt insbesondere in der Theorie und Praxis relationaler Datenbanken eine wichtige Rolle. Wir beschreiben hier Syntax und Semantik der relationalen Algebra und zeigen, dass sie im wesentlichen dieselbe Ausdrucksstärke wie die Prädikatenlogik hat.

Syntax der relationalen Algebra. Sei $\tau = \{R_1, \ldots, R_m\}$ eine relationale Signatur. Die Terme von $\text{RA}(\tau)$ werden aus den Relationssymbolen von τ mittels der Operatoren $\times$ (kartesisches Produkt), $-$ (Differenz), $\pi_{i_1,\ldots,i_s}$ (Projektion) und $\sigma_{i=j}$ (Auswahl) definiert. Hier ist eine formale, induktive Definition der Terme von $\text{RA}(\tau)$ (und ihrer Stelligkeit):

(1) Jedes Relationssymbol $R_j \in \tau$ ist ein Term von $\text{RA}(\tau)$.

(2) Wenn R und S r-stellige Terme von $\text{RA}(\tau)$ sind, dann auch $(R \cup S)$ und $(R - S)$.

(3) Seien R, S Terme von $\text{RA}(\tau)$ der Stelligkeit r bzw. s. Dann ist $(R \times S)$ ein $(r + s)$-stelliger Term.

(4) Wenn R ein r-stelliger Term von $\mathrm{RA}(\tau)$ ist, $i_1, \ldots, i_s \leq r$, dann ist $\pi_{i_1,\ldots,i_s}(R)$ ein s-stelliger Term von $\mathrm{RA}(\tau)$.

(5) Sei R ein r-stelliger Term von $\mathrm{RA}(\tau)$, $i, j \leq r$. Dann ist auch $\sigma_{i=j}(R)$ ein r-stelliger Term aus $\mathrm{RA}(\tau)$.

Semantik der relationalen Algebra. Sei $\mathfrak{A}$ eine τ-Struktur. Jeder r-stellige Term $R \in \mathrm{RA}(\tau)$ wird über $\mathfrak{A}$ interpretiert durch eine r-stellige Relation $R^{\mathfrak{A}} \subseteq A^r$, die wie folgt definiert ist.

(1) Relationssybole $R_j \in \tau$ werden durch die entsprechenden Relationen $R_j^{\mathfrak{A}}$ der Struktur $\mathfrak{A}$ interpretiert.

(2) $(R \cup S)^{\mathfrak{A}} := R^{\mathfrak{A}} \cup S^{\mathfrak{A}}$ und $(R - S)^{\mathfrak{A}} = R^{\mathfrak{A}} - S^{\mathfrak{A}}$.

(3) $(R \times S)^{\mathfrak{A}} := R^{\mathfrak{A}} \times S^{\mathfrak{A}} = \{(\bar{a}, \bar{b}) \in A^{r+s} : \bar{a} \in R^{\mathfrak{A}}, \bar{b} \in S^{\mathfrak{A}}\}$.

(4) $\pi_{i_1,\ldots,i_s}(R)^{\mathfrak{A}} = \{(a_{i_1}, \ldots, a_{i_s}) : (a_1, \ldots, a_r) \in R^{\mathfrak{A}}\}$.

(5) $\sigma_{i=j}(R)^{\mathfrak{A}} := \{(a_1, \ldots, a_r) \in R^{\mathfrak{A}} : a_i = a_j\}$.

Wir zeigen zunächst, dass jeder Term der relationalen Algebra äquivalent ist zu einer FO-Formel.

Lemma 5.6. *Jeden r-stelligen Term $R \in \mathrm{RA}(\tau)$ kann man in eine Formel $\psi_R(x_1, \ldots, x_r) \in \mathrm{FO}(\tau)$ transformieren, so dass für alle τ-Strukturen $\mathfrak{A}$ gilt:*

$$R^{\mathfrak{A}} = \{(a_1, \ldots, a_r) \in A^r : \mathfrak{A} \models \psi_R(a_1, \ldots, a_r)\}.$$

Beweis.

(1) Für $R_j \in \tau$, setze $\psi_{R_j}(\bar{x}) := Rx_1 \cdots x_r$.

(2) $\psi_{(R \cup S)}(\bar{x}) := \psi_R(\bar{x}) \vee \psi_S(\bar{x})$ und $\psi_{(R-S)}(\bar{x}) := \psi_R(\bar{x}) \wedge \neg\psi_S(\bar{x})$.

(3) $\psi_{(R \times S)}(\bar{x}) := \psi_R(x_1, \ldots, x_r) \wedge \psi_S(x_{r+1}, \ldots, x_{r+s})$.

(4) Für $S := \pi_{i_1,\ldots,i_s}(R)$, setze

$$\psi_S(x_1, \ldots, x_s) := \exists y_1 \cdots \exists y_r (\psi_R(y_1, \ldots, y_r) \wedge \bigwedge_{j=1}^{s} x_j = y_{i_j}).$$

(Natürlich kann man die Gleichungen $x_j = y_{i_j}$ vermeiden, wenn man in $\psi_R(\bar{y})$ die Komponenenten y_{i_j} direkt durch x_j ersetzt.)

(5) Für $S = \sigma_{i=j}(R)$, setze $\psi_S(\bar{x}) := \psi_R(\bar{x}) \wedge x_i = x_j$.

$\square$

FO ist also mindestens so ausdrucksstark wie die relationale Algebra. Damit stellt sich unmittelbar die Frage, ob auch die Umkehrung gilt, d.h. ob jede FO-Formel (mit relationaler Signatur) äquivalent ist zu einem Term der relationalen Algebra. Für die hier definierte Variante von RA ist dies *nicht* der Fall, da wir das Komplement einer Relation nicht definieren können (nur die Mengendifferenz zu einer anderen bereits definierten Relation).

Für jede Struktur $\mathfrak{A} = (A, R_1, \dots, R_m)$ definieren wir den *aktiven Bereich* $ad(\mathfrak{A})$ als die Menge derjenigen Elemente von $\mathfrak{A}$ die in mindestens einer Relation R_i vorkommen. Offensichtlich ist der aktive Bereich in der relationalen Algebra (und damit auch in FO) definierbar, z.B. durch den Term

$$aD := \bigcup_{j=1}^{s} \bigcup_{i=1}^{r_j} \pi_i(R_j).$$

Die durch den aktiven Bereich von $\mathfrak{A}$ induzierte Substruktur nennen wir die *aktive Substruktur* von $\mathfrak{A}$. Die folgende Beobachtung ergibt sich unmittelbar aus der Definition.

Lemma 5.7. *Für jeden r-stelligen Term $R \subseteq \mathrm{RA}(\tau)$ und jede τ-Struktur $\mathfrak{A}$ gilt: $R^{\mathfrak{A}} \subseteq (ad(\mathfrak{A}))^r$.*

Wenn also der aktive Bereich nicht mit dem Universum A übereinstimmt, ist z.B. die Relation $A \times A$ nicht RA-definierbar. Um dem abzuhelfen, nehmen wir zu RA ein Symbol für das Universum hinzu.

Definition 5.8. Sei RA^+ die Erweiterung von RA um die folgende zusätzliche Regel:

(0) Univ ist ein einstelliger Term von $\mathrm{RA}^+(\tau)$. Für jede τ-Struktur $\mathfrak{A}$ ist $\mathrm{Univ}^{\mathfrak{A}} := A$.

Satz 5.9. *Für jede Formel $\varphi \in \mathrm{FO}(\tau)$ und jedes $m \in \mathbb{N}$, so dass alle freien Variabeln von φ zu $x_1, \dots, x_m$ gehören, gibt es einen m-stelligen Term $R_{\varphi,m} \in \mathrm{RA}^+(\tau)$, so dass für alle τ-Strukturen $\mathfrak{A}$ gilt: $R^{\mathfrak{A}}_{\varphi,m} = \{(a_1, \dots, a_m) \in A^m : \mathfrak{A} \models \varphi(a_1, \dots, a_m)\}$.*

Beweis. Der Beweis wird per Induktion über den Formelaufbau geführt, wobei wir annehmen, dass φ reduziert (d.h. nur mit $\vee, \neg$ und $\exists$ aufgebaut) ist. Die einzige Schwierigkeit betrifft nicht etwa die Übersetzung der Junktoren und Quantoren (welche, wie wir sehen werden, einfach ist) sondern die Übersetzung der atomaren Formeln. Betrachte etwa, für eine gegebene 5-stellige Relation R, die Menge aller 4-Tupel $(a_1, \dots, a_4)$, so dass $Ra_2a_1a_1a_4a_4$ gilt, d.h. die durch die atomare Formel $Rx_2x_1x_1x_4x_4$ definierte 4-stellige Relation. Das Problem ist, dass die Variablen $x_1, \dots, x_4$ in der Relation R in beliebiger Reihenfolge, mehrfach, oder auch gar nicht als Argumente auftreten können, was die Übersetzung in die relationale Algebra nicht ganz trivial werden lässt. (Man versuche die Übersetzung vor dem Weiterlesen selbst durchzuführen.) Wir behaupten, dass dieselbe Relation durch den Term

$$\pi_{1,2,3,4}\sigma_{5=2}\sigma_{6=1}\sigma_{7=1}\sigma_{8=4}\sigma_{9=4}(\mathrm{Univ}^4 \times R)$$

definiert wird. Dies liegt daran, dass wir $Rx_2x_1x_1x_4x_4$ durch die scheinbar kompliziertere Formel

$$\exists x_5 \exists x_6 \cdots \exists x_9 (Rx_5x_6x_7x_8x_9 \wedge x_5 = x_2 \wedge x_6 = x_1 \wedge x_7 = x_1 \wedge x_8 = x_4 \wedge x_9 = x_4)$$

darstellen können, in der aber die Argumente von R in ihrer natürlichen Reihenfolge auftreten.

(1) Wenn φ ein Atom der Form $x_i = x_j$ ist, dann setze $R_{\varphi,m} := \sigma_{ij}\mathrm{Univ}^m$. Offensichtlich ist dann $R^{\mathfrak{A}}_{\varphi,m} := \{(a_1,\dots a_m) \in A^m : a_i = a_j\}$.

(2) Ein Atom $\varphi := Rx_{i_1}\cdots x_{i_s}$ wird durch den Term

$$R_{\varphi,m} := \pi_{1,\dots,m}\sigma_{m+1=i_1}\cdots\sigma_{m+s=i_s}(\mathrm{Univ}^m \times R)$$

beschrieben. Dann gilt

$$\begin{aligned} R^{\mathfrak{A}}_{\varphi,m} =& \{(a_1,\dots,a_m) : \text{es gibt ein Tupel } (a_{m+1},\dots,a_{m+s}) \in R^{\mathfrak{A}} \text{ mit} \\ & \qquad a_{m+1} = a_{i_1},\dots,a_{m+s} = a_{i_s}\} \\ =& \{(a_1,\dots,a_m) : (a_{i_1},\dots,a_{i_s}) \in R^{\mathfrak{A}}\}. \end{aligned}$$

(3) Für $\varphi = \neg\vartheta$ ist $R_{\varphi,m} := (\mathrm{Univ}^m - R_{\vartheta,m})$.

(4) Für $\varphi = \vartheta \vee \eta$ ist $R_{\varphi,m} := (R_{\vartheta,m} \cup R_{\eta,m})$.

(5) Für $\varphi = \exists x_i\vartheta$ haben wir eine Fallunterscheidung durchzuführen, je nachdem, ob $i = m+1$ oder $i \le m$. Für $\varphi = \exists x_{m+1}\vartheta(x_1,\dots,x_{m+1})$, setzen wir $R_{\varphi,m} := \pi_{1,\dots,m}R_{\vartheta,m+1}$. Offensichtlich gilt dann

$$\begin{aligned} R^{\mathfrak{A}}_{\varphi,m} =& \{(a_1,\dots a_m) : (a_1,\dots,a_m,a_{m+1}) \in R^{\mathfrak{A}}_{\vartheta,m+1}\} \\ =& \{(a_1,\dots a_m) : \mathfrak{A} \models \exists x_{m+1}\vartheta(a_1,\dots,a_m,x_{m+1})\}. \end{aligned}$$

Für $\varphi = \exists x_i\vartheta(x_1,\dots,x_m)$ mit $i \le m$ setzen wir dagegen

$$R_{\varphi,m} := \pi_{1,\dots,i-1,m+1,i+1,\dots,m}R_{\vartheta,m+1}.$$

Da x_{m+1} in ϑ gar nicht vorkommt ist $(a_1,\dots,a_{m+1}) \in R_{\vartheta,m+1}$ genau dann, wenn $\mathfrak{A} \models \vartheta(a_1,\dots,a_m)$. Also gilt

$$\begin{aligned} R^{\mathfrak{A}}_{\varphi,m} =& \{(a_1,\dots a_m) : \text{ es gibt ein } (b_1,\dots,b_m,b_{m+1}) \in R^{\mathfrak{A}}_{\vartheta,m+1} \text{ so dass} \\ & \qquad a_j = b_j \text{ für } j \ne i \text{ und } a_i = b_{m+1}\} \\ =& \{(a_1,\dots a_m) : \mathfrak{A} \models \exists x_i\vartheta(a_1,\dots,a_{i-1},x_i,a_{i+1},\dots,a_m)\}. \end{aligned}$$

□

5.4 Theorien und elementar äquivalente Strukturen

Definition 5.10. Eine *Theorie* ist eine erfüllbare Menge $T \subseteq \mathrm{FO}(\tau)$ von Sätzen, die unter $\models$ abgeschlossen ist, d.h. es gilt für alle τ-Sätze ψ:

$$T \models \psi \;\Rightarrow\; \psi \in T.$$

Eine Theorie T ist *vollständig* , wenn für jeden Satz $\psi \in \mathrm{FO}(\tau)$ entweder $\psi \in T$ oder $\neg\psi \in T$.

Sei $\mathfrak{A}$ eine τ-Struktur. Die *Theorie von* $\mathfrak{A}$ ist $\mathrm{Th}(\mathfrak{A}) := \{\psi : \mathfrak{A} \models \psi\}$. Offensichtlich ist $\mathrm{Th}(\mathfrak{A})$ vollständig. Die Theorie einer τ-Modellklasse $\mathcal{K}$ ist

$$\mathrm{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A}\in\mathcal{K}} \mathrm{Th}(\mathfrak{A}).$$

Wenn Φ ein Axiomensystem für $\mathcal{K}$ ist, dann ist $\mathrm{Th}(\mathcal{K}) = \{\psi : \Phi \models \psi\}$. Natürlich ist nicht jede Theorie vollständig. Zum Beispiel enthält die Theorie der Gruppen weder den Satz $\forall x \forall y (x \circ y = y \circ x)$ noch seine Negation, da es sowohl kommutative wie nicht-kommutative Gruppen gibt. Jede Theorie T lässt sich aber zu einer vollständigen Theorie erweitern; für jedes Modell $\mathfrak{A} \models T$ ist $\mathrm{Th}(\mathfrak{A})$ eine vollständige Erweiterung von T.

Definition 5.11. Zwei τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ sind *elementar äquivalent* (kurz: $\mathfrak{A} \equiv \mathfrak{B}$), wenn $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$, d.h., wenn für alle τ-Sätze ψ gilt:

$$\mathfrak{A} \models \psi \iff \mathfrak{B} \models \psi.$$

Lemma 5.12. *Eine Theorie ist vollständig genau dann, wenn alle ihre Modelle elementar äquivalent sind.*

Beweis. Sei T eine vollständige Theorie. Für jedes Modell $\mathfrak{A} \models T$ gilt $T \subseteq \mathrm{Th}(\mathfrak{A})$ und wegen der Vollständigkeit von T daher sogar $T = \mathrm{Th}(\mathfrak{A})$. Also haben alle Modelle von T dieselbe Theorie.

Wenn andererseits T nicht vollständig ist, dann gibt es einen Satz ψ, so dass sowohl $T \cup \{\psi\}$ und $T \cup \{\neg\psi\}$ erfüllbar sind. T besitzt daher zwei nicht elementar äquivalente Modelle. □

Aus dem Isomorphielemma folgt unmittelbar, dass isomorphe Strukturen auch elementar äquivalent sind. Wie wir später sehen werden, gilt die Umkehrung dieser Aussage nicht.

Definition 5.13. Der *Quantorenrang* $\mathrm{qr}(\psi)$ einer Formel ψ ist definiert durch:

(1) $\mathrm{qr}(\psi) = 0$ für quantorenfreie ψ

(2) $\mathrm{qr}(\neg\psi) = \mathrm{qr}(\psi)$

(3) $\mathrm{qr}(\psi \circ \varphi) = \max(\mathrm{qr}(\psi), \mathrm{qr}(\varphi))$ für $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

(4) $\mathrm{qr}(\exists x\psi) = \mathrm{qr}(\forall x\psi) = \mathrm{qr}(\psi) + 1$

Der Quantorenrang ist also die maximale Schachtelungstiefe von Quantoren in der gegebenen Formel.

Beispiel. Der Quantorenrang von $\forall x(\exists y Pxy \rightarrow \forall z Pxz)$ ist 2. Eine äquivalente Formel in PNF ist $\forall x \forall y \forall z (Pxy \rightarrow Pxz)$. Man beachte, dass die Transformation in PNF in der Regel den Quantorenrang erhöht.

Definition 5.14. Zwei τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ sind *m-äquivalent*, (kurz $\mathfrak{A} \equiv_m \mathfrak{B}$), wenn für alle τ-Sätze ψ mit $\mathrm{qr}(\psi) \leq m$ gilt: $\mathfrak{A} \models \psi$ gdw. $\mathfrak{B} \models \psi$.

Wir erweitern die Begriffe der elementaren Äquivalenz und der m-Äquivalenz auf Strukturen mit Parametern, d.h. in denen zusätzlich gewisse Elemente ausgezeichnet sind. Seien $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen, und $\bar{a} = a_1, \ldots, a_r$, $\bar{b} = b_1, \ldots, b_r$Tupel von Elementen aus A bzw. B. Dann ist $(\mathfrak{A}, \bar{a}) \equiv (\mathfrak{B}, \bar{b})$, wenn für alle τ-Formeln $\psi(x_1, \ldots, x_r)$ gilt: $\mathfrak{A} \models \psi(\bar{a})$ gdw. $\mathfrak{B} \models \psi(\bar{b})$. Analog definiert man $(\mathfrak{A}, \bar{a}) \equiv_m (\mathfrak{B}, \bar{b})$.

5.5 Ehrenfeucht-Fraïssé Spiele

— That isn't the way to play it.
— Why not?
— 'Cause it isn't the way to win.
— Is there a way to win?
— Well, there's a way to lose more slowly.

Robert Mitchum, Jane Greer, in: *Out of the Past*

In diesem Abschnitt präsentieren wir eine spieltheoretische Deutung der elementaren Äquivalenz und der m-Äquivalenz. Der Einfachheit halber betrachten wir für den Rest dieses Kapitels nur relationale Strukturen.

Definition 5.15. Sei τ eine relationale Signatur und $\mathfrak{A}$, $\mathfrak{B}$ τ-Strukturen. Ein *lokaler* (oder *partieller) Isomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ ist eine injektive Abbildung $p : \mathrm{Def}(p) \to B$ wobei $\mathrm{Def}(p) \subseteq A$, so dass für alle $n \in \mathbb{N}$, alle Relationssymbole $R \in R^n(\tau)$ und alle $a_1, \dots, a_n \in \mathrm{Def}(p)$ gilt:

$$(a_1, \dots, a_n) \in R^{\mathfrak{A}} \iff (pa_1, \dots, pa_n) \in R^{\mathfrak{B}}.$$

Die Menge aller lokalen Isomorphismen von $\mathfrak{A}$ nach $\mathfrak{B}$ bezeichnen wir mit $\mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$.

Das Bild von p ist $\mathrm{Bild}(p) := \{pa : a \in \mathrm{Def}(p)\}$. Die *leere Abbildung* p mit $\mathrm{Def}(p) = \mathrm{Bild}(p) = \varnothing$ ist trivialerweise ein lokaler Isomorphismus. Ein nicht-leerer lokaler Isomorphismus ist ein Isomorphismus zwischen den von $\mathrm{Def}(p)$ und $\mathrm{Bild}(p)$ induzierten Substrukturen von $\mathfrak{A}$ und $\mathfrak{B}$. Wir identifizieren einen lokalen Isomorphismus p oft mit seinem Graphen, d.h. mit der Menge $\{(a, pa) : a \in \mathrm{Def}(p)\}$. Insbesondere nennen wir p endlich, wenn sein Graph endlich ist.

Beispiele. (1) Betrachte die Graphen

$p = \{(2, a), (3, b), (4, d)\}$ ist ein lokaler Isomorphismus.

(2) Seien $(\mathfrak{A}, <^{\mathfrak{A}})$ und $\mathfrak{B} = (B, <^{\mathfrak{B}})$ lineare Ordnungen und $a_1, \dots, a_n$ paarweise verschiedene Elemente von A. Eine Abbildung $p : a_1 \mapsto b_1, \dots, a_n \mapsto b_n$ ist ein lokaler Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ genau dann wenn eine Permutation $s : \{1, \dots, n\} \to \{1, \dots, n\}$ existiert sodass $a_{s(1)} <^{\mathfrak{A}} a_{s(2)} <^{\mathfrak{A}} \cdots <^{\mathfrak{A}} a_{s(n)}$ und $b_{s(1)} <^{\mathfrak{B}} b_{s(2)} <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_{s(n)}$.

Das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$. Das Ehrenfeucht-Fraïssé Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ wird von zwei Spielern nach folgenden Regeln gespielt.

Das *Spielfeld* besteht aus den Strukturen $\mathfrak{A}$ und $\mathfrak{B}$. Wir setzten dabei voraus, dass $A \cap B = \varnothing$. Die Spieler sind der *Herausforderer* und die *Duplikatorin*, oft auch bezeichnet als Spieler I und II. Eine Partie besteht aus m Zügen.

Im *i-ten Zug* bestimmt der Herausforderer entweder ein Element $a_i \in A$ oder ein $b_i \in B$. Die Duplikatorin antwortet, indem sie ein Element aus der jeweils anderen Struktur auswählt.

Nach m Zügen sind also Elemente $a_1, \dots, a_m$ aus $\mathfrak{A}$ und $b_1, \dots, b_m$ aus $\mathfrak{B}$ ausgezeichnet. Die Duplikatorin hat die Partie gewonnen, wenn die Menge $\{(a_1, b_1), \dots, (a_m, b_m)\}$ ein lokaler Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ ist. Anderenfalls hat der Herausforderer gewonnen.

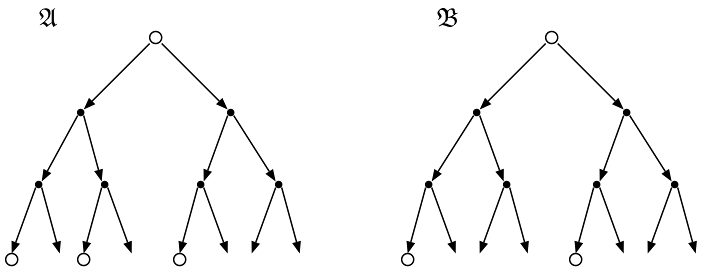
Nach i Zügen in $G_m(\mathfrak{A}, \mathfrak{B})$ ist eine *Position* $(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$ erreicht. Das verbleibende Teil-Spiel, mit $m - i$ Zügen, bezeichnen wir mit $G_{m-i}(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$.

Eine *Gewinn-Strategie* des Herausforderers für ein solches (Teil-)Spiel ist eine Funktion, die ihm in jeder erreichbaren Position mögliche Züge nennt, mit denen er die Partie gewinnt, egal wie seine Gegnerin spielt. Analog sind Gewinnstrategien für die Duplikatorin definiert.

Wir sagen, *der Herausforderer (bzw. die Duplikatorin) gewinnt das Spiel* $G_m(\mathfrak{A}, \mathfrak{B})$, wenn er (bzw. sie) eine Gewinnstrategie dafür hat. Per Induktion über die Anzahl der Züge zeigt man leicht, dass für jedes (Teil-)Spiel genau einer der Spieler eine Gewinnstrategie hat.

Beispiele. (1) Sei $\mathfrak{A} = (\mathbb{Z}, <)$, $\mathfrak{B} = (\mathbb{R}, <)$. Die Duplikatorin gewinnt $G_2(\mathfrak{A}, \mathfrak{B})$, aber der Herausforderer gewinnnt $G_3(\mathfrak{A}, \mathfrak{B})$.

(2) Für $\tau = \{E, P\}$ (wobei P einstelliges und E zweistelliges Relationssymbol) seien die folgenden Strukturen gegeben:



Auch hier gewinnt gewinnt der Herausforderer $G_3(\mathfrak{A}, \mathfrak{B})$, die Duplikatorin aber $G_2(\mathfrak{A}, \mathfrak{B})$.

Das Spiel $\mathbf{G}(\mathfrak{A}, \mathfrak{B})$. Eine wichtige Variante ist das Ehrenfeucht-Fraïssé Spiel $G(\mathfrak{A}, \mathfrak{B})$ ohne feste Beschränkung der Anzahl der Züge: In jeder Partie bestimmt der Herausforderer zunächst ein $m \in \mathbb{N}$, dann wird das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gespielt.

Der Herausforderer gewinnt also das Spiel $G(\mathfrak{A}, \mathfrak{B})$ genau dann, wenn es ein $m \in \mathbb{N}$ gibt so, dass er das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gewinnt. Anders ausgedrückt: die Duplikatorin gewinnt $G(\mathfrak{A}, \mathfrak{B})$ genau dann, wenn sie für jedes der Spiele $G_m(\mathfrak{A}, \mathfrak{B})$ eine Gewinnstrategie besitzt.

Satz 5.16 (Ehrenfeucht, Fraïssé). *Sei τ endlich und relational, $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen.*

(1) Folgende Aussagen sind äquivalent:

(i) $\mathfrak{A} \equiv \mathfrak{B}$

(ii) Die Duplikatorin gewinnt das Ehrenfeucht-Fraïssé Spiel $G(\mathfrak{A}, \mathfrak{B})$

(2) Für alle $m \in \mathbb{N}$ sind folgende Aussagen äquivalent:

(i) $\mathfrak{A} \equiv_m \mathfrak{B}$

(ii) Die Duplikatorin gewinnt $G_m(\mathfrak{A},\mathfrak{B})$.

Wir führen hier nur den Beweis, dass eine Gewinnstrategie der Duplikatorin für das Spiel $G(\mathfrak{A},\mathfrak{B})$ (bzw. für $G_m(\mathfrak{A},\mathfrak{B})$) die elementare Äquivalenz (bzw. m-Äquivalenz) von $\mathfrak{A}$ und $\mathfrak{B}$ impliziert.

Wir beweisen die folgende, etwas stärkere Aussage.

Satz 5.17. *Seien $\mathfrak{A},\mathfrak{B}$ τ-Strukturen, $\bar{a} = a_1,\dots,a_r \in A$, $\bar{b} = b_1,\dots,b_r \in B$. Wenn es eine Formel $\psi(\bar{x})$ mit $\mathrm{qr}(\psi) = m$ gibt, so dass $\mathfrak{A} \models \psi(\bar{a})$ und $\mathfrak{B} \models \neg\psi(\bar{b})$, dann hat der Herausforderer eine Gewinnstrategie für $G_m(\mathfrak{A},\bar{a},\mathfrak{B},\bar{b})$.*

Beweis. Sei $m = 0$. Quantorenfreie Formeln sind Boolesche Kombinationen von atomaren Formeln. Wenn $\mathfrak{A},\bar{a}$ und $\mathfrak{B},\bar{b}$ durch eine quantorenfreie Formel unterschieden werden, dann also bereits durch ein Atom. Daraus folgt, dass $\{(a_1,b_1),\dots,(a_r,b_r)\}$ kein partieller Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ ist, also gewinnt der Herausforderer $G_0(\mathfrak{A},\bar{a},\mathfrak{B},\bar{b})$.

Sei nun $\mathrm{qr}(\psi) = m > 0$, $\mathfrak{A} \models \psi(\bar{a})$ und $\mathfrak{B} \models \neg\psi(\bar{b})$. Die Formel $\psi(\bar{x})$ ist eine Boolesche Kombination von Formeln mit Quantorenrang $< m$ und von Formeln der Form $\exists y\varphi(\bar{x},y)$ mit $\mathrm{qr}(\varphi) = m-1$. Es muss also mindestens eine Formel dieser Gestalt geben, welche $\mathfrak{A},\bar{a}$ und $\mathfrak{B},\bar{b}$ unterscheidet. Wenn diese Formel Quantorenrang $< m$ hat, dann hat nach Induktionsvoraussetzung der Herausforderer eine Gewinnstrategie für $G_{m-1}(\mathfrak{A},\bar{a},\mathfrak{B},\bar{b})$ und also erst recht für $G_m(\mathfrak{A},\bar{a},\mathfrak{B},\bar{b})$. Andernfalls gibt es eine Formel $\exists y\varphi(\bar{x},y)$ mit $\mathrm{qr}(\varphi) = m-1$, so dass entweder

(1) $\mathfrak{A} \models \exists y\varphi(\bar{a},y)$ und $\mathfrak{B} \models \forall y\neg\varphi(\bar{b},y)$, oder

(2) $\mathfrak{A} \models \forall y\neg\varphi(\bar{a},y)$ und $\mathfrak{B} \models \exists y\varphi(\bar{b},y)$.

Im Fall (1) wählt der Herausforderer im ersten Zug ein $c \in A$ mit $\mathfrak{A} \models \varphi(\bar{a},c)$. Für jedes beliebige $d \in B$, welches die Duplikatorin wählen kann gilt $\mathfrak{B} \models \neg\varphi(\bar{b},d)$. Nach Induktionsvoraussetzung gewinnt der Herausforderer das Restspiel $G_{m-1}(\mathfrak{A},\bar{a},c,\mathfrak{B},\bar{b},d)$. Im Fall (2) gewinnt der Herausforderer, indem er ein $d \in B$ mit $\mathfrak{B} \models \varphi(\bar{b},d)$ wählt. Die Duplikatorin wählt ein beliebiges $c \in A$. Also ist nach diesem Zug eine Position $(\mathfrak{A},\bar{a},c,\mathfrak{B},\bar{b},d)$ erreicht, mit $\mathfrak{A} \models \neg\varphi(\bar{a},c)$ und $\mathfrak{B} \models \varphi(\bar{b},d)$. Da $\mathrm{qr}(\neg\varphi) = \mathrm{qr}(\varphi) = m-1$ gewinnt der Herausforderer nach Induktionsvoraussetzung das verbleibende Teilspiel $G_{m-1}(\mathfrak{A},\bar{a},c,\mathfrak{B},\bar{b},d)$. □

Daraus erhalten wir (indem wir $r = 0$ setzen und also Sätze betrachten) die Implikationen *(ii)* ⇒ *(i)* des Satzes von Ehrenfeucht und Fraïssé.

(1) Die Duplikatorin gewinnt $G(\mathfrak{A},\mathfrak{B}) \implies \mathfrak{A} \equiv \mathfrak{B}$

(2) Die Duplikatorin gewinnt $G_m(\mathfrak{A},\mathfrak{B}) \implies \mathfrak{A} \equiv_m \mathfrak{B}$.

Beispiel. Die Strukturen $\mathfrak{A} = (\mathbb{Z},<)$, $\mathfrak{B} = (\mathbb{R},<)$ lassen sich durch einen Satz ψ vom Quantorenrang 3 trennen, welcher ausdrückt, dass $<$ nicht dicht ist:

$$\psi := \exists x\exists y(x < y \wedge \forall z(\neg x < z \wedge z < y)).$$

Nach dem Satz von Ehrenfeucht-Fraïssé gilt $\mathfrak{A} \not\equiv_3 \mathfrak{B}$, d.h. der Herausforderer gewinnt $G_3(\mathfrak{A},\mathfrak{B})$. Eine Gewinnstrategie des Herausforderers besteht darin, in den ersten beiden Zügen zwei aufeinanderfolgende Elemente a und $a+1$ von $\mathbb{Z}$ zu wählen. Die Duplikatorin muss mit zwei Elementen $r,s \in \mathbb{R}$ antworten, so dass $r < s$. Aber dann gewinnt der Herausforderer, indem er im dritten Zug ein Element $t \in \mathbb{R}$ mit $r < t < s$ wählt.

Anwendungen. Dies liefert eine wichtige Methode, um zu zeigen, dass eine Modellklasse $\mathcal{K}$ *nicht* elementar definierbar ist. Wenn es gelingt, Strukturen $\mathfrak{A} \in \mathcal{K}$ und $\mathfrak{B} \notin \mathcal{K}$ zu finden, so dass die Duplikatorin das Spiel $G(\mathfrak{A}, \mathfrak{B})$ gewinnt, dann folgt, dass kein FO-Satz $\mathfrak{A}$ und $\mathfrak{B}$ unterscheiden kann, und damit auch kein FO-Satz $\mathcal{K}$ axiomatisiert.

Eine stärkere Variante der Ehrenfeucht-Fraïssé-Methode besteht darin, Folgen $(\mathfrak{A}_m)_{m \in \mathbb{N}}$, $(\mathfrak{B}_m)_{m \in \mathbb{N}}$ von τ-Strukturen zu konstruieren, so dass für alle m, $\mathfrak{A}_m \in \mathcal{K}$, $\mathfrak{B}_m \notin \mathcal{K}$ und die Duplikatorin das Spiel $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$ gewinnt. Die Annahme, dass $\mathcal{K}$ elementar ist, also $\mathcal{K} = \mathrm{Mod}(\psi)$ für ein $\psi \in \mathrm{FO}(\tau)$, führt nun sofort auf einen Widerspruch: Sei $m = \mathrm{qr}(\psi)$. Nach dem Satz von Ehrenfeucht und Fraïssé ist $\mathfrak{A}_m \equiv_m \mathfrak{B}_m$. Also $\mathfrak{A}_m \models \psi$ genau dann, wenn $\mathfrak{B}_m \models \psi$. Dies ist aber unmöglich, da $\mathfrak{A}_m \in \mathcal{K}$ und $\mathfrak{B}_m \notin \mathcal{K}$.

Beispiel. Sei $\tau = \varnothing$ und $\mathcal{K}_\infty$ die Klasse aller unendlichen τ-Strukturen, d.h. aller unendlichen Mengen. Wir haben gesehen, dass $\mathcal{K}$ durch eine unendliche Satzmenge Φ_∞ axiomatisiert wird. Mit der Ehrenfeucht-Fraïssé-Methode können wir nun zeigen, dass $\mathcal{K}_\infty$ *nicht* endlich axiomatisierbar ist.

Für alle $m \in \mathbb{N}$, setze $\mathfrak{A}_m = \mathbb{N}$ und $\mathfrak{B}_m = \{1, \ldots, m\}$. Offensichtlich gewinnt die Duplikatorin das Spiel $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$, also trennt kein Satz $\psi \in \mathrm{FO}(\varnothing)$ die endlichen von den unendlichen Mengen.

Transitive Hüllen sind nicht FO-definierbar. Eine fundamentale Einschränkung der Ausdrucksstärke von FO ist das Fehlen eines Rekursionsmechanismus. Eigenschaften, welche Rekursion (oder unbeschränkte Iteration) erfordern sind im Allgemeinen nicht FO-definierbar. Wir illustrieren dies am Beispiel der transitiven Hülle.

Satz 5.18. *Sei $\tau = \{E\}$ (die Signatur von Graphen). Es existiert* keine *Formel $\varphi(x, y) \in \mathrm{FO}(\tau)$ welche in jeder τ-Struktur $\mathfrak{A} = (A, E)$ die transitive Hülle von E definiert, d.h. für die gilt:*

$$\begin{aligned} \mathfrak{A} \models \varphi(a, b) &\iff \textit{es gibt in } \mathfrak{A} \textit{ einen } E\textit{-Pfad von } a \textit{ nach } b \\ &\iff \textit{es gibt } n > 0,\ c_0, \ldots, c_n \in A \textit{ mit } c_0 = a,\ c_n = b \\ &\qquad \textit{und } (c_i, c_{i+1} \in E \textit{ für alle } i < n. \end{aligned}$$

Satz 5.18 folgt unmittelbar aus dem folgendem Satz, den wir mit der Ehrenfeucht-Fraïssé-Methode beweisen.

Satz 5.19. *Es gibt keinen Satz $\psi \in \mathrm{FO}(\tau)$ so dass für jeden (endlichen, ungerichteten) Graph $G = (V, E)$ gilt:*

$$G \models \psi \iff G \textit{ zusammenhängend.}$$

Wenn Satz 5.18 falsch wäre, dann gäbe es eine Formel $\varphi(x, y)$ welche in G ausdrückt, dass ein Pfad von x nach y existiert. Aber dann würde $\psi := \forall x \forall y \varphi(x, y)$ ausdrückjen, dass G zusammenhängend ist.

Beweis. Wir definieren für jedes $m \in \mathbb{N}$ einen zusammenhängenden Graphen $\mathfrak{A}_m$ und einen nicht zusammenhängenden Graphen $\mathfrak{B}_m$ so dass die Duplikatorin das Spiel $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$ gewinnt.

Sei $\mathfrak{A}_m$ ein Zyklus der Länge 2^m und $\mathfrak{B}_m$ die disjunkte Vereinigung zweier Kopien von $\mathfrak{A}_m$. Zu zeigen ist:

Behauptung 1. *Die Duplikatorin gewinnt $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$.*

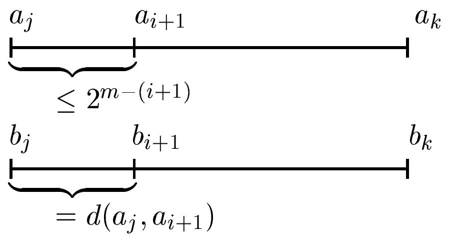
Auf Graphen haben wir für je zwei Knoten x, y eine Distanz $d(x,y)$, definiert als die Länge eines kürzesten Pfades von x nach y, wenn ein solcher existiert, und $d(x,y) = \infty$, wenn kein solcher Pfad existiert. Für Zahlen $u, v \in \mathbb{N} \cup \{\infty\}$ und $n \in \mathbb{N}$ schreiben wir $u =_n v$ wenn $u = v$ oder $u, v > n$.

Behauptung 2. *Die Duplikatorin kann so spielen, dass für alle $i \leq m$ und alle nach i Zügen ausgewählten Elemente $a_1, \ldots, a_i \in \mathfrak{A}_m$ und $b_1, \ldots, b_i \in \mathfrak{B}_m$ gilt:*

$$d(a_j, a_k) =_{2^{m-i}} d(b_j, b_k).$$

Für $i = 0, 1$ ist dies trivial. Wir nehmen an, die Behauptung sei nach i Schritten erfüllt und behandeln den Induktionsschritt durch Fallunterscheidung. Aus Symmetriegründen können wir annehmen, dass der Herausforderer im $(i+1)$-ten Zug ein Element $a_{i+1} \in \mathfrak{A})m$ auswählt. Sei a_j das am nächsten bei a_{i+1} liegende unter den bereits ausgewählten Elementen von $\mathfrak{A}_m$, d.h. $d(a_j, a_{i+1}) \leq d(a_k, a_{i+1})$ für alle $k \leq i$.

(a) Sei $d(a_j, a_{i+1} \leq 2^{m-(i+1)}$. Dann wählt die Duplikatorin b_{i+1} so, dass $d(b_j, b_{i+1} = d(a_j, a_{i+1})$.

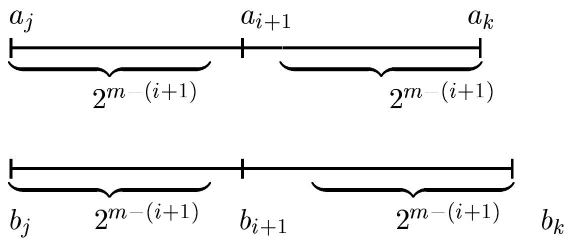


Da $d(a_j, a_k) =_{2^{m-i}} d(b_j, b_k))$ schliessen wir:

- wenn $d(a_j, a_k) = d(b_j, b_k)$, dann auch $d(a_{i+1}, a_k) = d(b_{i+1}, b_k)$.
- wenn $d(a_{i+1}, a_k) > 2^{m-i}$ und $d(b_{i+1}, b_k) > 2^{m-i}$, dann gilt $d(a_{i+1}, a_k) > 2^{m-i}/2 = 2^{m-(i+1)}$ und $d(b_{i+1}, b_k) > 2^{m-(i+1)}$.

Also gilt $d(a_{i+1}, a_j) = d(b_{i+1}, b_j)$ und $d(a_{i+1}, a_k) =_{2^{m-(i+1)}} d(b_{i+1}, d_k)$.

(b) Sei $d(a_{i+1}, a_j) > 2^{m-(i+1)}$. Die Duplikatorin wählt b_{i+1} so, dass $d(b_{i+1}, b_k > 2^{m-(i+1)}$ für alle $k \leq i$.



Am Ende des Spiels (nach m Zügen) gilt also $d(a_j, a_k) =_1 d(b_j, b_k)$ für alle $j, k \leq m$, d.h.

$$\begin{aligned} a_j = a_k &\iff b_k = b_k \\ (a_j, a_k) \in E &\iff (b_j, b_k) \in E \end{aligned}$$

Also ist die Abbildung $a_1 \mapsto b_1, \ldots, a_m \mapsto b_k$ ein lokaler Isdomorphismus von $\mathfrak{A}_m$ nach $\mathfrak{B}_m$, d.h. die Duplikatorin gewinnt $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$. $\square$

Kapitel 6

Vollständigkeitsatz, Kompaktheitssatz und Unentscheidbarkeit der Prädikatenlogik

6.1 Der Sequenzenkalkül

Wir erweitern den in Kapitel 1.6 beschriebenen aussagenlogischen Sequenzenkalkül auf die Prädikatenlogik.

Durch Einführen neuer Konstantensymbole können wir uns auf die Betrachtung von Sätzen beschränken und so die etwas lästigen Komplikationen vermeiden, die sich aus Konflikten zwischen freien und gebundenen Variablen ergeben können. Sei σ eine beliebige Signatur und seien $c_1, c_2, \ldots$ abzählbar viele, paarweise verschiedene und nicht in σ enthaltene Konstantensymbole. Wenn wir jede Formel $\psi(x_1, \ldots, x_n)$ mit den freien Variablen $x_1, \ldots, x_n$ durch den Satz $\psi(c_1, \ldots, c_n)$ ersetzten, dann können wir alle Fragen über Gültigkeit, Erfüllbarkeit und die Folgerungsbeziehung auf Sätze reduzieren.

Im Folgenden bezeichnet σ eine beliebige abzählbare Signatur und $\tau = \sigma \cup C$ für eine abzählbar unendliche Menge C von Konstanten, welche nicht in σ enthalten sind. Wenn von $\psi \in \mathrm{FO}(\tau)$ oder $\Gamma \subseteq \mathrm{FO}(\tau)$ die Rede ist, sind immer Sätze bzw. Satzmengen gemeint, es sei denn, wir deuten durch die Notation $\psi(x)$ explizit an, dass x in ψ frei vorkommt.

Definition 6.1. Eine *Sequenz* ist ein Ausdruck $\Gamma \Rightarrow \Delta$, wobei Γ, Δ endliche Mengen von Sätzen in $\mathrm{FO}(\tau)$ sind. Eine Sequenz $\Gamma \Rightarrow \Delta$ ist *korrekt*, wenn jedes Modell von Γ auch ein Modell mindestens einer Formel aus Δ ist. Die *Axiome* des Sequenzenkalküls sind alle Sequenzen der Form $\Gamma, \psi \Rightarrow \Delta, \psi$. Die *Schlussregeln* sind dieselben wie beim aussagenlogischen Sequenzenkalkül, erweitert um die Gleichheitsregel, die Substitutionsregeln und die Einführungsregeln für die Quantoren $\exists$ und $\forall$.

Die Gleichheitsregel ist

$$(=) \quad \frac{\Gamma, t = t \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$$

Die Substitutionsregeln erlauben das Austauschen von Termen. Die Schreibweise $t \doteq t'$ deutet an, dass entweder $t = t'$ oder $t' = t$ benutzt werden kann.

$$(S \Rightarrow) \quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, t \doteq t', \psi(t') \Rightarrow \Delta} \qquad (\Rightarrow S) \quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma, t \doteq t' \Rightarrow \Delta, \psi(t')}$$

Hier stehen t, t' für beliebige Grundterme aus $T(\tau)$; $\psi(x)$ ist eine beliebige Formel aus $\mathrm{FO}(\tau)$, in der keine andere Variable als x frei vorkommt, und $\psi(t)$ ist die Formel, die man daraus durch Substitution von t für x erhält.

Die Korrektheit der Gleichheitsregel ist trivial. Es ist auch leicht einzusehen, dass die Substitutionsregeln korrekt sind. Wir erläutern dies für $(\Rightarrow S)$: Sei $\Gamma \Rightarrow \Delta, \psi(t)$ eine gültige Sequenz, und $\mathfrak{A}$ ein Modell von $\Gamma, t \doteq t'$. Zu zeigen ist, dass $\mathfrak{A}$ dann entweder Modell einer Formel aus Δ oder Modell von $\psi(t')$ ist. Nehmen wir also an, dass in $\mathfrak{A}$ alle Formeln aus Δ falsch sind. Aber dann folgt $\mathfrak{A} \models \psi(t)$, denn $\Gamma \Rightarrow \Delta, \psi(t)$ ist gültig und $\mathfrak{A} \models \Gamma$. Da aber auch $\mathfrak{A} \models t = t'$, folgt $\mathfrak{A} \models \psi(t')$.

Die Einführungsregeln für $\exists$ und $\forall$ haben folgende Form:

$$(\exists \Rightarrow) \quad \frac{\Gamma, \psi(c) \Rightarrow \Delta}{\Gamma, \exists x \psi(x) \Rightarrow \Delta} \qquad (\Rightarrow \exists) \quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma \Rightarrow \Delta, \exists x \psi(x)}$$

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

$$(\forall \Rightarrow) \quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, \forall x \psi(x) \Rightarrow \Delta} \qquad (\Rightarrow \forall) \quad \frac{\Gamma \Rightarrow \Delta, \psi(c)}{\Gamma \Rightarrow \Delta, \forall x \psi(x)}$$

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

Beispiele. (1) Hier ist ein Beweis für die gültige Sequenz $\exists x \forall y Rxy \Rightarrow \forall y \exists x Rxy$, welcher die Anwendung der Quantorenregeln illustriert:

$Rcd \Rightarrow Rcd$	Axiom
$Rcd \Rightarrow \exists x Rxd$	$(\Rightarrow \exists)$
$\forall y Rcy \Rightarrow \exists x Rxd$	$(\forall \Rightarrow)$
$\forall y Rcy \Rightarrow \forall y \exists x Rxy$	$(\Rightarrow \forall)$
$\exists x \forall y Rxy \Rightarrow \forall y \exists x Rxy$	$(\exists \Rightarrow)$

(2) Um die Sequenz $Rfc, \forall x(fx = x) \Rightarrow Rffc$ abzuleiten, beginnt man mit dem Axiom $Rfc \Rightarrow Rfc$. Wenn wir $\psi(x) := Rfx$ wählen, dann ist dies die Sequenz $Rfc \Rightarrow \psi(c)$. Mit der Regel $(\Rightarrow S)$ können wir daraus die Sequenz $Rfc, fc = c \Rightarrow \psi(fc)$, also $Rfc, fc = c \Rightarrow Rffc$ ableiten. Durch Anwendung der Regel $(\forall \Rightarrow)$ erhalten wir daraus eine Ableitung von $Rfc, \forall x(fx = x) \Rightarrow Rffc$.

Übung 6.1. Beweisen Sie die Korrektheit der Quantorenregeln. Zeigen Sie, dass in den Regeln $(\exists \Rightarrow)$ und $(\Rightarrow \forall)$ die Bedingung, dass c nicht in Γ, ψ und Δ vorkommt, nicht weggelassen werden kann.

Die weiteren wesentlichen Begriffe können unmittelbar vom aussagenlogischen Sequenzenkalkül übernommen werden:

Die Menge der *ableitbaren Sequenzen* ist die kleinste Menge, welche alle Axiome umfasst und mit jeder Instanz der oberen Zeile einer Schlussregel auch die entsprechende Instanz der unteren Zeile enthält. Ein *Beweis* ist ein beschrifteter Baum, so dass alle Blätter mit Axiomen, alle inneren Knoten mit der Konklusion einer Schlussregel und deren Kinder mit den Prämissen derselben Regel beschriftet sind. Tabelle 6.1 fasst alle Regeln des Sequenzenkalküls nochmals zusammen.

Tabelle 6.1: Die Regeln des Sequenzenkalküls

$$(=)\quad \frac{\Gamma, t = t \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$$

$$(S \Rightarrow)\quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, t \doteq t', \psi(t') \Rightarrow \Delta} \qquad\qquad (\Rightarrow S)\quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma, t \doteq t' \Rightarrow \Delta, \psi(t')}$$

$$(\neg \Rightarrow)\quad \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma, \neg\psi \Rightarrow \Delta} \qquad\qquad (\Rightarrow \neg)\quad \frac{\Gamma, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\psi}$$

$$(\vee \Rightarrow)\quad \frac{\Gamma, \psi \Rightarrow \Delta \qquad \Gamma, \vartheta \Rightarrow \Delta}{\Gamma, \psi \vee \vartheta \Rightarrow \Delta} \qquad\qquad (\Rightarrow \vee)\quad \frac{\Gamma \Rightarrow \Delta, \psi, \vartheta}{\Gamma \Rightarrow \Delta, \psi \vee \vartheta}$$

$$(\wedge \Rightarrow)\quad \frac{\Gamma, \psi, \vartheta \Rightarrow \Delta}{\Gamma, \psi \wedge \vartheta \Rightarrow \Delta} \qquad\qquad (\Rightarrow \wedge)\quad \frac{\Gamma \Rightarrow \Delta, \psi \qquad \Gamma \Rightarrow \Delta, \vartheta}{\Gamma \Rightarrow \Delta, \psi \wedge \vartheta}$$

$$(\rightarrow\Rightarrow)\quad \frac{\Gamma \Rightarrow \Delta, \psi \qquad \Gamma, \vartheta \Rightarrow \Delta}{\Gamma, \psi \rightarrow \vartheta \Rightarrow \Delta} \qquad\qquad (\Rightarrow\rightarrow)\quad \frac{\Gamma, \psi \Rightarrow \Delta, \vartheta}{\Gamma \Rightarrow \Delta, \psi \rightarrow \vartheta}$$

$$(\exists \Rightarrow)\quad \frac{\Gamma, \psi(c) \Rightarrow \Delta}{\Gamma, \exists x \psi(x) \Rightarrow \Delta} \qquad\qquad (\Rightarrow \exists)\quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma \Rightarrow \Delta, \exists x \psi(x)}$$

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

$$(\forall \Rightarrow)\quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, \forall x \psi(x) \Rightarrow \Delta} \qquad\qquad (\Rightarrow \forall)\quad \frac{\Gamma \Rightarrow \Delta, \psi(c)}{\Gamma \Rightarrow \Delta, \forall x \psi(x)}$$

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

Da die Axiome des Sequenzenkalküls gültig sind, und die Schlussregeln gültige Sequenzen immer in gültige Sequenze überführen, folgt, dass im Sequenzenkalkül nur gültige Sequenzen ableitbar sind.

Satz 6.2 (Korrektheitssatz für den Sequenzenkalkül). *Jede im Sequenzenkalkül ableitbare Sequenz ist gültig.*

6.2 Der Vollständigkeitssatz

Ableitbarkeit in Theorien. Aus dem Sequenzenkalkül erhält man auch einen Ableitungsbegriff für einen einzelnen Satz oder eine Sequenz aus einer Menge von Hypthesen, z.B. aus den Axiomen einer mathematischen Theorie.

Definition 6.3. Sei $\Phi \subseteq \mathrm{FO}(\sigma)$ eine Menge von Sätzen. Ein Satz ψ ist *ableitbar* aus dem Axiomensystem Φ, (kurz $\Phi \vdash \psi$), wenn eine endliche Teilmenge Γ von Φ existiert, so dass die Sequenz $\Gamma \Rightarrow \psi$ im Sequenzenkalkül ableitbar ist. Eine Sequenz $\Gamma \Rightarrow \Delta$ ist ableitbar aus Φ, wenn es eine ableitbare Sequenz $\Gamma, \Gamma' \Rightarrow \Delta$ gibt mit $\Gamma' \subseteq \Phi$.

Die Ableitbarkeit von Sequenzen und die Ableitbarkeit von einzelnen Sätzen sind im Wesentlichen austauschbare Begriffe, denn die Sequenz $\Gamma \Rightarrow \Delta$ ist ableitbar aus Φ genau dann, wenn $\Phi \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta$.

Es gibt auch Satzmengen Φ aus denen *jeder* Satz (der entsprechenden Signatur) ableitbar ist. Eine solche Menge nennen wir *inkonsistent*. Aufgrund der Korrektheit des Sequenzenkalküls sind inkonsistente Mengen unerfüllbar.

Beispiel. Jede Menge, welche einen Satz und gleichzeitig auch dessen Negation enthält, ist inkonsistent. In der Tat können wir jede Sequenz der Form $\psi, \neg\psi \Rightarrow \varphi$ mit der Regel $(\neg \Rightarrow)$ aus dem Axiom $\psi \Rightarrow \psi, \varphi$ ableiten.

Wenn nicht jeder Satz aus Φ ableitbar ist, dann nennen wir Φ *konsistent*. Offensichtlich ist Φ konsistent genau dann, wenn jede endliche Teilmenge von Φ konsistent ist. Man beachte, dass Konsistenz und Ableitbarkeit ($\vdash$) *syntaktische* Begriffe sind, da sie sich auf Formelmengen und Sätze als sprachliche Objekte und nicht auf ihre Bedeutung beziehen. Die zugehörigen semantischen Begriffe sind die Erfüllbarkeit und die Folgerungsbeziehung ($\models$).

Der Korrektheitssatz für den Sequenzenkalkül impliziert: Wenn $\Phi \vdash \psi$, dann auch $\Phi \models \psi$. Der Vollständigkeitssatz besagt, dass auch die Umkehrung gilt.

Satz 6.4 (Vollständigkeitssatz für den Sequenzenkalkül). *Für jede Satzmenge* $\Phi \subseteq \mathrm{FO}(\sigma)$ *und jeden Satz* $\psi \in \mathrm{FO}(\sigma)$ *gilt:*

(i) $\Phi \models \psi \iff \Phi \vdash \psi$

(ii) Φ *erfüllbar* $\iff$ Φ *konsistent.*

6.3 Der Beweis des Vollständigkeitssatz

Bemerkung. In der Vorlesung wird nur ein kurze Skizze des Beweises präsentiert. Sie finden aber hier im Skript einen vollständigen Beweis.

Man beweist den Vollständigkeitssatz, indem man für jede beliebige, nicht aus Φ ableitbare Sequenz $\Gamma \Rightarrow \Delta$ ein Modell $\mathfrak{A}$ von $\Phi \cup \Gamma \cup \neg\Delta$ konstruieren. Dabei ist $\neg\Delta := \{\neg\psi : \psi \in \Delta\}$.

Daraus erhält man sofort die beiden Aussagen des Vollständigkeitssatzes:

(i) Wir wissen bereits, dass $\Phi \vdash \psi \;\Rightarrow\; \Phi \models \psi$. Wenn $\Phi \nvdash \psi$, dann ist insbesondere die Sequenz $\varnothing \Rightarrow \psi$ nicht aus Φ ableitbar. Die Existenz eines Modells $\mathfrak{A} \models \Phi \cup \{\neg\psi\}$ bedeutet aber, dass $\Phi \not\models \psi$.

(ii) Wir wissen bereits, dass jede erfüllbare Menge konsistent ist. Sei umgekehrt Φ konsistent. Dann gibt es ein ψ, so dass $\Phi \nvdash \psi$ und daher (nach *(i)*) auch $\Phi \not\models \psi$. Also ist $\Phi \cup \{\neg\psi\}$ und daher insbesondere Φ erfüllbar.

Wenn wir $\Phi = \varnothing$ setzen, zeigt dies insbesondere, dass jede gültige Sequenz im Sequenzenkalkül ableitbar ist.

Es bleibt also die Aufgabe, für jede nicht aus Φ ableitbare Sequenz $\Gamma \Rightarrow \Delta$ ein Modell von $\Phi \cup \Gamma \cup \neg\Delta$ zu konstruieren

6.3.1 Herbrandstrukturen und kanonische Modelle

Als Vorbereitung für die Modellkonstruktion behandeln wir Mengen von atomaren Sätzen. Wir definieren den Begriff einer Herbrandstruktur und konstruieren daraus, durch Übergang zu einer geeigneten Quotientenstruktur, für jede unter Substitution abgeschlossenen Menge von atomaren Aussagen das sogenannte *kanonische Modell*.

Definition 6.5. Eine *Herbrandstruktur* zu einer Signatur τ ist eine τ-Struktur $\mathfrak{H}$, deren Universum die Menge aller Grundterme der Signatur τ ist und deren Funktionssymbole durch ihre natürliche Operation auf den Termen interpretiert werden: Für n-stelliges $f \in \tau$ ist $f^{\mathfrak{H}}(t_1, \dots, t_n) := ft_1 \cdots t_n$. Die Interpretation der Relationssymbole aus τ ist beliebig.

Eine Herbrandstruktur $\mathfrak{H}$ ist eine Struktur, deren algebraisches Redukt gerade die Termalgebra über der leeren Variablenmenge ist. Beachte, dass in $\mathfrak{H}$ jeder Grundterm durch sich selbst interpretiert ist: $t^{\mathfrak{H}} = t$.

Sei Σ eine Menge von atomaren τ-Sätzen. Mit $\mathfrak{H}(\Sigma)$ bezeichnen wir die Herbrandstruktur mit folgender Interpretation der Relationssymbole: Für n-stelliges $R \in \tau$ ist

$$R^{\mathfrak{H}(\Sigma)} = \{(t_1, \dots, t_n) : Rt_1 \cdots t_n \in \Sigma\}.$$

Im Allgemeinen ist $\mathfrak{H}(\Sigma)$ *kein* Modell von Σ: Seien t und t' zwei (syntaktisch) verschiedene Terme, so dass aber Σ die Formel $t = t'$ enthält. Dann ist $\mathfrak{H}(\Sigma)$ Modell von $t \neq t'$ und daher kein Modell von Σ. Es ist also offensichtlich notwendig, Gleichheiten herauszufaktorisieren.

Definition 6.6. Eine Menge Σ von atomaren Sätzen in $\mathrm{FO}(\tau)$ ist *abgeschlossen unter Substitution*, wenn für jede atomare Formel $\psi(x)$ und alle Grundterme $t, t' \in T(\tau)$ gilt:

(i) Σ enthält die Gleichung $t = t$.

(ii) Wenn $t = t'$ und $\psi(t)$ zu Σ gehören, dann auch $\psi(t')$.

Beispiel. Sei $\mathfrak{A}$ eine τ-Struktur und Σ die Menge aller atomaren Sätze φ, so dass $\mathfrak{A} \models \varphi$. Dann ist Σ abgeschlossen unter Substitution.

Für beliebige Grundterme $t, t' \in T(\tau)$ setzen wir nun: $t \sim t'$ genau dann, wenn Σ die Formel $t = t'$ enthält.

Lemma 6.7. *Sei Σ abgeschlossen unter Substitution. Dann ist $\sim$ eine Kongruenzrelation auf $\mathfrak{H}(\Sigma)$.*

Beweis. Wir zeigen zuerst, dass $\sim$ eine Äquivalenzrelation ist. Nach Bedingung *(i)* von Definition 6.6 ist $\sim$ reflexiv. Sei nun $t \sim t'$ und also $t = t' \in \Sigma$. Wenn $\psi(x)$ die Formel $x = t$ ist, dann ist $\psi(t)$ die Gleichung $t = t$ und also in Σ. Nach Bedingung *(ii)* von Definition 6.6 enthält Σ dann auch $\psi(t')$; dies ist aber gerade die Gleichung $t' = t$. Also folgt $t' \sim t$. Schliesslich nehmen wir an, dass $t \sim t'$ und $t' \sim t''$. Sei $\psi(x)$ die Formel $t = x$. Also enthält Σ $\psi(t')$ und daher auch $\psi(t'')$; dies ist aber die Gleichung $t = t''$. Also $t \sim t''$.

Es bleibt zu zeigen, dass $\sim$ mit den Funktionen und Relationen von $\mathfrak{H}(\Sigma)$ kompatibel ist. Sei f ein n-stelliges Funktionssymbol und seien $s_1 \sim t_1, \ldots, s_n \sim t_n$. Wir müssen zeigen, dass $fs_1 \cdots s_n \sim ft_1 \cdots t_n$. Zu diesem Zweck sei $\psi_i(x)$ die Gleichung $fs_1 \cdots s_n = ft_1 \cdots t_{i-1}xs_{i+1} \cdots s_n$ für $i = 1, \ldots, n$. Per Induktion zeigen wir, dass $\psi_i(t_i) \in \Sigma$.

Die Formel $\psi_1(s_1)$ ist einfach $fs_1 \cdots s_n = fs_1 \cdots s_n$ und daher in Σ. Also ist auch $\psi_1(t_1) \in \Sigma$. Beachte nun, dass $\psi_{i+1}(s_{i+1})$ und $\psi_i(t_i)$ dieselbe Formel bezeichnen, nämlich $fs_1 \cdots s_n = ft_1 \cdots t_i s_{i+1} s_{i+2} \cdots s_n$. Nach Induktionsvoraussetzung gehört also $\psi_{i+1}(s_{i+1})$ zu Σ, und daher auch $\psi_{i+1}(t_{i+1})$. Damit folgt, dass $\psi_n(t_n) \in \Sigma$. Dies ist aber gerade die Gleichung $fs_1 \cdots s_n = ft_1 \cdots t_n$.

Schliesslich müssen wir zeigen, dass für jedes n-stellige Relationssymbol R und $s_1 \sim t_1, \ldots, s_n \sim t_n$ folgt

$$\mathfrak{H}(\Sigma) \models Rs_1 \cdots s_n \leftrightarrow Rt_1 \cdots t_n.$$

Die Argumentation ist wie bei den Funktionssymbolen, unter Verwendung der Formeln $\psi_i(x) := Rt_1 \cdots t_{i-1}xs_{i+1} \cdots s_n$. □

Wir können also die Faktorstruktur $\mathfrak{A}(\Sigma) := \mathfrak{H}(\Sigma)/_\sim$ bilden. Wir bezeichnen mit $[t]$ die Äquivalenzklasse von t bezüglich $\sim$; das Universum von $\mathfrak{A}(\Sigma)$ ist also die Menge $\{[t] : t \text{ Grundterm in } T(\tau)\}$ der Äquivalenzklassen aller Grundterme. Offensichtlich wird in $\mathfrak{A}(\Sigma)$ jeder Grundterm t durch seine Äquivalenzklasse interpretiert: $t^{\mathfrak{A}(\Sigma)} = [t]$. Unmittelbar aus der Definition folgt:

Lemma 6.8. *Für jeden atomaren Satz ψ aus $\mathrm{FO}(\tau)$ gilt: $\mathfrak{A}(\Sigma) \models \psi \iff \psi \in \Sigma$.*

$\mathfrak{A}(\Sigma)$ heisst das *kanonische Modell* von Σ. Leider lässt sich Lemma 6.8 nicht direkt auf Mengen von nicht-atomaren Sätzen übertragen. Betrachte etwa die Menge $\Sigma := \{t = t : t \text{ ein Grundterm}\} \cup \{\exists x Rx\}$. Diese Menge ist trivialerweise abgeschlossen unter Substitution, enthält aber keine Aussage der Form Rt. Daher ist $R^{\mathfrak{A}(\Sigma)} = \varnothing$ und also $\mathfrak{A}(\Sigma) \not\models \exists x Rx$. Analoges gilt für die Menge $\{t = t : t \text{ ein Grundterm}\} \cup \{Rx \vee Ry\}$. Man sieht aus diesen Beispielen, dass Σ neben der Abgeschlossenheit unter Substitution noch weitere Abschlusseigenschaften besitzen muss, damit $\mathfrak{A}(\Sigma) \models \Sigma$ gilt.

6.3.2 Hintikka-Mengen und Modell-Existenz-Satz

Sei $\Gamma \Rightarrow \Delta$ eine nicht aus Φ ableitbare Sequenz. Wir werden eine unendliche Folge von nicht aus Φ ableitbaren Sequenzen $\Gamma_n \Rightarrow \Delta_n$ konstruieren und damit eine Satzmenge gewinnen, welche $\Phi \cup \Gamma \cup \neg\Delta$ umfasst und welche hinreichende Abschlusseigenschaften besitzt, um zu garantieren, dass die dadurch definierte kanonische Struktur ein Modell von $\Phi \cup \Gamma \cup \neg\Delta$ ist.

Um den Beweis zu vereinfachen, beschränken wir uns auf reduzierte Sätze (d.h. solche, die aus den Atomen mittels $\vee, \neg$ und $\exists$ aufgebaut sind).

Obwohl wir im Sequenzenkalkül auch Schlussregeln für $\wedge, \rightarrow$ und $\forall$ angegeben haben, bedeutet die Reduktion auf reduzierte Sätze keine Einschränkung der Allgemeinheit: Sei etwa $\Gamma_0 \Rightarrow \Delta_0$ eine nicht-ableitbare Sequenz bestehend aus beliebigen Sätzen und sei $\Gamma_1 \Rightarrow \Delta_1$ die Sequenz, die wir erhalten, indem wir jeden Satz durch eine äquivalente reduzierte Variante ersetzen.

Zunächst überlegt man, dass auch $\Gamma_1 \Rightarrow \Delta_1$ nicht ableitbar ist. Wir zeigen exemplarisch, dass die Ableitung einer Sequenz der Form $\Gamma, (\psi \wedge \varphi) \Rightarrow \Delta$ aus $\Gamma, \psi \Rightarrow \Delta$ und $\Gamma, \varphi \Rightarrow \Delta$ mittels der Regel $(\wedge \Rightarrow)$ simuliert werden kann durch eine Ableitung der äquivalenten Sequenz $\Gamma, \neg(\neg\psi \vee \neg\varphi) \Rightarrow \Delta$ mit den Regeln $(\Rightarrow \neg), (\neg \Rightarrow)$ und $(\Rightarrow \vee)$.

$$\dfrac{\dfrac{\dfrac{\Gamma, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\psi} \qquad \dfrac{\Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}}{\Gamma \Rightarrow \Delta, (\neg\psi \vee \neg\varphi)}}{\Gamma \neg(\neg\psi \vee \neg\varphi) \Rightarrow \Delta}$$

Die Argumentation für Sequenzen mit Sätzen der Form $\psi \rightarrow \varphi$ und $\forall x \psi(x)$ ist analog.

Umgekehrt ist ein Modell von $\Gamma \wedge \neg\Delta$ natürlich auch ein Modell von $\Gamma' \wedge \neg\Delta'$ und erbringt damit den Nachweis, dass $\Gamma' \Rightarrow \Delta'$ nicht korrekt ist.

Sei $\Phi \subseteq \mathrm{FO}(\sigma)$ und sei $\tau = \sigma \cup C$ für eine abzählbar unendliche Menge von neuen Konstantensymbolen. Wir fixieren zunächst eine Aufzählung $(\varphi_0, t_0), (\varphi_1, t_1), \ldots,$ in der jedes Paar (φ, t), bestehend aus einem Satz $\varphi \in \mathrm{FO}(\tau)$ und einem Grundterm $t \in T(\tau)$ unendlich oft vorkommt, und eine Aufzählung $\psi_0(x_0), \psi_1(x_1), \ldots$ aller atomaren $\mathrm{FO}(\tau)$-Formeln mit genau einer freien Variablen.

Wir definieren induktiv aufsteigende Folgen $\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots$ und $\Delta_0 \subseteq \Delta_1 \subseteq \cdots$ wie folgt: Sei $\Gamma_0 := \Gamma$ und $\Delta_0 := \Delta$. Wir nehmen nun an, Γ_n und Δ_n seien bereits konstruiert und $\Gamma_n \Rightarrow \Delta_n$ sei nicht aus Φ ableitbar.

(a) Sei φ_n eine Formel aus Φ oder eine Gleichung $t = t$. Dann setze $\Gamma_{n+1} := \Gamma_n, \varphi_n$ und $\Delta_{n+1} := \Delta_n$.

Die Sequenz $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ ist nicht aus Φ ableitbar, denn sonst wäre auch $\Gamma_n \Rightarrow \Delta_n$ aus Φ ableitbar.

(b) Sei φ_n von der Gestalt $t = t'$. Wenn $\varphi_n \in \Gamma_n$ und ein $m \in \mathbb{N}$ existiert, so dass $\psi_m(t') \in \Gamma_n$, aber $\psi_m(t) \notin \Gamma_n$, dann wähle das kleinste solche m und setze $\Gamma_{n+1} := \Gamma_n, \psi_m(t)$ und $\Delta_{n+1} := \Delta_n$.

Die Sequenz $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ ist nicht aus Φ ableitbar, denn sonst würde mit Regel $(S \Rightarrow)$ folgen, dass auch $\Gamma_n, t = t', \psi_m(t') \Rightarrow \Delta_n$ ableitbar ist. Da $t = t'$ und $\psi_m(t')$ bereits in Γ_n enthalten sind, wäre also $\Gamma_n \Rightarrow \Delta_n$ ableitbar, im Widerspruch zur Induktionsannahme.

(c) Sei $\varphi_n := \neg\psi$. Wenn $\varphi_n \in \Gamma_n$, dann setze $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} := \Delta_n, \psi$. Wenn $\varphi_n \in \Delta_n$, dann setze $\Gamma_{n+1} := \Gamma_n, \psi$ und $\Delta_{n+1} := \Delta_n$.

Mit den Regeln $(\neg \Rightarrow)$ und $(\Rightarrow \neg)$ folgt, dass $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ nicht aus Φ ableitbar ist.

(d) Sei $\varphi_n = \psi \vee \vartheta$. Wenn $\varphi_n \in \Gamma_n$, dann setzen wir $\Delta_{n+1} := \Delta_n$ und können aufgrund der Regel ($\vee \Rightarrow$) entweder $\Gamma_{n+1} := \Gamma_n, \psi$ oder $\Gamma_{n+1} := \Gamma_n, \vartheta$ so wählen, dass $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ nicht ableitbar ist. Wenn $\varphi_n \in \Delta_n$, dann setzen wir $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} = \Delta_n, \psi, \vartheta$ und verwenden die Regel ($\Rightarrow \vee$).

(e) Sei φ_n von der Gestalt $\exists x \psi(x)$. Wenn $\varphi_n \in \Gamma_n$, dann wähle ein $c \in C$, welches in Γ_n und Δ_n nicht vorkommt. Setze $\Gamma_{n+1} := \Gamma_n, \psi(c)$ und $\Delta_{n+1} := \Delta_n$. Die Sequenz $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ ist nicht ableitbar; andernfalls würde (da c in Φ, Γ_n und Δ_n nicht vorkommt) mit der Regel ($\exists \Rightarrow$) folgen, dass auch $\Gamma_n, \exists x \psi(x) \Rightarrow \Delta_n$ und also $\Gamma_n \Rightarrow \Delta_n$ aus Φ ableitbar wäre.

Wenn $\varphi_n \in \Delta_n$, dann setze $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} = \Delta_n, \psi(t_n)$. Mit Regel ($\Rightarrow \exists$) folgt, dass $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ nicht ableitbar ist.

In allen andern Fällen sei $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} := \Delta_n$. Man beachte, dass aufgrund von Schritt (a) der Konstruktion Φ in $\bigcup_{n \in \mathbb{N}} \Gamma_n$ enthalten ist.

Lemma 6.9. *Die Mengen $\Gamma^* := \bigcup_{n \in \mathbb{N}} \Gamma_n$ und $\Delta^* := \bigcup_{n \in \mathbb{N}} \Delta_n$ besitzen folgende Eigenschaften:*

(1) Γ^* und Δ^* sind disjunkt.

(2) Die atomaren Sätze in Γ^* sind abgeschlossen unter Substitution (gemäss Defintion 6.6).

(3) Wenn $\neg\psi \in \Gamma^*$, dann ist $\psi \in \Delta^*$. Wenn $\neg\psi \in \Delta^*$, dann ist $\psi \in \Gamma^*$.

(4) Wenn $\psi \vee \vartheta \in \Gamma^*$, dann gehört ψ oder ϑ zu Γ^*. Wenn $\psi \vee \vartheta \in \Delta^*$ dann gehören ψ und ϑ zu Δ^*.

(5) Wenn $\exists x \psi(x) \in \Gamma^*$, dann gibt es einen Grundterm t, so dass $\psi(t) \in \Gamma^*$. Wenn $\exists x \psi(x) \in \Delta^*$, dann ist $\psi(t) \in \Delta^*$ für alle Grundterme t.

Beweis. Die Eigenschaften ergeben sich unmittelbar aus der Konstruktion der Sequenzen $\Gamma_n \Rightarrow \Delta_n$

(1) Wenn $\psi \in \Gamma^* \cap \Delta^*$, dann gibt es ein $n \in \mathbb{N}$, so dass $\psi \in \Gamma_n \cap \Delta_n$. Aber dann wäre $\Gamma_n \Rightarrow \Delta_n$ ein Axiom und somit ableitbar.

(2) Die Schritte (a), (b) in der Konstruktion garantieren, dass Γ^* alle Gleichungen $t = t$ enthält, und mit $t = t'$ und $\psi(t)$ auch $\psi(t')$, für alle atomaren Formeln $\psi(x)$.

(3) Wenn $\neg\psi \in \Gamma^*$, dann gibt es (da jeder Satz in der Aufzählung $\varphi_0, \varphi_1, \dots$ unendlich oft vorkommt) ein hinreichend grosses n, so dass $\varphi_n = \neg\psi \in \Gamma_n$. Nach Schritt (c) der Konstruktion folgt, dass $\psi \in \Delta^*$. Der Fall, dass $\neg\psi \in \Delta^*$ wird analog behandelt.

(4) Wenn $\psi \vee \vartheta \in \Gamma^*$, dann gibt es ein n, so dass $\varphi_n = \psi \vee \vartheta \in \Gamma_n$. Nach Schritt ($d$) ist entweder ψ oder ϑ in Γ_{n+1}. Das Argument für $\psi \vee \vartheta \in \Delta^*$ ist analog.

(5) Wenn $\exists x \psi(x)$ in Γ^*, dann gibt es nach Schritt (e) ein c, so dass $\psi(c) \in \Gamma^*$. Wenn $\exists x \psi(x) \in \Delta^*$ und t ein beliebiger Grundterm ist, dann gibt es hinreichend grosse n, so dass φ_n die Formel $\exists x \psi(x)$ und t_n der Term t ist. Nach Konstruktion ist $\psi(t_n) \in \Delta_{n+1}$.

□

Definition 6.10. Sei Γ^*, Δ^* ein Paar von Satzmengen welches die Eigenschaften (1)–(5) erfüllt. Dann heisst $\Gamma^* \cup \neg\Delta^*$ eine *Hintikka-Menge.*

Theorem 6.11 (Modell-Existenz-Satz). *Jede Hintikka-Menge besitzt ein Modell.*

Beweis. Sei $T = \Gamma^* \cup \neg\Delta^*$ eine Hintikka-Menge und Σ die Menge aller Atome in Γ^*. Nach Bedingung (2) ist Σ abgeschlossen unter Substitution. Wir behaupten, dass $\mathfrak{A}(\Sigma)$, die kanonische Struktur zu Σ, ein Modell von T ist. Dazu beweisen wir per Induktion über den Formelaufbau, dass für jeden Satz φ gilt:

$$\begin{aligned} \varphi \in \Gamma^* &\implies \mathfrak{A}(\Sigma) \models \varphi \\ \varphi \in \Delta^* &\implies \mathfrak{A}(\Sigma) \models \neg\varphi \end{aligned}$$

(i) Für atomare Sätze ist dies bereits bewiesen (Lemma 6.8).

(ii) Sei $\varphi = \neg\psi$. Wenn $\varphi \in \Gamma^*$, dann ist $\psi \in \Delta^*$. Per Induktionsvoraussetzung folgt $\mathfrak{A}(\Sigma) \models \neg\psi$. Wenn $\varphi \in \Delta^*$, dann ist $\psi \in \Gamma^*$, also $\mathfrak{A}(\Sigma) \models \psi$ und daher $\mathfrak{A}(\Sigma) \models \neg\varphi$.

(iii) Sei $\varphi := \psi \vee \vartheta$. Wenn $\varphi \in \Gamma^*$, dann ist entweder ψ oder ϑ in Γ^* und damit nach Induktionsvoraussetzung wahr in $\mathfrak{A}(\Sigma)$. Wenn $\varphi \in \Delta^*$, dann sind ψ und ϑ in Δ^*, also $\mathfrak{A}(\Sigma) \models \neg\varphi$.

(iv) Sei $\varphi = \exists x\psi(x)$. Wenn $\varphi \in \Gamma^*$, dann gibt es ein t, so dass $\psi(t) \in \Gamma^*$. Also gilt per Induktionsvoraussetzung $\mathfrak{A}(\Sigma) \models \psi(t)$ und daher $\mathfrak{A}(\Sigma) \models \exists x\psi$. Wenn $\exists x\varphi \in \Delta^*$, dann ist $\psi(t) \in \Delta^*$ und daher per Induktionsvoraussetzung $\mathfrak{A}(\Sigma) \models \neg\psi(t)$ für alle t. Da jedes Element von $\mathfrak{A}(\Sigma)$ einen Grundterm interpretiert, folgt $\mathfrak{A}(\Sigma) \models \neg\exists x\psi(x)$.

□

Wir sind ausgegangen von einer Satzmenge Φ und einer nicht aus Φ ableitbaren Sequenz $\Gamma \Rightarrow \Delta$. Wir haben daraus eine unendliche Folge von Sequenzen $\Gamma_n \Rightarrow \Delta_n$ konstruiert, und daraus eine Hintikka-Menge $T := \bigcup_{n\in\mathbb{N}} \Gamma_n \cup \bigcup_{n\in\mathbb{N}} \neg\Delta_n$ erhalten, welche $\Phi \cup \Gamma \cup \neg\Delta$ enthält. Wir haben schliesslich gezeigt, dass das kanonische Modell der Atome einer Hintikka-Menge ein Modell der gesamten Hinikka-Menge ist. Insbesondere folgt also, dass $\Phi\cup\Gamma\cup\neg\Delta$ erfüllbar ist. Damit ist der Vollständigkeitssatz bewiesen.

> **Überabzählbare Signaturen.** Wir haben hier den Vollständigkeitssatz nur für abzählbare Signaturen bewiesen. Er gilt aber auch für beliebige Signaturen (siehe etwa: H.-D Ebbinghaus, J. Flum, W. Thomas *Einführung in die Mathematsche Logik*, 4. Auflage, Spektrum Akademischer Verlag (1996), Kapitel V).

Die Menge aller Terme über einer abzählbaren Signatur ist selbst abzählbar. Das im Beweis des Vollständigkeitssatzes konstruierte Modell einer konsistenten Satzmenge ist also abzählbar. Damit erhalten wir unmittelbar eine interessante, rein semantische Folgerung.

Satz 6.12 (Löwenheim, Skolem). *Jede erfüllbare, abzählbare Satzmenge hat ein abzählbares Modell.*

Der Vollständigkeitssatz hat auch eine interessante *algorithmische* Konsequenz. Wie jeder Beweiskalkül erlaubt auch der Sequenzenkalkül die systematische Generierung aller ableitbaren Objekte. Aus dem Vollständigkeitssatz folgt demnach, dass es einen Algorithmus gibt, der alle allgemeingültigen FO(τ)-Sätze aufzählt. Dies bedeutet allerdings nicht, dass man einen Algorithmus zur Vefügung hätte, mit dem man zu jedem vorgelegten FO(τ)-Satz entscheiden könnte, ob dieser allgemeingültig ist: Sei etwa ψ der gegebene Satz. Man kann nun systematisch alle allgemeingültigen Sätze $\varphi_0, \varphi_1, \ldots$ aufzählen. Wenn ψ tatsächlich allgemeingültig ist, wird man irgendwann ein $\varphi_j := \psi$ erhalten und hat damit die richtige Antwort. Wenn aber ψ nicht allgemeingültig ist, dann kann man dies durch ein solches Aufzählungsverfahren nicht feststellen.

Wir werden im nächsten Kapitel die Begriffe der *rekursiv aufzählbaren* und der *entscheidbaren* Mengen genauer studieren und schliesslich zeigen, dass es *keinen* Algorithmus geben kann, welcher die Menge der allgemeingültigen Sätze der Prädikatenlogik entscheidet.

Schnitt-Elimination. Sequenzenkalküle gibt es in vielen verschiedenen Varianten. Interessant ist insbesondere die Erweiterung um die sogenannte *Schnittregel:*

$$\frac{\Gamma, \varphi \Rightarrow \Delta \quad \Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta}$$

Diese Regel ist eine Variante des *Modus Ponens*, welcher in andern Beweiskalkülen verwendet wird und die Ableitung von φ erlaubt, wenn vorher ψ und $\psi \to \varphi$ bewiesen wurden. Die Schnittregel erlaubt es, aus längeren Sequenzen kürzere abzuleiten. Beweise mit Schnittregel können sehr viel kürzer sein als solche ohne Schnitte, aber eine systematische Beweissuche und -analyse ist kaum mehr möglich. Gentzen formulierte seinen Sequenzenkalkül ursprünglich mit Schnittregel und bewies dann seinen berühmten *Schnitt-Elimationsssatz*, welcher besagt, dass beliebige Beweise durch solche ohne Schnitte simuliert werden können. Da wir hier direkt die Vollständigkeit des Sequenzenkalküls ohne Schnittregel bewiesen haben, kann man sich diesen (sehr aufwendigen) Beweis sparen.

6.4 Der Kompaktheitssatz

Der Vollständigkeitssatz schafft eine Brücke zwischen Syntax und Sematik der Prädikatenlogik und erlaubt es, Eigenschaften der Ableitungsbeziehung und der Konsistenz (also syntaktischer Begriffe) auf die Folgerungsbeziehung und die Erfüllbarkeit (also semantische Begriffe) zu übertragen. Die wichtigste Folgerung aus dem Vollständigkeitssatz ist der Kompaktheits- oder Endlichkeitssatz.

Satz 6.13 (Kompaktheitssatz der Prädikatenlogik). *Für jede Menge $\Phi \subseteq \mathrm{FO}(\tau)$ und jedes $\psi \in \mathrm{FO}(\tau)$*

(i) $\Phi \models \psi$ *genau dann, wenn eine endliche Teilmenge* $\Phi_0 \subseteq \Phi$ *existiert, so dass* $\Phi_0 \models \psi$.

(ii) Φ *ist erfüllbar genau dann, wenn jede endliche Teilmemge von* Φ *erfüllbar ist.*

Beweis. Aus der Definition der Ableitungsbeziehung folgen die entsprechenden syntaktischen Aussagen unmittelbar:

(i) $\Phi \vdash \psi$ genau dann, wenn $\Phi_0 \vdash \psi$ für eine endliche Teilmenge $\Phi_0 \subseteq \Phi$.

(ii) Φ ist konsistent genau dann, wenn jede endliche Teilmemge von Φ konsistent ist.

Da nach dem Vollständigkeitssatz eine Formelmenge erfüllbar ist genau dann, wenn sie konsistent ist, und die Folgerungsbeziehung $\models$ mit der Ableitungsbeziehung $\vdash$ zusammenfällt, ergeben sich die semantischen Aussagen des Kompaktheitssatzes. $\square$

Anwendungen des Kompaktheitssatzes. In Kapitel 5.1 haben wir gesehen, dass die Klasse aller Körper mit Charakteristik p endlich axiomatisierbar ist durch den Satz $\psi_{\text{Körper}} \wedge \chi_p$, wobei $\psi_{\text{Körper}}$ die Konjunktion der Körperaxiome und χ_p der Satz $\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$ ist.

Für Körper der Charakteristik 0 haben wir das unendliche Axiomensystem

$$\Phi_0 = \{\psi_{\text{Körper}}\} \cup \{\neg\chi_p : p \text{ Primzahl}\}$$

angegeben. Aus dem Kompaktheitssatz können wir nun folgern, dass *jedes* Axiomensystem für diese Klasse unendlich sein muss.

Satz 6.14. *Die Klasse der Körper der Charakteristik 0 ist nicht endlich axiomatisierbar.*

Beweis. Sei $\psi \in \text{FO}(\tau_{ar})$ ein beliebiger Satz, welcher in allen Körpern der Charakteristik 0 gilt; also $\Phi_0 \models \psi$. Aus dem Kompaktheitssatz folgt, dass es eine Primzahl q gibt, so dass bereits

$$\{\psi_{\text{Körper}}\} \cup \{\neg\chi_p : p < q, p \text{ Primzahl}\} \models \psi.$$

Also gilt ψ auch in allen Körpern mit hinreichend grosser Charakteristik und axiomatisiert also nicht die Körper der Charakteristik 0. $\square$

Satz 6.15. *Sei $\Phi \subseteq \text{FO}(\tau)$ eine Satzmenge mit beliebig grossen endliche Modellen (d.h. für jedes $n \in \mathbb{N}$ gibt es ein Modell $\mathfrak{A} \models \Phi$ mit endlichem $\mathfrak{A}$ und $|\mathfrak{A}| > n$). Dann hat Φ auch ein unendliches Modell.*

Beweis. Sei $\Theta := \Phi \cup \{\varphi_{\geqslant n} : n \in \mathbb{N}\}$ wobei $\varphi_{\geqslant n} := \exists x_1 \cdots \exists x_n \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j$. Die Modelle von Θ sind also gerade die unendlichen Modelle von Φ.

Es genügt zu zeigen, dass jede endliche Teilmenge $\Theta_0 \subseteq \Theta$ erfüllbar ist, denn mit dem Kompaktheitssatz folgt dann, dass auch Θ erfüllbar ist. Für jedes endliche Θ_0 gibt es aber ein $n_0 \in \mathbb{N}$, so dass $\Theta_0 \subseteq \Phi \cup \{\varphi_{\geqslant n} : n \leq n_0\}$. Da nach Voraussetzung Φ beliebig grosse endliche Modelle hat, ist Θ_0 erfüllbar. $\square$

Korollar 6.16. *Die Klasse aller endlichen τ-Strukturen ist nicht axiomatisierbar in* FO.

Ebenso folgt, dass die Klasse aller endlichen Gruppen, die Klasse aller endlichen Körper, die Klassen aller endlichen Graphen etc. nicht FO-axiomatisierbar sind.

Definition 6.17. Seien A, B zwei Mengen. Wir sagen, A ist mindestens so mächtig wie B (kurz $|A| \geq |B|$), wenn eine injektive Funktion $f : B \hookrightarrow A$ existiert.

Satz 6.18 (Aufsteigender Satz von Löwenheim-Skolem). *Φ besitze ein unendliches Modell. Dann gibt es zu jeder Menge M ein Modell $\mathfrak{D} \models \Phi$ über einem Universum D welches mindestens so mächtig wie M ist.*

Beweis. Sei $\Phi \subseteq \mathrm{FO}(\tau)$ und sei $\{c_m : m \in M\}$ eine Menge von paarweise verschiedenen Konstantensymbolen, welche nicht zu τ gehören. Setze

$$\Theta := \Phi \cup \{c_m \neq c_n : m, n \in M, m \neq n\}.$$

Wir zeigen, dass Θ erfüllbar ist. Wegen des Kompaktheitssatzes genügt es zu zeigen, dass für jede endliche Teilmengen $M_0 \subseteq M$ die Formelmenge

$$\Theta_0 := \Phi \cup \{c_m \neq c_n : m, n \in M_0, m \neq n\}$$

erfüllbar ist.

Nach Voraussetzung gibt es ein Modell $\mathfrak{B} \models \Phi$ mit unendlichem $\mathfrak{B}$. Da M_0 endlich ist, können wir in B paarweise verschiedene Elemente b_m für alle $m \in M_0$ auswählen. Sei $\mathfrak{A}$ die Expansion von $\mathfrak{B}$ durch die Konstanten $c_m^{\mathfrak{A}} := b_m$ für $m \in M_0$. Offensichtlich gilt $\mathfrak{A} \models \Theta_0$.

Damit ist gezeigt, dass Θ erfüllbar ist. Sei $\mathfrak{D}$ ein Modell von Θ mit Universum D. Die Abbildung $f : M \to D$ mit $f(m) = c_m^{\mathfrak{D}}$ ist injektiv, da für $m \neq n$ aus M gilt: $\mathfrak{D} \models c_m \neq c_n$. Da $\mathfrak{D} \models \Theta$ gilt insbesondere auch $\mathfrak{D} \models \Phi$. □

Wir erinnern daran, dass die *Theorie* $\mathrm{Th}(\mathfrak{A})$ einer τ-Struktur $\mathfrak{A}$ aus allen Sätzen $\psi \in \mathrm{FO}(\tau)$ mit $\mathfrak{A} \models \psi$ besteht, und dass zwei Strukturen $\mathfrak{A}, \mathfrak{B}$ elementar äquivalent sind (kurz $\mathfrak{A} \equiv \mathfrak{B}$), wenn sie dieselbe Theorie haben.

Lemma 6.19. *$\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\}$ ist die kleinste axiomatisierbare Modellklasse, die $\mathfrak{A}$ enthält.*

Beweis. Offensichtlich ist $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\} = \mathrm{Mod}(\mathrm{Th}(\mathfrak{A}))$ und also axiomatisierbar. Wenn $\mathfrak{A} \models \Phi$ und $\mathfrak{B} \equiv \mathfrak{A}$, dann gilt offensichtlich auch $\mathfrak{B} \models \Phi$. Also gilt für alle $\Phi \subseteq \mathrm{FO}(\tau)$: Wenn $\mathfrak{A} \in \mathrm{Mod}(\Phi)$, dann ist $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\} \subseteq \mathrm{Mod}(\Phi)$. □

Nach dem Isomorphielemma sind isomorphe Strukturen auch elementar äquivalent. Die Umkehrung gilt für unendliche Strukturen im Allgemeinen nicht.

Satz 6.20. *Sei $\mathfrak{A}$ eine unendliche Struktur. Dann gibt es eine Struktur $\mathfrak{B}$ mit $\mathfrak{A} \equiv \mathfrak{B}$, aber $\mathfrak{A} \not\cong \mathfrak{B}$. Insbesondere ist die Isomorphieklasse $\{\mathfrak{B} : \mathfrak{A} \cong \mathfrak{B}\}$ von $\mathfrak{A}$ nicht axiomatisierbar in der Prädikatenlogik.*

Beweis. $\mathrm{Th}(\mathfrak{A})$ besitzt ein unendliches Modell, und deshalb nach dem aufsteigenden Satz von Löwenheim-Skolem auch ein Modell $\mathfrak{B}$, das mindestens die Mächtigkeit der Potenzmenge $\mathcal{P}(A)$ von A hat. Nach Satz 2.2 ist $\mathfrak{B}$ nicht gleichmächtig zu $\mathfrak{A}$ und deshalb insbesondere auch nicht isomorph zu $\mathfrak{A}$. Da $\mathfrak{B} \models \mathrm{Th}(\mathfrak{A})$ (und $\mathrm{Th}(\mathfrak{A})$ vollständig ist) ist aber $\mathfrak{B}$ elementar äquivalent zu $\mathfrak{A}$. Also liegt in jeder axiomatisierbaren Modellklasse, welche $\mathfrak{A}$ enthält, auch eine zu $\mathfrak{A}$ nicht-isomorphe Struktur. □

Nichtstandardmodelle der Arithmetik. Die *Arithmetik* ist die Theorie $\mathrm{Th}(\mathfrak{N})$ der Struktur $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$. Ein *Nichtstandardmodell* der Arithmetik ist eine zu $\mathfrak{N}$ elementar äquivalente, aber nicht zu $\mathfrak{N}$ isomorphe τ_{ar}-Struktur.

Aus dem aufsteigenden Satz von Löwenheim-Skolem folgt: Es gibt ein (überabzählbares) Nichtstandardmodell der Arithmetik. Ein schärferes Resultat liefert der folgende Satz von Skolem.

Satz 6.21 (Skolem). *Es gibt ein abzählbares Nichtstandardmodell der Arithmetik.*

Beweis. Sei $\Phi := \mathrm{Th}(\mathfrak{N}) \cup \{c \neq \boldsymbol{n} : n \in \mathbb{N}\}$, wobei c ein neues Konstantensymbol ist, $\boldsymbol{0} := 0$, und $\boldsymbol{n} := \underbrace{1 + \cdots + 1}_{n \text{ mal}}$ für $n \geq 1$.

Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ besitzt ein Modell $\mathfrak{A} = (\mathfrak{N}, c^{\mathfrak{A}})$ mit hinreichend grossem $c^{\mathfrak{A}} \in \mathbb{N}$. Also ist nach dem Kompaktheitssatz Φ erfüllbar und hat daher nach dem Satz von Löwenheim-Skolem sogar ein abzählbares Modell $\mathfrak{B}$. Sei $\mathfrak{C} = \mathfrak{B} \restriction \tau_{ar}$ (das durch Weglassen von $c^{\mathfrak{B}}$ definierte Redukt von $\mathfrak{B}$). Da $\mathfrak{B} \models \mathrm{Th}(\mathfrak{N})$ ist $\mathfrak{N} \equiv (\mathfrak{B} \restriction \tau_{ar})$.

Es bleibt zu zeigen, dass es keinen Isomorphismus $\pi : \mathfrak{N} \to (\mathfrak{B} \restriction \tau_{ar})$ geben kann. Für jeden solchen Isomorphimus π müsste gelten, dass $\pi(n) = \pi(\boldsymbol{n}^{\mathfrak{N}}) = \boldsymbol{n}^{\mathfrak{B}}$ für alle $n \in \mathbb{N}$. Da π surjektiv ist, gibt es ein $k \in \mathbb{N}$, so dass $c^{\mathfrak{B}} = \pi(k) = \boldsymbol{k}^{\mathfrak{B}}$.

Damit erhalten wir einen Widerspruch: Einerseits gilt $\mathfrak{B} \models c = \boldsymbol{k}$, aber andererseits, da die Formel $c \neq \boldsymbol{k}$ in Φ enthalten ist, auch $\mathfrak{B} \models c \neq \boldsymbol{k}$. □

Übung 6.2. Sei $\mathfrak{A}$ ein abzählbares Nichtstandardmodell der Arithmetik, sei $\varphi(x, y)$ die Formel $x \neq y \wedge \exists z(x + z = y)$ und sei $(\mathfrak{A}, <^{\mathfrak{A}}) := (\mathfrak{A}, \varphi^{\mathfrak{A}})$.

(a) Zeigen Sie, dass $(\mathfrak{A}, <^{\mathfrak{A}})$ ein Modell von $\mathrm{Th}(\mathfrak{N}, <)$ ist (also ein abzählbares Nichtstandardmodell der geordneten Arithmetik).

(b) Zeigen sie, dass $(A, <^{\mathfrak{A}})$ keine Wohlordnung ist (also eine unendliche absteigende Kette enthält).

(c) Beschreiben Sie die Ordnungsstruktur von $(A, <^{\mathfrak{A}})$: Betrachten Sie die Ordnung $(B, <^B)$ mit $B = \mathbb{N} \times \{0\} \cup \mathbb{Z} \times \mathbb{Q}^{>0}$ und $(a, b) <^B (a', b')$, wenn $b < b'$ oder wenn $b = b'$ und $a < a'$; also informell: $(B, <^B)$ ist zusammengesetzt aus $(\mathbb{N}, <)$ und dahinter abzählbar vielen, dicht hintereinanderliegenden Kopien von $(\mathbb{Z}, <)$. Zeigen Sie, dass es eine Einbettung von $(B, <^B)$ in $(A, <^{\mathfrak{A}})$ gibt.

Übung 6.3. Zeigen Sie, dass es überabzählbar viele abzählbare Modelle der Arithmetik gibt. Hinweis: Sei $\varphi(x, y) := \exists z(x \cdot z = y)$. Die Primteiler eines Elements a eines Nichstandardmodells $\mathfrak{A}$ der Arithmetik seien die Primzahlen $p \in \mathbb{N}$, so dass $\mathfrak{A} \models \varphi[\boldsymbol{p}, a]$. Zeigen Sie, dass es zu jeder Menge Q von Primzahlen ein abzählbares Nichtstandardmodell $\mathfrak{A}$ der Arithmetik gibt, welches ein Element a enthält, dessen Primteiler genau die Elemente von Q sind.

***Warum der Kompakheitssatz so heisst.** Sei τ eine beliebige Signatur und S die Menge aller vollständigen τ-Theorien. Wir definieren eine Topologie auf S, deren Basis aus den Mengen $\mathcal{O}_\psi := \{T \in S : \psi \in S\}$ für alle Sätze $\psi \in FO(\tau)$ besteht. Man beachte, dass $\mathcal{O}_\psi \cap \mathcal{O}_\varphi = \mathcal{O}_{\psi \wedge \varphi}$. Ferner ist $S - \mathcal{O}_\psi = \{T \in S : \psi \notin T\} = \{T \in S : \neg\psi \in S\} = \mathcal{O}_{\neg\psi}$.

Die Basis der Topologie besteht also aus offen-abgeschlossenen Mengen. Zudem ist S hausdorffsch, d.h. je zwei verschiedene Punkte lassen sich durch disjunkte Umgebungen trennen. Zu zwei beliebigen vollständigen Theorien $T \neq T'$ gibt es nämlich einen Satz ψ mit $\psi \in T, \neg\psi \in T'$ und daher $T \in \mathcal{O}_\psi, T' \in \mathcal{O}_{\neg\psi}$ und natürlich $\mathcal{O}_\psi \cap \mathcal{O}_{\neg\psi} = \varnothing$.

Die offenen Mengen von S sind die Mengen der Form $\bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi$, die abgeschlossenen diejenigen der Form $\bigcap_{\varphi \in \Phi} \mathcal{O}_\varphi$, für beliebige Satzmengen $\Phi \subseteq \mathrm{FO}(\tau)$.

Der Kompaktheitssatz besagt nun, dass der topologische Raum S kompakt ist, d.h. dass jede offene Überdeckung von S eine endliche Teilüberdeckung besitzt. Dies zeigt man wie folgt:

Jede offene Überdeckung von S kann zu einer Überdeckung der Form $\bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi$ verfeinert werden, für eine geeignete Satzmenge $\Phi \subseteq \mathrm{FO}(\tau)$.

Also ist $\varnothing = S - \bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi = \bigcap_{\varphi \in \Phi_0} \mathcal{O}_{\neg\varphi}$.

Daher lässt sich die Satzmenge $\{\neg\varphi : \varphi \in \Phi\}$ nicht zu einer vollständigen Theorie erweitern und ist also unerfüllbar. Nach dem Kompaktheitssatz ist bereits $\{\neg\varphi : \varphi \in \Phi_0\}$ für ein endliches $\Phi_0 \in \Phi$ unerfüllbar. Folglich ist $S = S - \bigcap_{\varphi \in \Phi_0} \mathcal{O}_{\neg\varphi} = \bigcup_{\varphi \in \Phi_0} \mathcal{O}_\varphi$.

6.5 Die Unentscheidbarkeit der Prädikatenlogik

Das klassische Entscheidungsproblems der mathematischen Logik kann auf verschiedene, äquivalente Weisen formuliert werden:

Erfüllbarkeit: Man konstruiere einen Algorithmus, welcher zu jeder vorgelegten Formel der Prädikatenlogik entscheidet, ob sie erfüllbar ist oder nicht.

Gültigkeit: Man finde einen Algorithmus, welcher zu jeder Formel ψ der Prädikatenlogik entscheidet, ob sie allgemeingültig ist, d.h. ob jede zu ψ passende Interpretation ein Modell von ψ ist.

Beweisbarkeit: Man konstruiere einen Algorithmus, welcher zu jeder Formel $\psi \in \mathrm{FO}$ entscheidet, ob ψ (aus der leeren Hypothesenmenge) ableitbar ist. (Hier wird ein fester, vollständiger Beweiskalkül für die Prädikatenlogik zugrunde gelegt, z.B. der Sequenzenkalkül).

Die Äquivalenz dieser Probleme ist unmittelbar einsichtig: Eine Formel ψ ist erfüllbar genau dann, wenn $\neg\psi$ nicht allgemeingültig ist, und nach dem Vollständigkeitssatz ist eine Formel allgemeingültig genau dann, wenn sie ableitbar ist.

Das klassische Entscheidungsproblem wurde zu Beginn dieses Jahrhundert von Hilbert formuliert und war Teil seines formalistischen Programms zur Lösung der Grundlagenprobleme der Mathematik. Hilbert und Ackermann schrieben:

> *Das Entscheidungsproblem ist gelöst, wenn man ein Verfahren kennt, das bei einem vorgelegten logischen Ausdruck durch endlich viele Operationen die Entscheidung über die Allgemeingültigkeit bzw. Erfüllbarkeit erlaubt. (...) Das Entscheidungsproblem muss als das Hauptproblem der mathematischen Logik bezeichnet werden.*
>
> D. Hilbert, W. Ackermann, *Grundzüge der theoretischen Logik*, 1. Auflage, Berlin 1928, S. 73ff.

In der Tat hätte eine positive Lösung des Entscheidungsproblems weitreichende Folgen für die Mathematik. Man könnte dann, mindestens im Prinzip, zahlreiche offene Probleme der Mathematik (z.B. die Riemann-Hypothese) durch Anwendung des Entscheidungsalgorithmus lösen.

Für gewisse *Teilklassen* der Prädikatenlogik können solche Entscheidungsalgorithmen angegeben werden.

Übung 6.4. Man konstruiere einen Algorithmus, welcher das Erfüllbarkeitsproblem für Formeln löst, deren Signatur ausschliesslich aus monadischen (d.h. einstelligen) Relationssymbolen besteht. Hinweis: Man zeige, z.B. mit Hilfe des Ehrenfeucht-Fraïssé Spiels, dass jede erfüllbare Formel mit Quantorenrang m und q monadischen Relationssymbolen ein Modell mit höchstens $m2^q$ Elementen besitzt.

Übung 6.5. Zeigen sie, dass das Erfüllbarkeitsproblem entscheidbar ist für Formeln der Gestalt $\exists x_1 \cdots \exists x_r \forall y_1 \cdots \forall y_s \varphi$, wobei φ quantorenfrei und relational sein soll. Hinweis: Zeigen Sie, dass jeder erfüllbare Satz dieser Gestalt ein Modell mit höchstens r Elementen besitzt.

Übung 6.6. Zeigen Sie, das das Erfüllbarkeitsproblem für existentielle Formeln (mit beliebiger Signatur) entscheidbar ist.

Übung 6.7. Beurteilen Sie die Komplexität dieser Entscheidungsalgorithmen.

1936/37 haben Church und Turing unabhängig voneinander bewiesen, dass das Entscheidungsproblem nicht algorithmisch lösbar ist. Im Gegensatz zur Aussagenlogik und der Modallogik ist das also Erfüllbarkeitsproblem für die Prädikatenlogik unentscheidbar.

Aus Zeitgründen können wir diese Thematik hier nicht ausführlich behandeln. Ich weise in diesem Zusammenhang auf die im Sommersemester 2001 gehaltenen Vorlesung *Entscheidbarkeit und Komplexität von Logik-Problemen* hin.

Wir beweisen die Unentscheidbarkeit der Prädikatenlogik, indem wir ein bekanntes unentscheidbares Problem, das *Postsche Korrespondenzproblem*, auf das Gültigkeitsproblem für FO reduzieren.

Das Postsche Korrespondenzproblem (PCP).

Gegeben: Eine Folge $F = (u_1, v_1), \dots, (u_k, v_k)$ von Wortpaaren mit $u_i, v_i \in \{0,1\}^*$.

Frage: Gibt es eine Indexfolge $i_1, \dots, i_\ell$ so dass $u_{i_1} \cdots u_{i_\ell} = v_{i_1} \cdots v_{i_\ell}$. (Eine solche Indexfolge nennen wir eine Lösung für F.)

Es ist bekannt (und wird z.B. in der Vorlesung *"Berechenbarkeit und Komplexität"* bewiesen), dass es keinen Algorithmus gibt, der das PCP löst.

Satz 6.22 (Post). *Das PCP ist unentscheidbar.*

Wir zeigen, dass man Eingaben für das PCP durch einen Reduktionsalgorithmus in FO-Formeln transformieren kann, so dass die gegebene PCP-Eingabe eine Lösung zulässt genau dann, wenn die resultierende FO-Formel allgemeingültig ist. Daraus folgt, dass kein Algorithmus die Gültigkeit von FO-Formeln entscheiden kann. Gäbe es nämlich einen solchen Entscheidungsalgorithmus, dann könnte man das PCP-Problem lösen, indem man PCP-Eingaben mit dem Reduktionsalgorithmus auf FO-Formeln transformiert und dann mit dem Entscheidungsalgorithmus bestimmt, ob die erhaltene Formel allgemeingültig ist.

Satz 6.23 (Church, Turing). *Das Gültigkeitsproblem (und damit auch das Erfüllbarkeitsproblem) der Prädikatenlogik ist unentscheidbar.*

Beweis. Wir zeigen, dass man zu jeder Eingabe $F = (u_1, v_1), \dots, (u_k, v_k)$ für das PCP effektiv einen FO-Satz ψ_F konstruieren kann, so dass gilt:

$$\psi_F \text{ ist gültig} \iff \text{es gibt eine Lösung für } F.$$

Die Signatur von ψ_F besteht aus einem Konstantensymbol c, einstelligen Funktionssymbolen f_0 und f_1, und einem zweistelligen Relationssymbol P. Die Idee ist, dass man jedes Wort $w = w_0 w_1 \cdots w_{m-1} \in \{0,1\}^*$ durch den Term $t_w(x) := f_{w_0} f_{w_1} \cdots f_{w_{m-1}} x$ repräsentiert und die Lösbarkeitsbedingung für F durch die Formel

$$\begin{aligned}
\psi_F &:= (\varphi \wedge \vartheta) \to \exists x Pxx, \quad \text{mit} \\
\varphi &:= \bigwedge_{i=1}^{k} P(t_{u_i} c, t_{v_i} c) \\
\vartheta &:= \forall x \forall y \Big(Pxy \to \bigwedge_{i=1}^{k} P(t_{u_i} x, t_{v_i} y)\Big)
\end{aligned}$$

ausdrückt.

Nehmen wir zunächt an, ψ_F sei gültig. Dann gilt ψ_F in jeder zu ihr passenden Struktur, insbesondere also in $\mathfrak{A} = (A, c, f_0, f_1, P)$ mit

$$
\begin{aligned}
A :=& \{0,1\}^* \\
c :=& \lambda \quad \text{(das leere Wort)} \\
f_0(w) :=& 0w \\
f_1(w) :=& 1w \\
P :=& \{(u,v) : \text{ es gibt } i_1, \dots, i_\ell \text{ mit } u = u_{i_1} \cdots u_{i_\ell} \text{ und } v = v_{i_1} \cdots v_{i_\ell}\}
\end{aligned}
$$

Ein Wortpaar (u, v) ist also genau dann in P, wenn u mit derselben Indexfolge aus den u_i aufgebaut werden kann wie v aus den v_i. Man beachte dass für jedes $w \in \{0,1\}^*$ der Wert des Grundterms $t_w c$ in $\mathfrak{A}$ gerade das Wort w selbst ist, d.h. $[\![t_w c]\!]^{\mathfrak{A}} = w$. Also gilt $\mathfrak{A} \models \varphi$. Weiter gilt $[\![t_u t_w c]\!]^{\mathfrak{A}} = uw$ für alle $u, w \in \{0,1\}^*$. Daher folgt $\mathfrak{A} \models \vartheta$. Da $\mathfrak{A} \models \psi_F$ muss auch $\mathfrak{A} \models \exists x Pxx$ gelten. Also gibt es ein Wort z und eine Indexfolge $i_1, \dots, i\ell$ mit $z = u_{i_1} \cdots u_{i_\ell} = v_{i_1} \cdots v_{i_\ell}$, d.h. $i_1, \dots, i_\ell$ ist eine Lösung für F.

Wir nehmen nun umgekehrt an, dass F eine Lösung $i_1, \dots, i_\ell$ besitzt. Zu zeigen ist, dass $\mathfrak{A} \models \psi_F$ für jede zu ψ_F passende Struktur $\mathfrak{A} = (A, c, f_0, f_1, P)$. Wir nehmen also an, dass $\mathfrak{A} \models \varphi \wedge \vartheta$ (anderenfalls gilt $\mathfrak{A} \models \psi_F$ ohnehin) und betrachten die Abbildung $h : \{0,1\}^* \to A$ welche jedem Wort $w \in \{0,1\}^*$ den Wert $h(w) := [\![t_w c]\!]^{\mathfrak{A}}$ zuordnet. Insbesondere gilt $h(\lambda) = c$, $h(0w) = f_0(h(w))$ und $h(1w) = f_1(h(w))$. Da $\mathfrak{A} \models \varphi$ ist $(h(u_i), h(v_i)) \in P$ für $i = 1, \dots, k$. Wegen $\mathfrak{A} \models \vartheta$ gilt für $i = 1, \dots, k$, dass aus $(x, y) \in P$ auch $(h(u_i x), h(v_i y)) \in P$ folgt. Per Induktion schliuessen wir, dass $(h(u_{i_1} \cdots u_{i_\ell}), h(v_{i_1} \cdots v_{i_\ell})) \in P$. Das heisst, für die Lösung $w = u_{i_1} \cdots u_{i_\ell} = v_{i_1} \cdots v_{i_\ell}$ folgt $(h(w), h(w)) \in P$. Damit ist gezeigt, dass $\mathfrak{A} \models \exists x Pxx$ und somit $\mathfrak{A} \models \psi_F$. $\square$

Well, so long, mister. Thanks for the ride, the three cigarettes and for not laughing at my theories on life.

John Garfield, in: *The Postman Always Rings Twice*