Mathematische Logik
SS 2017

Prof. Dr. Erich Grädel

Mathematische Grundlagen der Informatik
RWTH Aachen

Inhaltsverzeichnis

0 Notation und Konventionen

In dieser Vorlesung ist 0 ein Element der natürlichen Zahlen.

Um klar zwischen logischen Formeln und metasprachlichen Aussagen und Beweisen über logische Formeln zu unterscheiden, ist es in der Logik nicht üblich, logische Junktoren und Quantoren ($\forall, \exists, \neg, \wedge, \vee, \rightarrow$) außerhalb von Formeln zu benutzen. Das gleiche gilt für das Symbol $\Rightarrow$, das in Kapitel 1 definiert wird und nicht mit dem Junktor $\rightarrow$ zu verwechseln ist. An vielen Stellen bietet es sich an, metasprachliche Aussagen in Prosa zu formulieren.

1 Aussagenlogik

1.1 Syntax und Semantik der Aussagenlogik

In dieser Vorlesung untersuchen wir verschiedene logische Systeme. Eine besonders simple und bekannte Logik ist die Aussagenlogik, die insbesondere in den Grundlagen der Informatik oft genutzt wird oder implizit vorkommt.

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. Viele der Konzepte, die wir hier vorstellen, werden im späteren Verlauf der Vorlesung für ausdrucksstärkere Logiken verallgemeinert. 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 (Zeichenketten) 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 $\tau = \{X_0, X_1, X_2 \ldots\}$ von Aussagenvariablen zugrundegelegt. Für gewisse Anwendungen der Aussagenlogik ist es 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 Aussagenvariablen 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 Verbesserung 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 anderen 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 $\bigvee_{i=1}^{n} \varphi_i$.

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) – (3) festgelegten Formeln keine weiteren Zeichenketten aussagenlogische Formeln sind. Mit anderen 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 φ auch die Zeichenketten $\neg\psi$, $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $(\psi \rightarrow \varphi)$ enthält.

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:

- Alle atomaren Formeln haben die Eigenschaft E.
- 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* $\mathrm{d}(\psi)$ einer Formel $\psi \in \mathrm{AL}$ induktiv wie folgt definieren:

- $\mathrm{d}(\psi) := 0$ für atomare ψ,
- $\mathrm{d}(\neg\psi) := \mathrm{d}(\psi) + 1$,
- $\mathrm{d}((\psi \circ \varphi)) := \max(\mathrm{d}(\psi), \mathrm{d}(\varphi)) + 1$.

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, welches 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 $\to \psi\varphi$.

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 $\psi \to \varphi$ 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 $\Phi \subseteq \mathrm{AL}$ ist $\tau(\Phi) = \bigcup_{\varphi\in\Phi} \tau(\varphi)$.

Definition 1.2. Eine *(aussagenlogische) Interpretation* ist eine Abbildung $\mathfrak{I} : \sigma \to \{0,1\}$ 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:

- $[\![0]\!]^{\mathfrak{I}} := 0$, $[\![1]\!]^{\mathfrak{I}} := 1$.
- $[\![X]\!]^{\mathfrak{I}} := \mathfrak{I}(X)$ für $X \in \sigma$.
- $[\![\neg\psi]\!]^{\mathfrak{I}} := 1 - [\![\psi]\!]^{\mathfrak{I}}$.
- $[\![\psi \wedge \varphi]\!]^{\mathfrak{I}} := \min([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.
- $[\![\psi \vee \varphi]\!]^{\mathfrak{I}} := \max([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.
- $[\![\psi \to \varphi]\!]^{\mathfrak{I}} := [\![\neg\psi \vee \varphi]\!]^{\mathfrak{I}}$.

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.

Ein *Modell* einer Formelmenge $\Phi \subseteq \mathrm{AL}$ ist eine Interpretation $\mathfrak{I}$ mit $\mathfrak{I} \models \psi$ für alle $\psi \in \Phi$, wofür wir auch $\mathfrak{I} \models \Phi$ schreiben.

Bemerkung. Eine Aussagenvariable oder Formel ist also nicht inhärent „wahr“ oder „falsch“, wie es weniger formale Notation oft nahelegt. Wahrheitswerte werden einer Formel erst durch Interpretationen zugeordnet.

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 Aussagenvariablen 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 $\psi, \varphi, \vartheta, \ldots$ immer für aussagenlogische Formeln und große griechische Buchstaben Φ, Γ für Mengen aussagenlogischer Formeln. Wir verwenden die Schreibweise $\psi(X_1, \ldots, X_n)$ um anzudeuten, dass $\tau(\psi)$ eine

Teilmenge von $\{X_1, \ldots, X_n\}$ ist. Sei $\mathfrak{I}(X_1) = w_1, \ldots, \mathfrak{I}(X_n) = w_n$. Dann schreiben wir auch $[\![\psi(w_1, \ldots, w_n)]\!]$ oder $[\![\psi(w)]\!]$ 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:

- $\neg\neg\psi \equiv \psi$ (Elimination der doppelten Negation)
- $\neg(\psi \wedge \varphi) \equiv \neg\psi \vee \neg\varphi$
  $\neg(\psi \vee \varphi) \equiv \neg\psi \wedge \neg\varphi$ (De Morgan'sche Gesetze)
- $\psi \wedge (\varphi \vee \vartheta) \equiv (\psi \wedge \varphi) \vee (\psi \wedge \vartheta)$
  $\psi \vee (\varphi \wedge \vartheta) \equiv (\psi \vee \varphi) \wedge (\psi \vee \vartheta)$ (Distributivgesetze)
- $\psi \to \varphi \equiv \neg\varphi \to \neg\psi$ (Kontraposition)
- $\psi \wedge (\psi \vee \varphi) \equiv \psi \vee (\psi \wedge \varphi) \equiv \psi$ (Absorption)
- $\psi \wedge \psi \equiv \psi$
  $\psi \vee \psi \equiv \psi$ (Idempotenz von $\wedge$ und $\vee$)
- $\psi \wedge \varphi \equiv \varphi \wedge \psi$
  $\psi \vee \varphi \equiv \varphi \vee \psi$ (Kommutativität von $\wedge$ und $\vee$)
- $\psi \wedge (\varphi \wedge \vartheta) \equiv (\psi \wedge \varphi) \wedge \vartheta$
  $\psi \vee (\varphi \vee \vartheta) \equiv (\psi \vee \varphi) \vee \vartheta$ (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 $\varphi_1, \ldots, \varphi_n$ von Formeln nicht auf die Reihenfolge und Multiplizität der Formeln ankommt. Dies rechtfertigt, dass wir Konjunktionen und Disjunktionen über endliche Formelmengen $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ bilden; anstelle von $\bigwedge_{i=1}^n \varphi_i$ verwenden wir auch die Schreibweisen $\bigwedge_{\varphi\in\Phi} \varphi$ 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) $\neg\varphi_1 \vee \neg\varphi_2 \vee \cdots \vee \neg\varphi_n \vee \psi \equiv \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n \to \psi$
$\neg\varphi_1 \vee \neg\varphi_2 \vee \cdots \vee \neg\varphi_n \equiv \varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n \to 0$
(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 $\psi(X_1, \ldots, X_n)$ erfüllbar (oder allgemeingültig) ist: Man prüft für alle Interpretationen $\mathfrak{I} : \{X_1, \ldots, X_n\} \to \{0, 1\}$ mittels des in Übung 1.3 entwickelten Auswertungsalgorithmus nach, ob $\mathfrak{I} \models \psi$. Obwohl für jede einzelne Interpretation $\mathfrak{I}$ dies sehr schnell nachgeprüft 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.

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 Boolesche Funktionen und Normalformen

Im Folgenden stellen wir einen Zusammenhang her zwischen Funktionen und aussagenlogischen Formeln. Neben einer Normalform für Formeln liefert dieser Zusammenhang eine Möglichkeit, die Ausdrucksstärke von aussagenlogischen Formeln zu analysieren.

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 $\psi(X_1, \ldots, X_n) \in \mathrm{AL}$ definiert eine Boolesche Funktion $h_\psi \in B^n$, durch die Vorschrift $h_\psi(w_1, \ldots, w_n) := [\![\psi(w_1, \ldots, w_n)]\!]$. 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 $\psi(X_1, \ldots, X_n)$ 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 $v = v_1, \ldots, v_n$ die Formel $\varphi^v := X_1^{v_1} \wedge \cdots \wedge X_n^{v_n}$. Man beachte, dass für alle $v, w \in \{0,1\}^n$ gilt:

$$[\![\varphi^v(w)]\!] = 1 \text{ gdw. } v = w$$

Die Funktion f wird nun dargestellt durch die Formel

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

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

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

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 von Literalen 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 $\bigwedge_{i=1}^n \bigvee_{j=1}^{m_i} Y_{ij}$.

Beispiel. Die Formel $(X_1 \wedge X_2 \wedge \neg X_3) \vee (X_1 \neg X_2 \wedge X_4)$ ist in DNF, die Formel $(\neg X_1 \vee X_3) \wedge (X_1 \vee \neg X_2)$ ist in KNF.

Die im Beweis von Satz 1.7 konstruierte Formel

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

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 $\vartheta_1, \ldots, \vartheta_n$ 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 $\psi \in \mathrm{AL}$ 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 $\psi(X_1, \ldots, X_n)$ gibt.

Übung 1.8. Geben Sie einen Algorithmus an, welcher unter Verwendung elementarer Umformungsregeln, z.B. der De Morgan'schen 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 müssen 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 man zu jeder Formel ψ in KNF eine erfüllbarkeitsäquivalente Formel in 3-KNF konstruieren kann, und zwar mit einem

Verfahren, dessen Laufzeit durch ein Polynom 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 (bezüglich 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 $\varphi_1, \ldots, \varphi_n \in \mathrm{AL}$ bildet man eine neue Formel $f(\varphi_1, \ldots, \varphi_n)$, deren Semantik auf naheliegende Weise festgelegt ist:

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

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 $f \in B^n$ ($n \geq 1$) 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, denn es gilt:

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

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 $\{\mid\}$ 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 $\{\wedge, \vee, \rightarrow\}$ nicht funktional vollständig, da für jede nur mit diesen Junktoren gebildete Formel $\psi(X_1, \ldots, X_n)$ gilt, dass $\psi[1, \ldots, 1] = 1$. Insbesondere kann mit $\wedge, \vee, \rightarrow$ 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 $\mathrm{sel} \in B^3$ sei definiert durch $\mathrm{sel}(u, v, w) = v$, wenn $u = 0$ und $\mathrm{sel}(u, v, w) = w$, wenn $u = 1$. Zeigen Sie, dass $\{\mathrm{sel}, 0, 1\}$ 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 ein lineares Polynom $f(X_1, \ldots, X_n) = a_0 + a_1X_1 + \cdots + a_nX_n$ 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* $f^\delta \in B^n$ ist definiert durch $f^\delta(x_1, \ldots, x_n) := \neg f(\neg x_1, \ldots, \neg x_n)$.

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

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

$$T_k^n(x_1, \ldots, x_n) = 1 \text{ gdw. } |\{i : x_i = 1\}| \geq k.$$

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

(c) Zeigen Sie, dass die über der Junktorenmenge $\{\neg, T_2^3\}$ 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). Z.B. wird in der Programmiersprache Prolog eine Verallgemeinerung der Horn-Formeln genutzt, um Programme effizient maschinell auswerten zu können. 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) $\neg X_1 \vee \ldots \vee \neg X_k \vee X \;\equiv\; X_1 \wedge \ldots \wedge X_k \rightarrow X$;

(2) $\neg X_1 \vee \ldots \vee \neg X_k \;\equiv\; X_1 \wedge \ldots \wedge X_k \rightarrow 0$.

Implikationen vom Typ (1) mit $k = 0$ werden in der Form $(1 \rightarrow X)$ 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 mit dem folgenden *Markierungsalgorithmus* in polynomieller Zeit auf Erfüllbarkeit getestet werden.

Algorithmus 1.1 Erfüllbarkeitstest für Horn-Formeln

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

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

Beispiel. Sei $\varphi = (X \wedge Y \to Z) \wedge (X \to Z) \wedge (1 \to X) \wedge (Y \to 0)$. Der Markierungsalgorithmus markiert im ersten Schritt $M_1 = \{X\}$. Im zweiten Schritt markiert er zusätzlich Z, also $M_2 = \{X\} \cup \{Z\}$, und gibt dann „erfüllbar“ aus.

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 Aussagenvariablen 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 Aussagenvariablen X, welche im Laufe dieser Prozedur markiert werden (d.h. die zu M hinzugefügt werden). Weiter kann es keine Teilformel C_i der Form $X_1 \wedge \ldots \wedge X_k \to 0$ mit $X_1, \ldots, X_k \in M$ geben, da sonst $[\![\psi]\!]^{\mathfrak{I}} = 0$. Also stellt der Algorithmus korrekt die Erfüllbarkeit von ψ fest.

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

- Für alle Unterformeln $X_1 \wedge \ldots \wedge X_k \to X$ gilt: Wenn $\{X_1, \ldots, X_k\} \subseteq M$, dann ist $X \in M$ (sonst würde die while-Schleife noch nicht verlassen).
- Für alle Unterformeln $X_1 \wedge \ldots \wedge X_k \to 0$ gilt: $\{X_1, \ldots, X_k\} \not\subseteq M$ (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. Q.E.D.

Bemerkung. Das durch den Markierungsalgorithmus gefundene Modell $\mathfrak{I}_M$ von ψ (falls es existiert) ist das *kleinste Modell* von ψ, d.h. 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 auf die Formel $X \vee Y$ zu. Q.E.D.

1.4 Der Kompaktheitssatz der Aussagenlogik

In vielen Anwendungen der Aussagenlogik hat man Erfüllbarkeit und Folgerungsbeziehungen 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 ausdrucksstärkere Logiken und deren Anwendungen. Die Folgerungsbeziehung erlaubt Aussagen darüber, welche Formeln in einem durch eine Formelmenge beschriebenen System gelten. Wenn z.B. ein Roboter Informationen über seine Umgebung als Formeln vorhält,

wird über die Folgerungsbeziehung ausgedrückt, welche nicht explizit angegebenen Formeln in der Umgebung auch gelten.

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, dass ψ *aus* Φ *folgt* (kurz: $\Phi \models \psi$), 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, dass dasselbe Symbol $\models$ sowohl für die Modellbeziehung ($\mathfrak{I} \models \psi$, bzw. $\mathfrak{I} \models \Phi$), als auch für die Folgerungsbeziehung ($\Phi \models \psi$) verwendet wird. Die Bedeutung ist immer eindeutig, da sie durch die linke Seite festgelegt wird.

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

(a) $\{\psi, \varphi\} \models \psi \wedge \varphi$,
$\{\psi, \psi \to \varphi\} \models \varphi$.
(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 $\Phi \models (\psi \to \varphi)$.
(d) ψ ist genau dann eine Tautologie, wenn ψ aus der leeren Menge folgt. (Dies rechtfertigt die Notation $\models \psi$ als abgekürzte Schreibweise für $\emptyset \models \psi$.)
(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 genau dann äquivalent, 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* $\psi \in \mathrm{AL}$.

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.

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 (in A).

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 (Kompaktheitssatz). Wir zeigen zunächst, dass (ii) aus (i) folgt: 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 $\mathfrak{I} : \tau \to \{0,1\}$ 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 $\Phi \models \psi$.

Es bleibt (i) zu zeigen. 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

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

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

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

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

- Für atomare ψ folgt dies unmittelbar aus der Definition.
- Sei $\psi = \neg\varphi$. Dann ist nach Induktionsvoraussetzung und nach der soeben gezeigten Eigenschaft von $\Phi_{\max}$

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

- Sei $\psi = \varphi \wedge \vartheta$. Nach Induktionsvoraussetzung folgt, dass genau dann $\mathfrak{I} \models \psi$ gilt, 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.
- Die Argumentation in allen anderen Fällen ist analog. (Es wird empfohlen, zur Übung mindestens einen dieser Fälle, z.B. für Formeln $(\varphi \to \vartheta)$ selbst nachzuvollziehen.)

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

Das Lemma von König. Ein *Baum mit Wurzel* w ist ein zusammenhängender, zykelfreier, gerichteter Graph $T = (V, E)$ mit einem ausgezeichneten 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 anderen Knoten genau eine Kante endet. Ein solcher Baum heißt *endlich verzweigt*, wenn von jedem $v \in V$ nur endlich viele Kanten ausgehen. Als Anwendung des Kompaktheitssatzes beweisen wir das folgende Lemma.

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:

- $|W \cap S_n| = 1$ für alle n;
- 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:

$$\alpha_n := \bigvee_{v \in S_n} X_v,$$

$$\beta_n := \bigwedge_{u,v \in S_n, u \neq v} \neg(X_u \wedge X_v),$$

$$\Phi := \{\alpha_n : n \in \mathbb{N}\} \cup \{\beta_n : n \in \mathbb{N}\} \cup \{(X_v \to X_u) : (u,v) \in E\}.$$

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:

- Da $\alpha_n, \beta_n \in \Phi$, gibt es genau ein v in $W \cap S_n$.
- 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 $u \in W$. Q.E.D.

Bemerkung. Man beachte, dass das Lemma von König nicht trivial ist. Es gilt z.B. nicht für Bäume mit unendlichen Verzweigungen. Man betrachte etwa den Baum in Abbildung 1.1. In diesem Baum gibt es für jedes n, ausgehend von w, einen Weg der Länge n, aber es gibt keinen unendlichen Weg.

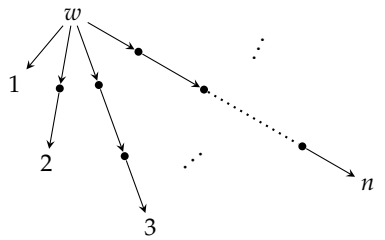


Abbildung 1.1. Ein unendlicher Baum ohne unendlichen Weg

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 $\Phi \subseteq$ AL ist *endlich axiomatisierbar*, wenn eine endliche Formelmenge $\Phi_0 \subseteq$ 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 mit $1 \leq i \leq k$ 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 $\Phi \subseteq$ AL eine Formelmenge, $X \in \tau(\Phi)$ eine Aussagenvariable. X heißt *explizit definierbar* in Φ, wenn eine Formel $\varphi \in$ AL existiert, die 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 Aussagenvariablen $Z \neq X$, dann auch $\mathfrak{I}(X) = \mathfrak{I}'(X)$. (In Modellen von Φ ist also der Wahrheitswert von X durch die Wahrheitswerte der anderen 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

In der Praxis können viele Sachverhalte über die Erfüllbarkeit aussagenlogischer Formeln dargestellt werden. 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 $\square$ 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* $\mathrm{K}(\psi)$ 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 $\mathrm{K}(\psi) := \{C_1, \ldots, C_n\}$.

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.

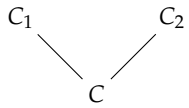
Beispiel. Die Formeln $(X_1 \vee \neg X_2) \wedge X_3$, $(X_1 \vee X_1 \vee \neg X_2) \wedge (X_3 \vee X_3) \wedge X_3$ und $X_3 \wedge (X_1 \vee \neg X_2) \wedge (\neg X_2 \vee X_1)$ haben alle dieselbe Klauselmenge $K = \{\{X_1, \neg X_2\}, \{X_3\}\}$.

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

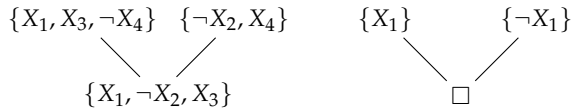
Wir können also Klauseln und Klauselmengen wie Formeln und Formelmengen behandeln und benutzen Begriffe wie Erfüllbarkeit und Äquivalenz entsprechend. Insbesondere ist eine Klauselmenge erfüllbar, wenn es eine Interpretation $\mathfrak{I}$ gibt, so dass jede Klausel $C \in K$ ein Literal Y enthält mit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

- Die leere Klauselmenge ist erfüllbar.
- Wenn $\square \in K$, 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 $C = (C_1 \setminus \{Y\}) \cup (C_2 \setminus \{\overline{Y}\})$. Dies wird folgendermaßen notiert:



Beispiel.



Wir zeigen im Folgenden, dass Resolution auf allen Klauselmengen korrekt die Erfüllbarkeit bzw. Unerfüllbarkeit nachweist.

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 $C = (C_1 \setminus \{Y\}) \cup (C_2 \setminus \{\overline{Y}\})$.

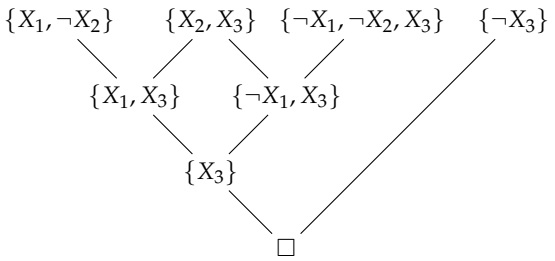
- Wenn $[\![Y]\!]^{\mathfrak{I}} = 1$, dann ist $[\![C_2 \setminus \{\overline{Y}\}]\!]^{\mathfrak{I}} = 1$, da sonst $[\![C_2]\!]^{\mathfrak{I}} = 0$. Also ist $[\![C]\!]^{\mathfrak{I}} = 1$.
- Wenn $[\![Y]\!]^{\mathfrak{I}} = 0$, dann ist $[\![C_1 \setminus \{Y\}]\!]^{\mathfrak{I}} = 1$ und also wiederum $[\![C]\!]^{\mathfrak{I}} = 1$.

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

Definition 1.21. Für jede Klauselmenge K sei

- $\mathrm{Res}(K) := K \cup \{C : C \text{ Resolvente zweier Klauseln aus } K\}$.
- $\mathrm{Res}^0(K) := K$, $\mathrm{Res}^{n+1}(K) := \mathrm{Res}(\mathrm{Res}^n(K))$ für $n \in \mathbb{N}$.
- $\mathrm{Res}^*(K) := \bigcup_{n\in\mathbb{N}} \mathrm{Res}^n(K)$.

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



Korrektheit und Vollständigkeit. Ein Beweiskalkül ist *korrekt*, wenn keine falschen Aussagen darin ableitbar sind, und *vollständig*, wenn alle wahren Aussagen ableitbar sind. Ist der Resolutionskalkül korrekt, gibt er also *nur* für unerfüllbare Klauselmengen „unerfüllbar" aus, ist er vollständig, stellt er die Unerfüllbarkeit für *jede* unerfüllbare Klauselmenge fest. 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 Resolutionskalküls wird durch den Resolutionssatz ausgedrückt.

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

Beweis. (Korrektheit) Aus dem Resolutionslemma folgt $K \equiv \mathrm{Res}(K)$ und damit per Induktion $K \equiv \mathrm{Res}^*(K)$. Wenn also $\square \in \mathrm{Res}^*(K)$, dann ist $\mathrm{Res}^*(K)$ 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 $X_0, \ldots, X_{n-1}$ enthält. Wir zeigen per Induktion nach n, dass $\square \in \mathrm{Res}^*(K_0) \subseteq \mathrm{Res}^*(K)$.

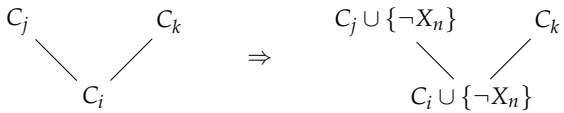
Sei $n = 0$. Es gibt nur zwei Klauselmengen ohne Aussagenvariablen, nämlich $\emptyset$ und $\{\square\}$. Da die leere Klauselmenge erfüllbar ist, muss $K_0 = \{\square\}$ sein. Für den Induktionsschluss nehmen wir an, dass alle Aussagenvariablen von K_0 in $\{X_0, \ldots, X_n\}$ enthalten seien. Wir konstruieren zwei Klauselmengen K_0^+ und K_0^-, in denen X_n nicht vorkommt:

$$K_0^+ := \{C \setminus \{\neg X_n\} : X_n \notin C, C \in K_0\},$$
$$K_0^- := \{C \setminus \{X_n\} : \neg X_n \notin C, C \in K_0\}$$

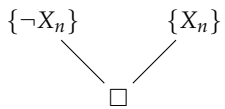
(d.h. wir streichen aus K_0 alle Klauseln, in denen X_n bzw. $\neg X_n$ vorkommt und streichen $\neg X_n$ bzw. X_n aus allen verbleibenden Klauseln).

K_0^+ und K_0^- sind unerfüllbar. Andernfalls gäbe es etwa eine Interpretation $\mathfrak{I} : \{X_0, \ldots, X_{n-1}\} \to \{0, 1\}$, so dass $[\![K_0^+]\!]^{\mathfrak{I}} = 1$. Erweitere $\mathfrak{I}$ durch $\mathfrak{I}(X_n) = 1$. Wir zeigen, dass dann $[\![K_0]\!]^{\mathfrak{I}} = 1$ gilt. Sei $C \in K_0$ eine beliebige Klausel. Diese kann nun X_n enthalten, dann gilt aber stets $[\![C]\!]^{\mathfrak{I}} = 1$, da $\mathfrak{I}(X_n) = 1$. Enthält C nicht X_n so ist $C \setminus \{\neg X_n\}$ in K_0^+. Da $[\![K_0^+]\!]^{\mathfrak{I}} = 1$ gilt, muss also $[\![C \setminus \{\neg X_n\}]\!]^{\mathfrak{I}} = 1$ gelten. Also wird ein Literal in der reduzierten Klausel unter $\mathfrak{I}$ positiv ausgewertet, welches demnach auch in C positiv ausgewertet wird. Es folgt also $[\![C]\!]^{\mathfrak{I}} = 1$ und damit insgesamt $[\![K_0]\!]^{\mathfrak{I}} = 1$ im Widerspruch zur Unerfüllbarkeit von K_0. Die Unerfüllbarkeit von K_0^- lässt sich analog nachweisen, indem eine angenommene erfüllende Interpretation $\mathfrak{I}$ mit $\mathfrak{I}(X_n) = 0$ erweitert wird, welche dann auch K_0 erfüllt.

Aus der Induktionsvoraussetzung folgt, dass $\square \in \mathrm{Res}^*(K_0^+)$ und $\square \in \mathrm{Res}^*(K_0^-)$. Also gibt es Klauseln $C_1, C_2, \ldots, C_m$, so dass $C_m = \square$, und für $i = 1, \ldots, m$ 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 $C_1, \ldots, C_m$ auch in $\mathrm{Res}^*(K_0)$, also $\square \in \mathrm{Res}^*(K_0)$. Wenn ja, erhalten wir durch Wiedereinfügen von $\neg X_n$ eine Folge von Klauseln $C_1', \ldots, C_m'$, welche beweist, dass $\{\neg X_n\} \in \mathrm{Res}^*(K_0)$.



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



folgt, dass $\square \in \text{Res}^*(K_0)$. Q.E.D.

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

$$K = \text{Res}^0(K) \subseteq \text{Res}^1(K) \subseteq \ldots \subseteq \text{Res}^m(K) \subseteq \ldots$$

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

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

Algorithmus 1.2 Erfüllbarkeitstest mit Resolution

Input K (endliche Klauselmenge)
$R := \emptyset, S := K$
while $R \neq S$ **do**
  $R := S$
  $S := \text{Res}(R)$
  if $\square \in S$ **then**
    output „K unerfüllbar“
end do
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 Aussagen durch äquivalente Existenzaussagen auszudrücken: ψ ist unerfüllbar, wenn eine Deduktion der leeren Klausel existiert.

Man beachte aber folgende Asymmetrie: Das Aufschreiben eines 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 = coNP.

Für unendliche Klauselmengen kann es durchaus passieren, dass $\text{Res}(K) \setminus K$ unendlich ist oder dass die Kette

$$K = \text{Res}^0(K) \subset \text{Res}^1(K) \subset \ldots \subset \text{Res}^n(K) \subset \ldots$$

nicht stationär wird (auch wenn K erfüllbar ist).

Beispiel. Sei $K = \{\{X_0\}\} \cup \{\{\neg X_n, X_{n+1}\} : n \in \mathbb{N}\}$. Dann ist $X_{n+1} \in \mathrm{Res}^{n+1}(K) \setminus \mathrm{Res}^n(K)$ für jedes $n \in \mathbb{N}$.

Einheitsresolution für Horn-Formeln. Die einer Horn-Formel ψ zugeordnete Klauselmenge $\mathrm{K}(\psi)$ 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 $\square$ und die Klauseln $\{X\}$, welche aus einer einzigen Aussagenvariablen bestehen, auch Horn-Klauseln sind. Wir präsentieren nun eine eingeschränkte Variante des Resolutionskalküls, welche vollständig für Horn-Formeln ist.

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 genau dann unerfüllbar, wenn $\square$ durch Einheitsresolution aus $\mathrm{K}(\psi)$ ableitbar ist.

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

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

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

Die Korrektheit des Erfüllbarkeitstests (Satz 1.12) ergibt: ψ ist unerfüllbar genau dann, wenn $X_1, \ldots, X_k \in M^*$ existieren, so dass $\{\neg X_1, \ldots, \neg X_k\} \in \mathrm{K}(\psi)$. Wir zeigen: Wenn $X \in M^*$, dann ist $\{X\}$ per Einheitsresolution aus $\mathrm{K}(\psi)$ 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 $X_1, \ldots, X_k \in M^i$, so dass $\{\neg X_1, \ldots, \neg X_k, X\} \in \mathrm{K}(\psi)$. Nach Induktionsvoraussetzung lassen sich die Klauseln $\{X_1\}, \ldots, \{X_k\}$ aus $\mathrm{K}(\psi)$ per Einheitsresolution ableiten. Unter Zuhilfenahme der Klausel $\{\neg X_1, \ldots, \neg X_k, X\}$ lässt sich dann auch $\{X\}$ per Einheitsresolution aus $\mathrm{K}(\psi)$ ableiten.

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

1.6 Der aussagenlogische Sequenzenkalkül

Während der Resolutionskalkül die Erfüllbarkeit von Formeln und Formelmengen überprüft, beschreiben wir nun ein Verfahren, das Zusammenhänge zwischen Formeln, wie z.B. die Folgerungsbeziehung, algorithmisch verifiziert. 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*.

Beispiel.

- Jede Sequenz $\Gamma \Rightarrow \Delta$ mit $\Gamma \cap \Delta \neq \emptyset$ ist gültig. Solche Sequenzen sind die *Axiome* des Sequenzenkalküls.
- Seien Γ, Δ Mengen von Aussagenvariablen. Die Sequenz $\Gamma \Rightarrow \Delta$ ist genau dann falsifizierbar, wenn Γ und Δ disjunkt sind.
- Eine Sequenz der Form $\Gamma \Rightarrow \emptyset$ ist genau dann gültig, wenn Γ unerfüllbar ist.
- Eine Sequenz $\emptyset \Rightarrow \Delta$ ist genau dann gültig, wenn $\bigvee \Delta$ allgemeingültig 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:

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

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

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

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

Hierbei 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:

- Jedes Blatt ist mit einem Axiom beschriftet.

- 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. Die Sequenz $\psi, (\varphi \vee \vartheta) \Rightarrow (\psi \wedge \varphi), (\psi \wedge \vartheta)$ kann wie folgt in SK bewiesen werden:

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

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 aussagenlogische 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 genau dann gültig ist, 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 $\emptyset \Rightarrow \psi$ in SK abgeleitet werden kann.

Der Sequenzenkalkül erlaubt die *systematische Suche und Analyse* von Beweisen. Dies ist ein wichtiger Vorteil gegenüber vielen anderen 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 Formel 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.

Beispiel.

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

$$\frac{(X \to Y) \Rightarrow (\neg Y \to \neg X)}{\emptyset \Rightarrow (X \to Y) \to (\neg Y \to \neg X)}$$

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

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

  Die beiden Blätter werden nun mit den Regeln $(\Rightarrow\to)$ und dann $(\neg\ \Rightarrow)$ und $(\Rightarrow\ \neg)$ weiter bearbeitet. Dies führt schließlich zu

folgendem Ableitungsbaum:

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

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

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

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

- 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

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

  Die Blätter bestehen nur aus Aussagenvariablen, aber nur die äußeren 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 Ausgangs-

sequenz $(X \vee Y) \Rightarrow (X \wedge Y)$. 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 Ableitungsbaums 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 können nun einen Algorithmus angeben, welcher zu jeder aussagenlogischen Sequenz einen Beweis oder eine Widerlegung findet.

Satz 1.32. Algorithmus 1.3 terminiert auf jeder gegebenen Sequenz $\Gamma \Rightarrow \Delta$ in endlich vielen Schritten. Er findet genau dann einen Beweis, 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 Ableitungsbaums 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. Q.E.D.

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.

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

Übung 1.22. 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 1.23. 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.

Algorithmus 1.3. 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 anderen 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.

2 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. Üblicherweise werden in der Mathematik Aussagen über konkrete Strukturen getroffen, z.B. „alle Quadratzahlen sind positiv, $25 = 5 \cdot 5$, also ist 25 positiv“. Bereits dieses kurze Argument widersetzt sich einer Formalisierung in der Aussagenlogik. Abstrakt hat es die Gestalt $\psi \wedge \varphi \to \vartheta$, 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.

2.1 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 2.1. Eine *Signatur* τ ist eine Menge von Funktions- und Relationssymbolen. Jedes dieser Symbole hat eine feste endliche Stelligkeit.

Eine Signatur heißt *relational*, wenn sie nur Relationssymbole enthält bzw. *funktional* oder *algebraisch*, wenn sie ausschließlich Funktionssymbole enthält. Nullstellige Funktionssymbole heißen auch *Konstantensymbole*.

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

Beispiel.

- Die Signatur der Arithmetik ist $\tau_{ar} = \{+, \cdot, 0, 1\}$, wobei $+$ und $\cdot$ zweistellige Funktionsymbole, 0 und 1 Konstantensymbole sind.
- Die Signatur der geordneten Arithmetik ist $\tau_{ar}^{<} = \{+, \cdot, 0, 1, <\}$. Sie erweitert τ_{ar} um das zweistellige Relationssymbol $<$.
- Die Signatur von Graphen ist $\tau_G = \{E\}$, 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 Funktionssymbole über diesem Universum.

Definition 2.2. Eine τ-*Struktur* $\mathfrak{A}$ besteht aus

- einer nichtleeren Menge A, dem *Universum* (oder *Träger*) von $\mathfrak{A}$,
- einer Interpretationsfunktion welche jedem n-stelligen Relationssymbol $P \in \tau$ eine n-stellige Relation $P^{\mathfrak{A}} \subseteq A^n$ und jedem n-stelligen Funktionssymbol $f \in \tau$ eine n-stellige 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.

Bemerkung. 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.

Insbesondere sind die Schreibweisen $(A, P_1, P_2, \ldots, f_1, f_2, \ldots)$ und (A, τ) immer als Abkürzung für $(A, P_1^{\mathfrak{A}}, P_2^{\mathfrak{A}}, \ldots, f_1^{\mathfrak{A}}, f_2^{\mathfrak{A}}, \ldots)$ zu verstehen.

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

Definition 2.3. Seien $\mathfrak{A}$ und $\mathfrak{B}$ τ-Strukturen. $\mathfrak{A}$ ist *Substruktur* von $\mathfrak{B}$ (kurz: $\mathfrak{A} \subseteq \mathfrak{B}$), wenn

- $A \subseteq B$,
- für alle Relationssymbole $R \in \tau$ gilt: $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$ (wobei n die Stelligkeit von R ist),
- für alle Funktionssymbole $f \in \tau$ 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 n-stelligen $f \in \tau$ und alle $a_1, \dots, a_n \in A$ ist $f^{\mathfrak{B}}(a_1, \dots, a_n) \in A$. 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 2.4. Seien $\sigma \subseteq \tau$ Signaturen, und sei $\mathfrak{B}$ eine τ-Struktur. Das *σ-Redukt* $\mathfrak{B} \restriction \sigma$ von $\mathfrak{B}$ ist die σ-Struktur, die wir aus $\mathfrak{B}$ erhalten, wenn wir die Relationen und Funktionen in $\tau \setminus \sigma$ 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 $(\mathbb{R}, +, \cdot, 0, 1)$.

2.2 Ein Zoo von Strukturen

Mengen. Sei $\tau = \emptyset$. Die $\emptyset$-Struktur mit Universum A ist einfach die Menge A.

Graphen. Die Signatur von Graphen ist $\tau_G = \{E\}$, wobei E ein binäres Relationssymbol ist. Eine beliebige τ_G-Struktur ist ein *gerichteter Graph*. 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 $u, v \in V$: Wenn $(u, v) \in E^G$, dann auch $(v, u) \in E^G$.

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 $a < b$, $a = b$ 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 $a_0, a_1, a_2, \dots$ 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.

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 $\{<\} \cup \{P_a : a \in \Gamma\}$ mit einstelligen Relationssymbolen P_a zu. Das Universum von $\mathfrak{B}(w)$ ist die Menge $\{0, \dots, n-1\}$ 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

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

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

In der Logik wird die Menge der natürlichen Zahlen oft mit ω bezeichnet. Ein *unendliches Wort* oder *ω-Wort* ist eine unendliche Folge $z = z_0 z_1 \cdots \in \Gamma^\omega$ von Symbolen aus Γ. Die entsprechende Wortstruktur ist $\mathfrak{B}(z) := (\omega, <, (P_a)_{a\in\Gamma})$ mit $P_a = \{i \in \omega : z_i = a\}$.

Bemerkung (Bemerkung zur Anwendung). In der Automatentheorie wird häufig der Zusammenhang zwischen Logiken und Automatenmodellen untersucht. Dafür ist es notwendig, ein Wort (also die Eingabe für einen Automaten) als Struktur (also als Objekt, über dem Formeln ausgewertet werden können) darzustellen.

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.

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 *Domänen* sind (z.B. Integers, Strings,...). Sei D die Vereinigung aller in der Datenbank vorkommenden Domänen. 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 die *aktive Domäne* $\mathrm{ad}(\mathfrak{D})$, welche aus all denjenigen Objekten besteht, die in einer der Relationen $R_1, \ldots, R_m$ vorkommen, also

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

Da alle Relationen R_i endlich sind, ist auch $\mathrm{ad}(\mathfrak{D})$ endlich und die endliche Substruktur $(\mathrm{ad}(\mathfrak{D}), R_1, \ldots, R_m)$ 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. Ein Teilgebiet der mathematischen Logik befasst sich sogar mit der Datenbanktheorie, was insbesondere Fragestellungen zur Ausdrucksstärke von Logiken umfasst.

Arithmetische Strukturen. Die Signatur der Arithmetik ist $\tau_{\mathrm{ar}} = \{+, \cdot, 0, 1\}$, die Signatur der geordneten Arithmetik $\tau_{\mathrm{ar}}^{<} = \tau_{\mathrm{ar}} \cup \{<\}$, wobei wir annehmen, dass die Symbole $+, \cdot, 0, 1, <$ in der üblichen Wei-

se 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 $a \in \mathbb{N} \cup \{\infty\}$.

Beweise in der Mathematik lassen sich grundlegend auf Ableitungen prädikatenlogischer Formeln über arithmetischen und anderen bekannten mathematischen Strukturen zurückführen. Man kann sogar sagen, dass die Logik dazu dient, eine formale Grundlage für die Mathematik zu beschreiben.

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

Gruppen. Wie können Gruppen (im Sinne der Algebra) durch Strukturen gemäß Definition 2.2 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

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

Die Wahl der Signatur ist abhängig von der jeweiligen Absicht: Will man eine möglichst minimale Formalisierung, wird man (1) oder (2) 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.

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.

2.3 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 $\mathrm{Alph}(\tau)$, welches aus folgenden Symbolen besteht:

- den Relations- und Funktionssymbolen in τ,
- einer festen abzählbar unendlichen Menge $\mathrm{VAR} = \{v_0, v_1, v_2, \ldots\}$ 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 2.5. Die Menge $\mathrm{T}(\tau)$ der *τ-Terme* ist induktiv wie folgt definiert:

- $\mathrm{VAR} \subseteq \mathrm{T}(\tau)$, d.h. jede Variable ist ein τ-Term.
- Sind $t_1, \ldots, t_n$ τ-Terme und f ein n-stelliges Funktionssymbol aus τ, so ist auch $ft_1 \cdots t_n$ ein τ-Term.

Wenn wir einen Term in der Form $t(x_1, \ldots, x_n)$ schreiben, dann meinen wir, dass $x_1, \ldots, x_n$ paarweise verschiedene Variablen sind und dass in t keine anderen Variablen als diese vorkommen.

Man beachte, dass insbesondere jedes Konstantensymbol c aus τ ein τ-Term ist. Ein *Grundterm* ist ein Term in dem keine Variablen auftreten.

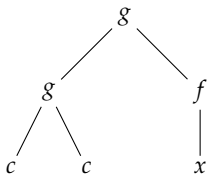
Beispiel. Die Signatur τ enthalte die Funktionssymbole f (einstellig), g (zweistellig) und c (nullstellig). Sei $x \in \mathrm{VAR}$ eine Variable. Dann sind die folgenden Wörter τ-Terme.

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

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 $\mathrm{Alph}(\tau)^*$ 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 $t_1, \ldots, t_n$ eindeutig bestimmt sind.

Definition 2.6. Die Menge $\mathrm{FO}(\tau)$ 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 $t_1, \ldots, t_n$ τ-Terme 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*, *Atom-Formel* oder einfach *Atom*. *Literale* sind Atome und deren Negationen. Formeln, die nur nach den Regeln (1) – (4) definiert sind, heißen *quantorenfrei*.

Wie in der Aussagenlogik ist auch die Syntax der Prädikatenlogik induktiv definiert. Man beachte allerdings, dass die Atome bereits induktiv definiert und damit beliebig komplexe Objekte sind.

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

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

Konventionen zur Notation von Formeln. Wie bei der Aussagenlogik benutzen wir auch bei der Prädikatenlogik abkürzende oder vereinfachende Schreibweisen. Zum Beispiel bezeichnen wir Variablen in der Regel mit anderen Symbolen, etwa $x, y, z, x_0, x_1, \ldots$, anstelle von $v_0, v_1, \ldots \in \mathrm{VAR}$. 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: 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. Allerdings sind Klammern zur eindeutigen Lesbarkeit von Formeln mit Quantoren oft notwendig. So bezeichnet die Schreibweise $\forall x\varphi \vee \psi$ nicht die Formel $\forall x(\varphi \vee \psi)$, sondern könnte (weniger formal) auch als $(\forall x\varphi) \vee \psi$ geschrieben werden. Wie später bei der Definition der Semantik deutlich wird, sind diese Formeln nicht logisch äquivalent.

Man beachte, dass diese anschaulichen Mitteilungsweisen keine Terme und Formeln im eigentlichen Sinn mehr sind sondern metasprachliche Umschreibungen solcher Objekte. Die präzise 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.

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

Man 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 2.7. Sei $t \in \mathrm{T}(\tau)$ 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:

- Für atomare Formeln ψ ist $\mathrm{frei}(\psi) := \mathrm{var}(\psi)$.
- $\mathrm{frei}(\neg\psi) := \mathrm{frei}(\psi)$.
- $\mathrm{frei}(\psi \circ \varphi) := \mathrm{frei}(\psi) \cup \mathrm{frei}(\varphi)$ für $\circ \in \{\wedge, \vee, \to\}$.
- $\mathrm{frei}(\exists x\psi) = \mathrm{frei}(\forall x\psi) := \mathrm{frei}(\psi) \setminus \{x\}$.

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

2.4 Semantik der Prädikatenlogik

Definition 2.8 (Modellbeziehung)**.** Sei τ eine Signatur. Eine τ-*Interpretation* ist ein Paar $\mathfrak{I} = (\mathfrak{A}, \beta)$, wobei $\mathfrak{A}$ eine τ-Struktur und $\beta : X \to A$ eine Belegung von Variablen durch Elemente von A ist. Dabei ist $X = \mathrm{dom}(\beta) \subseteq \mathrm{VAR}$. Eine τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ ordnet

- jedem Term $t \in \mathrm{T}(\tau)$ mit $\mathrm{var}(t) \subseteq \mathrm{dom}(\beta)$ einen Wert $[\![t]\!]^{\mathfrak{I}} \in A$ zu, und
- jeder Formel $\psi \in \mathrm{FO}(\tau)$ mit $\mathrm{frei}(\psi) \subseteq \mathrm{dom}(\beta)$ 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. Für einen Term t ist $[\![t]\!]^{\mathfrak{I}}$ definiert durch:

- Für $x \in \mathrm{dom}(\beta)$ ist $[\![x]\!]^{\mathfrak{I}} := \beta(x)$.
- Für $t = ft_1 \cdots t_n$ ist $[\![t]\!]^{\mathfrak{I}} := f^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{I}}, \ldots, [\![t_n]\!]^{\mathfrak{I}})$.

Für atomare Formeln ψ ist $[\![\psi]\!]^{\mathfrak{I}}$ wie folgt definiert:

- $[\![t_1 = t_2]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{wenn } [\![t_1]\!]^{\mathfrak{I}} = [\![t_2]\!]^{\mathfrak{I}}, \\ 0 & \text{sonst.} \end{cases}$
- $[\![Pt_1 \cdots t_n]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{wenn } ([\![t_1]\!]^{\mathfrak{I}}, \ldots, [\![t_n]\!]^{\mathfrak{I}}) \in P^{\mathfrak{A}}, \\ 0 & \text{sonst.} \end{cases}$

Die Bedeutung der Junktoren $\neg, \wedge, \vee$ und $\to$ ist genau die gleiche wie in der Aussagenlogik:

- $[\![\neg\psi]\!]^{\mathfrak{I}} := 1 - [\![\psi]\!]^{\mathfrak{I}}$.
- $[\![\psi \vee \varphi]\!]^{\mathfrak{I}} := \max([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.
- $[\![\psi \wedge \varphi]\!]^{\mathfrak{I}} := \min([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.
- $[\![\psi \to \varphi]\!]^{\mathfrak{I}} := [\![\neg\psi \vee \varphi]\!]^{\mathfrak{I}} = \max(1 - [\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.

Um $[\![\exists x\psi]\!]^{\mathfrak{I}}$ und $[\![\forall x\psi]\!]^{\mathfrak{I}}$ zu definieren, verwenden wir folgende Notation: Sei $\beta : X \to A$ eine Belegung, x eine Variable und a ein Element von A. Wir definieren eine neue Belegung $\beta[x/a] : X \cup \{x\} \to A$ durch

$$\beta[x/a](y) := \begin{cases} \beta(y) & \text{wenn } y \neq x, \\ a & \text{sonst.} \end{cases}$$

und definieren:

- $[\![\exists x\psi]\!]^{\mathfrak{I}} := \max_{a \in A} [\![\psi]\!]^{\mathfrak{I}[x/a]}$.
- $[\![\forall x\psi]\!]^{\mathfrak{I}} := \min_{a \in A} [\![\psi]\!]^{\mathfrak{I}[x/a]}$.

Es gilt also genau dann $[\![\exists x\psi]\!]^{\mathfrak{I}} = 1$, wenn ein $a \in A$ existiert, so dass $[\![\psi]\!]^{\mathfrak{I}[x/a]} = 1$, und $[\![\forall x\psi]\!]^{\mathfrak{I}} = 1$, wenn für alle $a \in A$ gilt, dass $[\![\psi]\!]^{\mathfrak{I}[x/a]} = 1$.

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

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.

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 (oder eine Formelmenge Φ) wenn alle Funktions- und Relationssymbole von ψ (bzw. Φ) in der Signatur von $\mathfrak{A}$ enthalten sind und alle freien Variablen von ψ (bzw. Φ) 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 2.9 (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) $\mathrm{frei}(\psi) \subseteq \mathrm{dom}(\beta) \cap \mathrm{dom}(\beta')$ und $\beta(x) = \beta'(x)$ für alle $x \in \mathrm{frei}(\psi)$.

Dann gilt $\mathfrak{A} \models \psi[\beta]$ genau dann, wenn $\mathfrak{A}' \models \psi[\beta']$.

Notation. Wie erwähnt, deuten wir mit der Notation $\psi(x_1, \ldots, x_k)$ an, dass $\mathrm{frei}(\psi) \subseteq \{x_1, \ldots, x_k\}$. Sei nun $(\mathfrak{A}, \beta)$ eine Interpretation welche die Variablen $x_1, \ldots, x_k$ durch die Elemente $a_1 = \beta(x_1), \ldots, a_k = \beta(x_k)$ bewertet. Wir schreiben dann anstelle von $\mathfrak{A} \models \psi[\beta]$ meistens $\mathfrak{A} \models \psi(a_1, \ldots, a_k)$. (Diese Notation ist durch das Koinzidenzlemma gerechtfertigt, denn es gilt dann $\mathfrak{A} \models \psi[\beta']$ für *alle* Belegungen β', welche $x_1, \ldots, x_k$ auf $a_1, \ldots a_k$ abbilden.) Ist ψ ein Satz (also $\mathrm{frei}(\psi) = \emptyset$) so schreiben wir $[\![\psi]\!]^{\mathfrak{A}} = 1$ bzw. $\mathfrak{A} \models \psi$ und nennen $\mathfrak{A}$ ein Modell von ψ.

Beispiel. Sei $\psi := \exists z(Exz \wedge Ezy)$ und $\varphi := \forall x \forall y(Exy \to \psi)$. 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 $\mathfrak{A} = (\mathbb{N}, E^{\mathfrak{A}})$, $E^{\mathfrak{A}} = \{(m, n) : m \text{ ist ein echter Teiler von } n\}$ 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 $(Exy \to \psi)$ 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.

Definition 2.10. 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 $\mathcal{K}$.

Beispiel.

- Die Klasse aller *ungerichteten Graphen* ist die Modellklasse von

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

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

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

- Ein Axiomensystem für die Klasse aller linearen Ordnungen ist

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

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

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

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

Die semantische Folgerungsbeziehung $\Phi \models \psi$ („ψ folgt aus Φ“), sowie die Begriffe „erfüllbar“, „allgemeingültig“ und „logisch äquivalent“($\varphi \equiv \psi$) sind wie für die Aussagenlogik definiert.

Definition 2.11 (Semantische Folgerungsbeziehung)**.** Sei $\Phi \subseteq \mathrm{FO}(\tau)$ eine Formelmenge, $\psi \in \mathrm{FO}(\tau)$ eine Formel. Wir sagen, dass ψ *aus* Φ *folgt* (kurz: $\Phi \models \psi$), wenn jede zu $\Phi \cup \{\psi\}$ passende Interpretation, welche ein Modell von Φ ist, auch Modell von ψ ist. Wenn $\Phi = \{\varphi\}$ schreiben wir auch $\varphi \models \psi$ anstelle von $\{\varphi\} \models \psi$.

Beispiel.

- $\Phi_{\mathrm{Gruppe}} \models \psi$ bedeutet, dass ψ in jeder Gruppe gilt. Man beachte, dass Φ_{Gruppe} eine Menge von Sätzen ist, dass aber in ψ durchaus

freie Variablen 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.

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

Definition 2.12. Hat eine Formel ψ (oder 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 zu $\emptyset \models \psi$. Zwei Formeln ψ und φ heißen *logisch äquivalent* (kurz: $\psi \equiv \varphi$), wenn $\psi \models \varphi$ und $\varphi \models \psi$.

Definition 2.13. 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 2.14.

(i) Eine Formel ist genau dann erfüllbar, wenn ihr existentieller Abschluss erfüllbar ist.
(ii) Eine Formel ist genau dann allgemeingültig, wenn ihr universeller Abschluss allgemeingültig ist.

2.5 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) ein Begriff der Äquivalenz gegeben ist (formalisiert durch eine Äquivalenzrelation[1] $\sim$). 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

[1] Erinnerung: Eine Äquivalenzrelation ist reflexiv, symmetrisch und transitiv. Die Äquivalenzklasse von a unter $\sim$ ist $[a] = \{b \mid a \cong b\}$, Elemente von $[a]$ heiß Repräsentanten.

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 2.15 (Ersetzungslemma)**.** Für beliebige Formeln $\psi, \psi', \varphi, \varphi' \in \mathrm{FO}(\tau)$ 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 $\circ \in \{\wedge, \vee, \to\}$.
(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). Q.E.D.

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

(1) $\psi \wedge \varphi \equiv \neg(\neg\psi \vee \neg\varphi)$,
(2) $\psi \to \varphi \equiv \neg\psi \vee \varphi$ und
(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 $\wedge, \to$ und $\forall$ nicht vorkommen, *reduziert*.

Lemma 2.16. 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.[2] 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 Abschnitt 2.6) ist es praktisch, den nicht-monotonen Junktor $\to$ auszuschließen und die Anwendung der Negation auf atomare Formeln einzuschränken.

Definition 2.17. 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 2.18 (Satz über die Negationsnormalform)**.** Jede Formel aus FO ist logisch äquivalent zu einer Formel in Negationsnormalform.

Beweis. Wir haben bereits gesehen, dass $\to$ 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 den Quantorenregeln

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

sowie der Regel

$$\neg\neg\psi \equiv \psi$$

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

kann jede FO-Formel in eine äquivalente Formel transformiert werden, in der Negationen nur noch auf Atome angewandt werden. Q.E.D.

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

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

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).

Termreduzierte Formeln ermöglichen einfachere Induktionsbeweise, weil so keine Induktion über den Aufbau der atomaren Formeln notwendig ist.

Lemma 2.19. 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 $R\ldots t\ldots$ 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 solchen 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. Q.E.D.

PRÄNEX-NORMALFORM. Wir betrachten zunächst einige logische Äquivalenzen für einfache Quantorenanwendungen.

Lemma 2.20. Für alle Formeln $\psi, \varphi \in \mathrm{FO}(\tau)$ gelten die folgenden logischen Äquivalenzen.

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

(ii) Falls x nicht in ψ vorkommt, gilt:

$$\psi \vee \exists x\varphi \equiv \exists x(\psi \vee \varphi), \qquad \psi \wedge \exists x\varphi \equiv \exists x(\psi \wedge \varphi),$$
$$\psi \vee \forall x\varphi \equiv \forall x(\psi \vee \varphi), \qquad \psi \wedge \forall x\varphi \equiv \forall x(\psi \wedge \varphi).$$

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

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

Beweis. 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:

$\mathfrak{I} \models \psi \vee \exists x\varphi$

gdw. $\mathfrak{I} \models \psi$ oder es gibt ein $a \in A$, so dass $\mathfrak{I}[x/a] \models \varphi$

gdw. es gibt ein $a \in A$, so dass $\mathfrak{I}[x/a] \models \psi$ oder $\mathfrak{I}[x/a] \models \varphi$

(Da $x \notin \mathrm{frei}(\psi)$ gilt nach dem Koinzidenzlemma, dass $\mathfrak{I} \models \psi$ gdw. $\mathfrak{I}[x/a] \models \psi$.)

gdw. es gibt ein $a \in A$, so dass $\mathfrak{I}[x/a] \models \psi \vee \varphi$

gdw. $\mathfrak{I} \models \exists x(\psi \vee \varphi)$. Q.E.D.

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) nicht gelten müssen, wenn x in ψ vorkommt.

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

Wir sehen 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 Variablen zu jeder Formel eine äquivalente bereinigte Formel konstruieren kann.

Definition 2.21. 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 und $Q_i \in \{\exists, \forall\}$ ist. Das Anfangsstück $Q_1x_1 \cdots Q_rx_r$ nennt man das *(Quantoren-)Präfix* der Formel.

Die Pränex-Normalform ermöglicht es also, den quantorenfreien Teil einer Formel und das Quantorenpräfix unabhängig voneinander zu untersuchen. Außerdem wird oft die Ausdrucksstärke von prädikatenlogischen Formeln anhand der Struktur des Quantorenpräfix klassifiziert.

Satz 2.22 (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 den Junktor $\rightarrow$ nicht enthält.

- Quantorenfreie Formeln sind bereits in PNF.
- 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 2.20 (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.

- 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 Umbenennung gebundener Variablen erreichen wir, dass diese Formeln die Form $\varphi_1' = Q_1 x_1 \cdots Q_r x_r \vartheta_1$ und $\varphi_2' = Q_1' y_1 \ldots Q_s' y_s \vartheta_2$ haben, 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

  $$\psi' := Q_1 x_1 \cdots Q_r x_r Q_1' y_1 \cdots Q_s' y_s (\vartheta_1' \circ \vartheta_2').$$

  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 2.20 (ii), dass $\psi \equiv \psi'$.
- Sei $\psi = Qx\varphi$ für $Q \in \{\exists, \forall\}$ und sei $\varphi' := Q_1 x_1 \cdots Q_r x_r \vartheta'$ 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. Q.E.D.

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

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

Übung 2.1. Geben Sie zu den folgenden Formeln äquivalente Formeln in PNF an:

(a) $\forall x \exists y Pxy \vee (\neg Qz \wedge \neg \exists x Rxy)$,
(b) $\exists y Rxy$ gdw. $\forall x Rxx$.

Skolem-Normalform. Im Gegensatz zur Pränex-Normalform ist die *Skolem-Normalform* einer Formel im Allgemeinen nicht zur ursprünglichen Formel logisch äquivalent; sie ist jedoch *erfüllbarkeitsäquivalent*

(d.h. die Formel in Skolem-Normalform genau dann erfüllbar, wenn die ursprüngliche Formel erfüllbar ist).

Formeln werden oft in Skolem-Normalform überführt, bevor sie algorithmisch verarbeitet werden, z.B. in automatisierten Beweissystemen oder für prädikatenlogische Resolution (eine Variante der zuvor vorgestellten aussagenlogischen Resolution).

Satz 2.23 (Satz über die Skolem-Normalform)**.** Zu jedem Satz $\psi \in \mathrm{FO}(\sigma)$ lässt sich ein Satz $\varphi \in \mathrm{FO}(\tau)$ mit $\sigma \subseteq \tau$ konstruieren, so dass gilt:

(i) $\varphi = \forall y_1 \cdots \forall y_s \varphi'$, wobei φ' quantorenfrei ist.
(ii) $\varphi \models \psi$.
(iii) 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

$$\psi = Q_1 x_1 \ldots Q_r x_r \vartheta(x_1, \ldots, x_r),$$

wobei $\vartheta(x_1, \ldots, x_r)$ quantorenfrei ist. Für jedes $k \leq r$ sei

$$\psi_k(x_1, \ldots, x_k) := Q_{k+1} x_{k+1} \ldots Q_r x_r \vartheta(x_1, \ldots, x_k, x_{k+1}, \ldots, x_r).$$

Wir eliminieren Existenzquantoren schrittweise von außen nach innen durch folgenden Algorithmus. Sei Q_k der vorderste Existenzquantor. Die gegebene Formel hat also die Form

$$\psi = \forall x_1 \ldots \forall x_{k-1} \exists x_k \psi_k(x_1, \ldots, x_k).$$

Sei f ein neues, d.h. nicht in ψ vorkommendes, $(k-1)$-stelliges Funktionssymbol (für $k = 1$ also ein Konstantensymbol). Setze

$$\psi' := \forall x_1 \cdots \forall x_{k-1} \psi_k(x_1, \ldots, x_{k-1}, f x_1 \cdots x_{k-1}).$$

Also ist ψ' die Formel, die wir aus ψ erhalten, indem wir die vorderste existentiell quantifizierte Variable x_k durch den Term $fx_1 \dots x_{k-1}$ ersetzen und den dazugehörenden Existenzquantor $\exists x_k$ eliminieren. 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

$$\mathfrak{A} \models \psi' := \forall x_1 \cdots \forall x_{k-1} \psi_k(x_1, \dots, x_{k-1}, fx_1 \cdots x_{k-1}).$$

Also folgt, dass für alle $a_1, \dots, a_{k-1} \in A$, und für $b := f^{\mathfrak{A}}(a_1, \dots, a_{k-1})$ gilt, dass $\mathfrak{A} \models \psi_k(a_1, \dots, a_{k-1}, b)$. Damit ist gezeigt, dass

$$\mathfrak{A} \models \forall x_1 \cdots \forall x_{k-1} \exists x_k \psi_k(x_1, \dots, x_k),$$

also $\mathfrak{A} \models \psi$.

Zur zweiten Behauptung nehmen wir an, dass $\mathfrak{A} \models \psi$. Da f in ψ nicht vorkommt, können wir annehmen, dass f nicht in der Signatur von $\mathfrak{A}$ enthalten ist. Wir definieren eine Funktion $f^{\mathfrak{A}} : A^{k-1} \to A$, so dass die Expansion $(\mathfrak{A}, f^{\mathfrak{A}})$ ein Modell von ψ' ist.

Da $\mathfrak{A} \models \forall x_1 \cdots \forall x_{k-1} \exists x_k \psi_k(x_1, \dots, x_k)$ gibt es für alle $a_1, \dots, a_k$ ein b, so dass $\mathfrak{A} \models \psi_k(a_1, \dots, a_{k-1}, b)$. Wir wählen nun für jedes Tupel $(a_1, \dots, a_{k-1})$ *ein* solches b und setzen $f^{\mathfrak{A}}(a_1, \dots, a_{k-1}) := b$. Offensichtlich gilt also für alle $a_1, \dots, a_{k-1}$, dass $(\mathfrak{A}, f^{\mathfrak{A}}) \models \psi_k(a_1, \dots, a_{k-1}, b)$. Damit folgt, dass

$$(\mathfrak{A}, f^{\mathfrak{A}}) \models \forall x_1 \cdots \forall x_{k-1} \psi_k(x_1, \dots, x_{k-1}, fx_1 \cdots x_{k-1}),$$

d.h. $(\mathfrak{A}, f^{\mathfrak{A}}) \models \psi'$. Q.E.D.

Übung 2.2 (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.

2.6 Spieltheoretische Semantik

> Denn, um es endlich auf einmal herauszusagen,
> 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: Über Gott und die Welt*

Die Semantik der Prädikatenlogik kann man auch spieltheoretisch formulieren. Diese Formulierung liefert oft eine intuitivere Sichtweise auf komplexere Formeln. Aus dem hier vorgestellten Auswertungsspiel ergibt sich außerdem ein Algorithmus zur Auswertung von prädikatenlogischen Formeln.

Ein FO-Satz ψ und eine dazu passende Struktur $\mathfrak{A}$ definieren ein *Auswertungsspiel* (Model-Checking-Spiel) $\mathrm{MC}(\mathfrak{A}, \psi)$ zwischen zwei Spielern, der *Verifiziererin V* und dem *Falsifizierer F*. Die Verifiziererin möchte zeigen, dass $\mathfrak{A}$ 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 Positionen des Spiels sind Paare (φ, β) bestehend aus einer Unterformel φ von ψ und einer Belegung $\beta : \mathrm{frei}(\varphi) \to A$. Für $\varphi = \varphi(\bar{x})$ und $\beta : \bar{x} \mapsto \bar{a}$ bezeichnen wir die Position (φ, β) in der Regel durch $\varphi(\bar{a})$.

Das Spiel beginnt bei der Position ψ. Sei $\varphi(\bar{a})$ 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 $\mathfrak{A} \models \varphi(\bar{a})$, andernfalls hat der Falsifizierer gewonnen.
- An einer Position $(\vartheta \vee \eta)$ ist die Verifiziererin am Zug und kann entweder zu ϑ oder zu η ziehen.
- Analog zieht von einer Position $(\vartheta \wedge \eta)$ der Falsifizierer entweder zu ϑ oder zu η.

- An einer Position der Form $\exists x \vartheta(x, \bar{b})$ wählt die Verifiziererin ein Element $a \in A$ und zieht zu $\vartheta(a, \bar{b})$.
- Entsprechend darf an einer Position der Form $\forall x \vartheta(x, \bar{b})$ der Falsifizierer ein Element $a \in A$ auswählen und zur Position $\vartheta(a, \bar{b})$ ziehen.

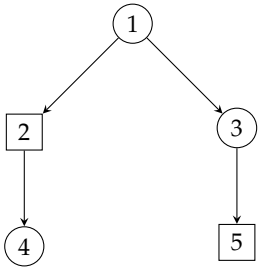


Abbildung 2.1. Ein Spielgraph

Endliche Spiele. Wir geben hier eine allgemeinere Beschreibung von Spielen an (genauer: von Zweipersonenspielen mit vollständiger Information und positionaler Gewinnbedingung). Wir bezeichnen die Spieler als Spieler 0 und Spieler 1 und beschreiben das Spiel durch einen Spielgraphen $\mathcal{G} = (V, V_0, E)$ bestehend aus

- der Menge V aller *Spielpositionen*,
- der Teilmenge $V_0 \subseteq V$ der Positionen, an denen Spieler 0 am Zug ist; entsprechend ist $V_1 := V \setminus V_0$ die Menge der Positionen an denen Spieler 1 am Zug ist,
- der Menge $E \subseteq V \times V$ der möglichen *Züge*.

Beispiel. Abbildung 2.1 zeigt einen Spielgraphen. Dabei ist die Menge V_0 mit Kreisen, die Menge V_1 mit Rechtecken dargestellt.

Für eine Position v sei $vE := \{w : (v, w) \in E\}$ die Menge der unmittelbaren Nachfolgepositionen. Eine Position v mit $vE = \emptyset$ ist eine *Endposition*. Wenn im Spiel eine Endposition erreicht wird, hat der Spieler verloren der am Zug ist (aber nicht ziehen kann). Mit anderen

Worten: Für $\sigma \in \{0, 1\}$ ist die Menge T_σ der Endpositionen, an denen Spieler σ gewonnen hat, definiert durch

$$T_\sigma := \{v \in V_{1-\sigma} : vE = \emptyset\}.$$

Beispiel. Im Beispielgraphen hat also Spieler 0 in Knoten 4 verloren, und Spieler 1 verliert in Knoten 5.

Eine *Partie* mit Anfangsposition v_0 ist ein endlicher oder unendlicher Pfad $(v_0, v_1, \ldots, v_m)$ bzw. $(v_0, v_1, \ldots)$, so dass $(v_{i-1}, v_i) \in E$ für alle $i > 0$ und v_m eine Endposition ist.

Beispiel. Partien sind z.B. die Folgen $(1, 2, 4)$ und $(3, 5)$ im Beispielgraphen.

Auswertungsspiele für FO sind insofern speziell als alle Partien endlich sind (da jeder Zug die Komplexität der Formel reduziert). Spiele mit dieser Eigenschaft nennt man *fundiert*.[3]
Eine *Strategie* für Spieler σ ist eine Funktion

$$f : \{v \in V_\sigma : vE \neq \emptyset\} \to V,$$

so dass $(v, f(v)) \in E$; sie ordnet also jeder nicht-terminalen Position von Spieler σ einen Zug zu. Wenn Spieler σ jede Partie mit Anfangsposition v_0 gewinnt, wenn er mit Strategie f spielt, dann ist f eine *Gewinnstrategie* von Position v_0 aus. Formaler: Eine Partie $v_0 v_1 \ldots$ ist konsistent mit der Strategie f wenn für alle i mit $v_i \in V_\sigma$ gilt, dass $v_{i+1} = f(v_i)$; f ist Gewinnstrategie für Spieler σ von v_0, wenn jede bei v_0 beginnende und mit f konsistente Partie endlich ist und in einer Position in T_σ endet. Die *Gewinnregion* von Spieler σ ist

$$W_\sigma := \{v : \text{Spieler } \sigma \text{ hat eine Gewinnstrategie von Position } v\}.$$

Ein Spiel ist *determiniert*, wenn von jeder Position aus einer der beiden Spieler eine Gewinnstrategie hat, d.h. wenn $W_0 \cup W_1 = V$.

Beispiel. Die Strategien für Spieler 0 im Spiel in Abbildung 2.1 sind die

[3] Allgemeine Spiele lassen auch unendliche Partien zu. In der Theorie unendlicher Spiele braucht man daher Gewinnbedingungen für unendliche Partien. Hier werten wir unendliche Partien als unentschieden.

Funktionen $f : 1 \mapsto 2, 3 \mapsto 5$ und $g : 1 \mapsto 3, 3 \mapsto 5$. Nur g ist auch eine Gewinnstrategie von Position 1 aus. Die Partie $(1, 3, 5)$ ist konsistent mit g. Die Gewinnregion von Spieler 0 ist $\{1, 3, 5\}$, die Gewinnregion von Spieler 1 ist $\{2, 4\}$. Das Spiel ist also determiniert.

Übung 2.3. Zeigen Sie, dass fundierte Spiele determiniert sind.

Sei nun $\psi \in \mathrm{FO}$ und $\mathfrak{A}$ eine zu ψ passende Struktur. Per Induktion über den Aufbau von $\varphi(\bar{x})$ zeigt man leicht, dass in dem Spiel $\mathrm{MC}(\mathfrak{A}, \psi)$ die Verifiziererin eine Gewinnstrategie von Position $\varphi(\bar{a})$ hat, wenn $\mathfrak{A} \models \varphi(\bar{a})$, und dass der Falsifizierer eine Gewinnstrategie von Position $\varphi(\bar{a})$ hat, wenn $\mathfrak{A} \models \neg\varphi(\bar{a})$. Insbesondere folgt damit:

Satz 2.24. Für jeden Satz $\psi \in \mathrm{FO}(\tau)$ und jede τ-Struktur $\mathfrak{A}$ gilt: $\mathfrak{A} \models \psi$ genau dann, wenn die Verifiziererin eine Gewinnstrategie für das Spiel $\mathrm{MC}(\mathfrak{A}, \psi)$ von der Anfangsposition ψ hat.

Algorithmen für Strategieprobleme. Sei Game das Strategieproblem für Spiele mit endlichen Spielgraphen, d.h.

$$\textsc{Game} = \{(\mathcal{G}, v) : \text{Spieler 0 hat eine Gewinnstrategie für } \mathcal{G} \text{ von Position } v\}.$$

Es ist nicht schwer einzusehen, dass man Game in Polynomialzeit lösen kann. Sei W_σ^n die Menge der Positionen von denen Spieler σ eine Strategie hat, um in höchstens n Zügen zu gewinnen. Dann ist $W_\sigma^0 = T_\sigma = \{v \in V_{1-\sigma} : vE = \emptyset\}$ die Menge der Endpositionen an denen Spieler σ gewonnen hat, und wir können die Mengen W_σ^n induktiv berechnen mit

$$W_\sigma^{n+1} := \{v \in V_\sigma : vE \cap W_\sigma^n \neq \emptyset\} \cup \{v \in V_{1-\sigma} : vE \subseteq W_\sigma^n\}$$

bis $W_\sigma^{n+1} = W_\sigma^n$.

Beispiel. Für den Beispielgraphen in Abbildung 2.1 würden die Gewinnregionen wie folgt berechnet. W_0^0 besteht aus allen Knoten in V_1, die keine Nachfolger haben, also $W_0^0 = \{5\}$. Analog gilg $W_1^0 = \{4\}$. W_0^1 besteht aus allen Knoten, in denen Spieler 0 am Zug ist und die

mindestens einen Nachfolger in W_0^0 haben, sowie Knoten von Spieler 1, die nur Nachfolger in W_0^0 haben. Also $W_0^1 = \{3, 5\}$ und $W_1^1 = \{2, 4\}$. Schließlich gilt $W_0^2 = \{1, 3, 5\}$, da $1 \in V_0$ und $3 \in W_0^1$.

Man kann das Game-Problem sogar in *Linearzeit* lösen. Der folgende Algorithmus ist eine Variante der Tiefensuche und berechnet die Gewinnregionen W_σ für beide Spieler in Zeit $O(|V| + |E|)$.

Satz 2.25. Die Gewinnregionen von endlichen Spielen kann man in Linearzeit berechnen.

Beweis. Wir präsentieren einen Algorithmus welcher für jede Position bestimmt, ob einer der Spieler von dieser Position aus eine Gewinnstrategie hat, und wenn ja welcher. Wir benutzen die folgenden Arrays:

- $\mathrm{win}[v]$ enthält entweder $\sigma \in \{0, 1\}$, wenn schon festgelegt ist, dass $v \in W_\sigma$ oder $\perp$, wenn dies noch nicht ausgerechnet ist, oder wenn keiner der Spieler von v aus eine Gewinnstrategie hat.
- $P[v]$ enthält die Vorgänger von v.
- $n[v]$ ist die Anzahl der Nachfolger $w \in vE$ für die $\mathrm{win}[w] = \perp$.

Der Kern von Algorithmus 2.1 ist die Prozedur $\mathrm{Propagate}(v, \sigma)$ welche immer dann aufgerufen wird, wenn festgestellt wurde, dass Spieler σ eine Gewinnstrategie von Position v hat. $\mathrm{Propagate}(v, \sigma)$ speichert dies ab und untersucht, ob wir nun den Gewinner für die Vorgänger von v bestimmen können. Dies wird mit folgenden Regeln festgestellt:

- Wenn der Vorgänger u auch eine Position von Spieler σ ist, dann hat er eine Gewinnstrategie, indem er im ersten Zug zu v zieht.
- Wenn der Gegner von Position u zieht, $\mathrm{win}[u]$ noch undefiniert ist, und der Gewinner für alle Nachfolger w von u bereits festgestellt ist, dann ist $\mathrm{win}[w] = \sigma$ für alle diese w, und Spieler σ gewinnt daher auch von u unabhängig vom Zug seines Gegners.

Da (4) und (5) für jede Position v nur einmal erreicht werden, wird der innere Teil der Schleife in (5) höchstens $\sum_v |P[v]| = |E|$-mal durchlaufen. Die Laufzeit des Algorithmus ist daher $O(|V| + |E|)$.

Die Korrektheit des ausgerechneten Wertes $\mathrm{win}[v]$ beweist man durch Induktion über die minimale Anzahl der Züge mit der ein Spieler

Algorithmus 2.1. Ein Linearzeit-Algorithmus für das GAME-Problem

Input: Ein Spiel $\mathcal{G} = (V, V_0, E)$

for all $v \in V$ **do** $(*$ 1: Initialisierung $*)$
  $\text{win}[v] := \bot$
  $P[v] := \emptyset$
  $n[v] := 0$
end do

for all $(u, v) \in E$ **do** $(*$ 2: Berechne P und n $*)$
  $P[v] := P[v] \cup \{u\}$
  $n[u] := n[u] + 1$
end do

for all $v \in V_0$ $(*$ 3: Berechne win $*)$
  if $n[v] = 0$ **then** Propagate(v, 1)
for all $v \in V \setminus V_0$
  if $n[v] = 0$ **then** Propagate(v, 0)
return win

procedure Propagate(v, σ)
  if $\text{win}[v] \neq \bot$ **then return**
  $\text{win}[v] := \sigma$ $(*$ 4: Markiere v als gewinnend für σ $*)$
  for all $u \in P[v]$ **do** $(*$ 5: Propagiere zu Vorgängern $*)$
    $n[u] := n[u] - 1$
    if $u \in V_\sigma$ or $n[u] = 0$ **then** Propagate(u, σ)
  end do
end

von v aus gewinnen kann. Man beachte, dass die Positionen mit $n[v] = 0$ in (3) genau die Endpositionen sind, auch wenn $n[v]$ durch Propagate modifiziert wird. Q.E.D.

Übung 2.4 (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 2.5. Formulieren Sie ein Auswertungsspiel für FO-Formeln, welche nicht notwendigerweise in Negationsnormalform sind. Welcher spieltheoretischen Operation entspricht die Negation?

Übung 2.6. Wir wissen bereits, dass das Erfüllbarkeitsproblem für aussagenlogische Hornformeln in Polynomialzeit lösbar ist. Mit Hilfe des GAME-Problems kann man auf relativ einfache Weise zeigen, dass es sogar einen Linearzeit-Algorithmus gibt.

Konstruieren Sie zu einer gegebenen Hornformel $\psi = \bigwedge_{i \in I} C_i$ mit Aussagenvariablen $X_1, \ldots, X_n$ und Horn-Implikationen C_i der Form $X_{i_1} \wedge \cdots X_{i_m} \to Z$ ein Spiel $\mathcal{G}_\psi$: Die Positionen von Spieler 0 sind die Anfangsposition 0 und die Aussagenvariablen $X_1, \ldots, X_n$, die Positionen von Spieler 1 sind die C_i. Spieler 0 kann von einer Position X zu irgendeiner Implikation C_i mit rechter Seite X ziehen, und Spieler 1 kann von Position C_i zu irgendeiner Variable ziehen, die auf der linken Seite von C_i vorkommt. Zeigen Sie, dass Spieler 0 genau dann eine Gewinnstrategie für $\mathcal{G}_\psi$ von Position X hat, wenn $\psi \models X$. Insbesondere ist ψ genau dann unerfüllbar, wenn Spieler 0 von der Anfangsposition 0 gewinnt.

Übung 2.7 (Umkehrung der letzten Übung)**.** Konstruieren Sie zu jedem Spiel $\mathcal{G}$ eine aussagenlogische Hornformel $\psi_\mathcal{G}$, deren Aussagenvariablen die Positionen von $\mathcal{G}$ sind und deren minimales Modell gerade die Gewinnregion W_0 ist. Insbesondere ist $v \in W_0$ genau dann, wenn $\psi_\mathcal{G} \wedge (v \to 0)$ unerfüllbar ist.

3 Definierbarkeit in der Prädikatenlogik

3.1 Definierbarkeit

Axiomatisierbare Strukturklassen. Wir haben bereits in Kapitel 2 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 3.1. Sei (τ) die Klasse aller τ-Strukturen. Eine Strukturklasse $\mathcal{K} \subseteq (\tau)$ 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 und 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 2.4 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.

Beispiel 3.2.

- Die Klasse aller Körper ist axiomatisiert durch $\psi_{\text{Körper}} \in \text{FO}(\tau_{\text{ar}})$, die Konjunktion aller Körperaxiome. Für jede Primzahl p ist auch die Klasse der Körper mit Charakteristik p[1] 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

  $$\Phi = \{\psi_{\text{Körper}}\} \cup \{\neg\chi_p : p \text{ Primzahl}\}.$$

- Auch die Klasse ACF der algebraisch abgeschlossenen Körper[2] (algebraically closed fields) 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 $\underbrace{x \cdot x \cdot \cdots \cdot x}_{n \text{ mal}}$ aufzufassen.) Also ist $\Phi_{\text{ACF}} = \{\psi_{\text{Körper}}\} \cup \{\psi_n : n \geq 1\}$ ein Axiomensystem für algebraisch abgeschlossene Körper.

Übung 3.1. Sei $\mathfrak{A}$ eine endliche Struktur mit endlicher Signatur. Zeigen Sie, dass die Klasse $\{\mathfrak{B} : \mathfrak{B} \cong \mathfrak{A}\}$ der zu $\mathfrak{A}$ isomorphen Strukturen 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 zumindest kein endliches Axiomensystem zulässt, sind andere Methoden erforderlich, welche in diesem und dem folgenden Kapitel entwickelt werden sollen.

[1] Ein Körper hat Charakteristik p, wenn p die kleinste natürliche Zahl ist, sodass p-faches addieren des Einselements das Nullelement ergibt. Falls kein solches p existiert, hat der Körper Charakteristik 0.

[2] Ein Körper K ist algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom mit Koeffizienten aus K eine Nullstelle in K besitzt.

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 3.3. 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 $x = t$.

Beispiel 3.4.

- Die Ordnungsrelation $<$ auf $\mathbb{R}$ ist elementar definierbar in $(\mathbb{R}, +, \cdot, 0, 1)$, denn für die Formel $\varphi(x, y) := \exists z (z \neq 0 \wedge x + z \cdot z = y)$ gilt:

  $$a < b \quad \text{gdw.} \quad (\mathbb{R}, +, \cdot, 0, 1) \models \varphi(a, b).$$

- In $(\mathbb{Z}, <)$ ist die Nachfolgerfunktion $z \mapsto z + 1$ elementar definierbar durch die Formel $\varphi(x, y) := x < y \wedge \forall z (x < z \wedge y \neq z \to y < z)$.
- In $(\mathbb{N}, +, 0, 1)$ ist jedes n termdefinierbar durch den Term $\underline{n} = \underbrace{1+\cdots+1}_{n \text{ mal}}$ (für $n \geq 1$).

- 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 $\underline{p} \cdot x = \underline{q}$ oder $\underline{p} \cdot x + \underline{q} = 0$, nicht aber termdefinierbar.
- 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 $\varphi(x) \in \mathrm{FO}(\tau_{\mathrm{ar}})$.

Als nächstes beobachten wir, dass das Hinzunehmen definierbarer Relationen zu einer Struktur keinen Gewinn an Ausdruckstärke bringt.

Lemma 3.5. 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 $R_1, \dots, R_s$ bzw. $f_1, \dots, f_t$ aus $\tau \setminus \sigma$ 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 2.19 annehmen, dass ψ termreduziert ist, d.h. dass Funktionssymbole aus $\tau \setminus \sigma$ nur in Atomen der Form $f_j\bar{y} = z$ auftreten. Indem wir in $\psi(\bar{x})$ die Relations- und Funktionssymbole aus $\tau \setminus \sigma$ 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 $\psi^{\mathfrak{B}} = \varphi^{\mathfrak{A}}$. Q.E.D.

Exkurs: Relativierte Quantoren. Wir illustrieren hier die Verwendung relativierter Quantoren an einem Beispiel.

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 ...“ bzw. „für alle x mit α gilt ...“ durch $\exists x(\alpha \wedge \cdots)$ bzw. $\forall x(\alpha \to \cdots)$ formalisiert werden können. Gelegentlich wird die Schreibweise $(\exists x\,.\,\alpha)\psi$ als Umschreibung für $\exists x(\alpha \wedge \psi)$ und $(\forall x\,.\,\alpha)\psi$ für $\forall x(\alpha \to \psi)$ benutzt. [3]

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 wird nun beschrieben durch den Ausdruck

$$\psi(x) := (\forall u\,.\,0 < u)(\exists z\,.\,0 < z)\forall y(\varphi(x, y, z) \to \varphi(fx, fy, u)).$$

Mit den oben dargestellten Äquivalenzen lässt sich die Stetigkeit dann als Formel der Prädikatenlogik ausdrücken.

3.2 Das Isomorphielemma

Zwei Strukturen sind isomorph, wenn sie sich nur durch Umbenennung der Elemente des Universums unterscheiden. Logiken sollen, im Gegensatz zu Algorithmen, nur Aussagen über Eigenschaften einer Struktur treffen, die unabhängig von deren Kodierung sind. Daher wird, um zu prüfen, ob ein Formalismus eine sinnvolle Logik ist, sichergestellt, dass sie nicht zwischen isomorphen Strukturen unterscheiden kann. Im

[3] Beachten Sie jedoch, dass im Rahmen der Vorlesung und Übung mit „Prädikatenlogik“ immer die Logik ohne die so erweiterte Syntax gemeint ist (da sich insbesondere nicht alle vorgestellten Beweise und Verfahren direkt auf diese Schreibweise übertragen lassen).

folgenden beweisen wir das Isomorphielemma, das besagt, dass die Prädikatenlogik in diesem Sinne eine sinnvolle Logik ist.

Definition 3.6. $\mathfrak{A}$ und $\mathfrak{B}$ seien τ-Strukturen. Ein *Isomorphismus von* $\mathfrak{A}$ *nach* $\mathfrak{B}$ ist eine bijektive Abbildung $\pi : A \to B$, so dass folgende Bedingungen erfüllt sind:

(1) Für jedes (n-stellige) Relationssymbol $R \in \tau$ und alle $a_1, \dots, a_n \in A$ gilt:

$$(a_1, \dots, a_n) \in R^{\mathfrak{A}} \text{ gdw. } (\pi a_1, \dots, \pi a_n) \in R^{\mathfrak{B}}.$$

(2) Für jedes (n-stellige) Funktionssymbol $f \in \tau$ und alle $a_1, \dots, a_n \in A$ gilt:

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

Bemerkung 3.7. Für jedes $n \in \mathbb{N}$ lässt sich π auf natürliche Weise zu einer Abbildung $\pi : A^n \to B^n$ erweitern mit $\pi(a_1, \dots, a_n) := (\pi a_1, \dots, \pi a_n)$. Bedingung (1) können wir dann auch so formulieren: Für alle Relationssymbole $R \in \tau$ ist $\pi(R^{\mathfrak{A}}) = R^{\mathfrak{B}}$. Bedingung (2) bedeutet, dass für alle Funktionssymbole $f \in \tau$ gilt: $\pi \circ f^{\mathfrak{A}} = f^{\mathfrak{B}} \circ \pi$.

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

Definition 3.8. 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. Die Identitätsabbildung auf $\mathfrak{A}$ bezeichnen wir mit $1_{\mathfrak{A}}$.

Die Menge aller Automorphismen einer Struktur $\mathfrak{A}$ bilden bezüglich Hintereinanderausführung 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 der triviale Automorphismus $1_{\mathfrak{A}}$ der einzige Automorphismus der Struktur ist.

Isomorphe Strukturen betrachten wir als gleich. Insbesondere können FO-Formeln nicht zwischen isomorphen Strukturen unterscheiden.

Lemma 3.9 (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 $a_1, \dots, a_n \in A$:

$$\mathfrak{A} \models \psi(a_1, \dots, a_n) \text{ gdw. } \mathfrak{B} \models \psi(\pi a_1, \dots, \pi a_n).$$

Beweis. Per Induktion über den Termaufbau zeigt man sofort, dass für jeden Term $t(\bar{x}) \in \mathrm{T}(\tau)$ mit Variablen aus $x_1, \dots, x_n$ und für alle $\bar{a} = a_1, \dots, a_n$ gilt:

$$\pi[\![t(\bar{a})]\!]^{\mathfrak{A}} = [\![t(\pi\bar{a})]\!]^{\mathfrak{B}}. \tag{*}$$

Wir führen nun den Beweis per Induktion über den Formelaufbau; nach Lemma 2.16 können wir dabei annehmen, dass ψ reduziert ist.

(1) Für Formeln der Form $t_1(\bar{x}) = t_2(\bar{x})$ gilt

$$\begin{aligned}
\mathfrak{A} \models t_1(\bar{a}) = t_2(\bar{a}) \text{ gdw. } & [\![t_1(\bar{a})]\!]^{\mathfrak{A}} = [\![t_2(\bar{a})]\!]^{\mathfrak{A}} \\
\text{gdw. } & \pi[\![t_1(\bar{a})]\!]^{\mathfrak{A}} = \pi[\![t_2(\bar{a})]\!]^{\mathfrak{A}} \\
& \text{(da } \pi \text{ injektiv ist)} \\
\text{gdw. } & [\![t_1(\pi\bar{a})]\!]^{\mathfrak{B}} = [\![t_2(\pi\bar{a})]\!]^{\mathfrak{B}} \\
& \text{(nach (*))} \\
\text{gdw. } & \mathfrak{B} \models t_1(\pi\bar{a}) = t_2(\pi\bar{a})
\end{aligned}$$

(2) Für Atome $Pt_1 \dots t_n$ gilt

$$\begin{aligned}
\mathfrak{A} \models Pt_1(\bar{a}) \cdots t_n(\bar{a}) \text{ gdw. } & ([\![t_1(\bar{a})]\!]^{\mathfrak{A}}, \dots, [\![t_n(\bar{a})]\!]^{\mathfrak{A}}) \in P^{\mathfrak{A}} \\
\text{gdw. } & (\pi[\![t_1(\bar{a})^{\mathfrak{A}}]\!], \dots, \pi[\![t_n(\bar{a})]\!]^{\mathfrak{A}}) \in P^{\mathfrak{B}} \\
& \text{(da } \pi \text{ ein Isomorphismus ist)} \\
\text{gdw. } & ([\![t_1(\pi\bar{a})]\!]^{\mathfrak{B}}, \dots, [\![t_n(\pi\bar{a})]\!]^{\mathfrak{B}}) \in P^{\mathfrak{B}} \\
& \text{(nach (*))} \\
\text{gdw. } & \mathfrak{B} \models Pt_1(\pi\bar{a}) \cdots t_n(\pi\bar{a})
\end{aligned}$$

(3) Für Formeln der Form $\neg\psi$ oder $\psi \vee \varphi$ ist der Induktionsschluss trivial.
(4) Für Formeln $\exists y\psi(\bar{x}, y)$ gilt

$$\begin{aligned}
\mathfrak{A} \models \exists y\psi(\bar{a}, y) \text{ gdw. } & \mathfrak{A} \models \psi(\bar{a}, c) \text{ für ein } c \in A \\
\text{gdw. } & \mathfrak{B} \models \psi(\pi\bar{a}, \pi c) \text{ für ein } c \in A \\
& \text{(nach Induktionsvoraussetzung)} \\
\text{gdw. } & \mathfrak{B} \models \psi(\pi\bar{a}, b) \text{ für ein } b \in B \\
& \text{(da } \pi \text{ bijektiv ist)} \\
\text{gdw. } & \mathfrak{B} \models \exists y\psi(\pi\bar{a}, y). \qquad \text{Q.E.D.}
\end{aligned}$$

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:

$$\mathfrak{A} \models \psi \text{ gdw. } \mathfrak{B} \models \psi.$$

Daraus folgt, dass axiomatisierbare Modellklassen unter Isomorphie abgeschlossen sind. Dies bedeutet, dass für jede Klasse $\mathcal{K} = \mathrm{Mod}(\psi)$ und jedes Paar von isomorphen Strukturen $\mathfrak{A} \cong \mathfrak{B}$ gilt:

$$\mathfrak{A} \in \mathcal{K} \text{ gdw. } \mathfrak{B} \in \mathcal{K}.$$

In manchen Fällen liefert das Isomorphielemma ein einfaches Kriterium, um nachzuweisen, dass eine Relation in einer Struktur *nicht* elementar definierbar ist: Wir zeigen, dass sich nach dem Isomorphielemma nur Eigenschaften in FO definieren lassen, die unter Automorphismen erhalten bleiben.

Lemma 3.10. Sei π ein Automorphismus einer τ-Struktur $\mathfrak{A}$, und sei $\psi \in \mathrm{FO}(\tau)$. Dann ist π auch ein Automorphismus der expandierten Struktur $(\mathfrak{A}, \psi^{\mathfrak{A}})$.

Beweis. Da π ein Automorphismus ist, gilt für alle Tupel $\bar{a}$ aus A:

$$\mathfrak{A} \models \psi(\bar{a}) \text{ gdw. } \mathfrak{A} \models \psi(\pi\bar{a}).$$

Also ist $\pi(\psi^{\mathfrak{A}}) = \psi^{\mathfrak{A}}$. Q.E.D.

Natürlich folgt aus dem Isomorphielemma, dass π nicht in $\mathfrak{A}$ definierbar sein kann.

Beispiel 3.11. 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 3.2. Sei $\tau = \emptyset$ und A unendlich. Beschreiben Sie alle in A elementar definierbaren Relationen $R \subseteq A^n$.

Übung 3.3. Zeigen Sie, dass in $(\mathbb{N}, \cdot, 1)$ die Addition nicht elementar definierbar ist.

3.3 Theorien und elementar äquivalente Strukturen

Das Isomorphielemma liefert ein Kriterium dafür, dass bestimmte Strukturen in FO nicht unterscheidbar sind. Die Definition der Nichtunterscheidbarkeit, genannt elementare Äquivalenz, basiert auf dem Begriff der Theorie:

Definition 3.12. 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 mit $T \models \psi$, dass $\psi \in T$ gilt.

Eine Theorie T ist *vollständig*, wenn für jeden Satz $\psi \in \mathrm{FO}(\tau)$ entweder $\psi \in T$ oder $\neg\psi \in T$ gilt.

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 3.13. 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:

$$\mathfrak{A} \models \psi \text{ gdw. } \mathfrak{B} \models \psi.$$

Lemma 3.14. Eine Theorie ist genau dann vollständig, 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. Q.E.D.

Aus dem Isomorphielemma folgt unmittelbar, dass isomorphe Strukturen auch elementar äquivalent sind. Wie wir später sehen werden, gilt die Umkehrung dieser Aussage nicht.

Definition 3.15. 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 $\circ \in \{\wedge, \vee, \to, \leftrightarrow\}$ und
(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 3.16. Der Quantorenrang von $\forall x(\exists y Pxy \to \forall z Pxz)$ ist 2. Eine äquivalente Formel in PNF ist $\forall x \forall y \forall z(Pxy \to Pxz)$. Man beachte, dass die Transformation in PNF in der Regel den Quantorenrang erhöht.

Definition 3.17. Zwei τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ sind *m-äquivalent* ($\mathfrak{A} \equiv_m \mathfrak{B}$), wenn für alle τ-Sätze ψ mit $\mathrm{qr}(\psi) \leq m$ gilt:

$$\mathfrak{A} \models \psi \text{ gdw. } \mathfrak{B} \models \psi.$$

Wir erweitern die Begriffe der elementaren Äquivalenz und der m-Äquivalenz auf Strukturen mit Parametern, d.h. Strukturen, 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 $(\mathfrak{A}, \bar{a}) \equiv_m (\mathfrak{B}, \bar{b})$.

3.4 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 Methode, um elementare Äquivalenz und m-Äquivalenz nachzuweisen. Solche Methoden liefern eine vergleichsweise intuitive Möglichkeit, zu beweisen, dass eine Eigenschaft nicht logisch definierbar ist.

Der Einfachheit halber betrachten wir für den Rest dieses Kapitels nur relationale Strukturen.

Definition 3.18. 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 $p : \mathrm{dom}(p) \to B$ wobei $\mathrm{dom}(p) \subseteq A$, so dass für alle $n \in \mathbb{N}$, alle n-stelligen Relationssymbole $R \in \tau$ und alle $a_1, \ldots, a_n \in \mathrm{dom}(p)$ gilt:

$$(a_1, \ldots, a_n) \in R^{\mathfrak{A}} \text{ gdw. } (pa_1, \ldots, pa_n) \in R^{\mathfrak{B}}.$$

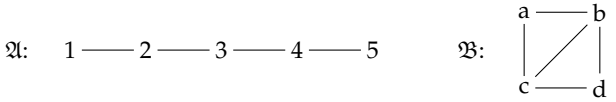
Die Menge aller lokalen Isomorphismen von $\mathfrak{A}$ nach $\mathfrak{B}$ bezeichnen wir mit $\mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$.

Lokale Isomorphismen erhalten also auf einer Substruktur Gleichheiten und Relationen, und damit genau die Eigenschaften, die mit atomaren Formeln über Elementen der Substruktur ausgedrückt werden können.

Das Bild von p ist $\mathrm{bild}(p) := \{pa : a \in \mathrm{dom}(p)\}$. Die *leere Abbildung* p mit $\mathrm{dom}(p) = \mathrm{bild}(p) = \emptyset$ ist trivialerweise ein lokaler Isomorphismus. Ein nicht-leerer lokaler Isomorphismus ist ein Isomorphismus zwischen den von $\mathrm{dom}(p)$ 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 $\{(a, pa) : a \in \mathrm{dom}(p)\}$. Insbesondere nennen wir p endlich, wenn sein Graph endlich ist.

Beispiel 3.19.

- Betrachte die beiden folgenden Graphen $\mathfrak{A}$ und $\mathfrak{B}$:



  Dann ist $p = \{(2, a), (3, b), (4, d)\}$ ein lokaler Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$.
- Seien $(\mathfrak{A}, <^{\mathfrak{A}})$ und $\mathfrak{B} = (B, <^{\mathfrak{B}})$ lineare Ordnungen und $a_1, \ldots, a_n$ paarweise verschiedene Elemente von A. Eine Abbildung $p : a_1 \mapsto b_1, \ldots, a_n \mapsto b_n$ ist ein lokaler Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ genau dann wenn eine Permutation $s : \{1, \ldots, n\} \to \{1, \ldots, n\}$ 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 $A \cap B = \emptyset$. 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 $a_1, \ldots, a_m$ aus $\mathfrak{A}$ und $b_1, \ldots, b_m$ aus $\mathfrak{B}$ ausgezeichnet. Die Duplikatorin hat die Partie gewonnen, wenn die Menge $\{(a_1, b_1), \ldots, (a_m, b_m)\}$ 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* $(a_1, \ldots, a_i, b_1, \ldots, b_i)$ erreicht. Das verbleibende Teilspiel, mit $m - i$ Zügen, bezeichnen wir mit $G_{m-i}(\mathfrak{A}, a_1, \ldots, a_i, \mathfrak{B}, b_1, \ldots, b_i)$.

Eine *Gewinnstrategie* 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 (vgl. Übung 2.3).

Beispiel 3.20.

- Sei $\mathfrak{A} = (\mathbb{Z}, <)$, $\mathfrak{B} = (\mathbb{R}, <)$. Die Duplikatorin gewinnt $G_2(\mathfrak{A}, \mathfrak{B})$, aber der Herausforderer gewinnt $G_3(\mathfrak{A}, \mathfrak{B})$ (siehe auch Beispiel 3.23).
- Für $\tau = \{E, P\}$ (wobei P einstelliges und E zweistelliges Relationssymbol) betrachte die beiden Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ in Abbildung 3.1. Auch hier gewinnt der Herausforderer $G_3(\mathfrak{A}, \mathfrak{B})$, die Duplikatorin aber $G_2(\mathfrak{A}, \mathfrak{B})$ (Beweis: Übung).

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

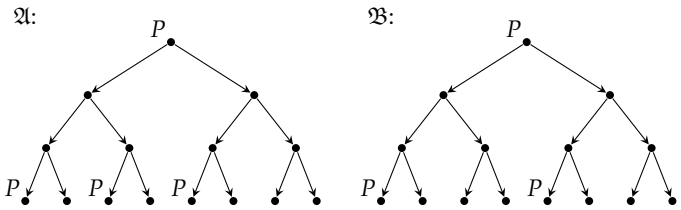


Abbildung 3.1. Zwei Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ mit $\mathfrak{A} \equiv_2 \mathfrak{B}$ und $\mathfrak{A} \not\equiv_3 \mathfrak{B}$

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 3.21 (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. Dazu beweisen wir die folgende etwas stärkere Aussage.

Satz 3.22. Seien $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen, $\bar{a} = a_1, \ldots, a_r \in A$, $\bar{b} = b_1, \ldots, b_r \in B$. 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 $\{(a_1, b_1), \ldots, (a_r, b_r)\}$ 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 $(\bar{a}, c, \bar{b}, d)$ 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 $G_{m-1}(\mathfrak{A}, \bar{a}, c, \mathfrak{B}, \bar{b}, d)$. Q.E.D.

Daraus erhalten wir (indem wir $r = 0$ setzen und somit Sätze betrachten) die Implikationen *(ii)* $\Rightarrow$ *(i)* des Satzes von Ehrenfeucht und Fraïssé:

(1) Wenn die Duplikatorin das Spiel $G(\mathfrak{A}, \mathfrak{B})$ gewinnt, so gilt $\mathfrak{A} \equiv \mathfrak{B}$;
(2) Wenn die Duplikatorin das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gewinnt, so gilt $\mathfrak{A} \equiv_m \mathfrak{B}$.

Beispiel 3.23. 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 gewinnt der Herausforderer also $G_3(\mathfrak{A}, \mathfrak{B})$. 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. Hier ist insbesondere zu sehen, dass der Herausforderer gewinnt, indem er die Struktur wechselt.

ANWENDUNGEN. Der Satz von Ehrenfeucht-Fraïssé liefert eine wichtige Methode, um zu zeigen, dass eine Modellklasse $\mathcal{K}$ *nicht* elementar axiomatisierbar 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 $(\mathfrak{A}_m)_{m\in\mathbb{N}}$ und $(\mathfrak{B}_m)_{m\in\mathbb{N}}$ 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 axiomatisierbar 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 3.24. Sei $\tau = \emptyset$ 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 $\mathfrak{B}_m = \{1, \dots, m\}$. Dann gewinnt die Duplikatorin das Spiel $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$, weil jede injektive Funktion, die nur auf m Elementen definiert ist, ein partieller Isomorphismus ist, sie also nur Gleichheiten und Ungleichheiten erhalten muss. Also trennt kein Satz $\psi \in \mathrm{FO}(\emptyset)$ 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 3.25. 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:

$$\begin{aligned}\mathfrak{A} \models \varphi(a, b) \text{ gdw. es gibt in } \mathfrak{A} \text{ einen } E\text{-Pfad von } a \text{ nach } b\\ \text{gdw. es gibt } n > 0 \text{ und } c_0, \dots, c_n \in A \text{ mit } c_0 = a,\\ c_n = b \text{ und } (c_i, c_{i+1}) \in E \text{ für alle } i < n.\end{aligned}$$

Satz 3.25 folgt unmittelbar aus dem folgendem Satz, den wir mit der Ehrenfeucht-Fraïssé-Methode beweisen.

Satz 3.26. Es gibt keinen Satz $\psi \in \mathrm{FO}(\tau)$, so dass für jeden (endlichen, ungerichteten) Graphen $G = (V, E)$ gilt:

$$G \models \psi \text{ gdw. } G \text{ ist zusammenhängend.}$$

Wenn Satz 3.25 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 $\psi := \forall x \forall y \varphi(x, y)$ ausdrücken, 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 $\mathfrak{A}_m$ (wie in Abbildung 3.2 illustriert). Es ist zu zeigen, dass die Duplikatorin $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$ gewinnt.

Um die Gewinnstrategie für die Duplikatorin zu motivieren, betrachten wir zunächst eine Gewinnstrategie für den Herausforderer im Spiel mit $m+1$ Zügen. Dabei wählt der Herausforderer zunächst Elemente b_1, b_2, die in verschiedenen Zusammenhangskomponenten von $\mathfrak{B}_m$ liegen. Da $\mathfrak{A}_m$ nur eine Zusammenhangskomponente hat, muss die Duplikatorin zwei Elemente a_1, a_2 von $\mathfrak{A}_m$ wählen, die durch einen Pfad der Länge höchstens 2^{m-1} verbunden sind. In den folgenden $m-1$

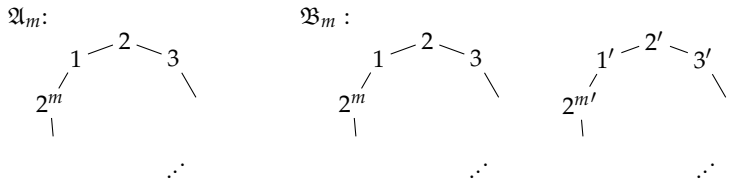


Abbildung 3.2. Die Strukturen $\mathfrak{A}_m$ und $\mathfrak{B}_m$.

Zügen weist der Herausforderer die Existenz dieses Pfades nach, indem er die Distanz zwischen je zwei bereits gewählten Knoten in jedem Zug halbiert. In Abbildung 3.3 sind die Züge des Herausforderers für $m = 4$ eingezeichnet, für den Fall, dass die Duplikatorin b_3 in derselben Zusammenhangskomponente wie b_2 wählt. Dann kann sie im letzten Zug kein Element b_5 wählen, das eine Kante zu b_1 und b_4 hat.

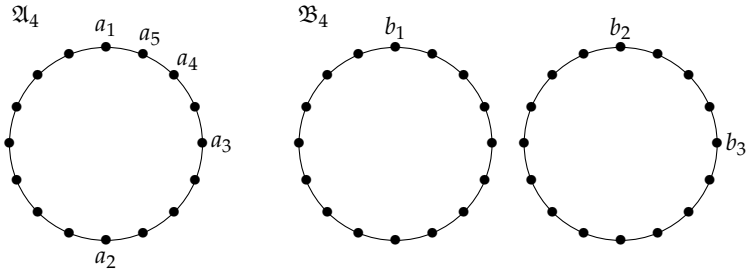


Abbildung 3.3. Eine Gewinnstrategie für den Herausforderer im Spiel $\mathcal{G}_5(\mathfrak{A}_4, \mathfrak{B}_4)$.

Wir zeigen, dass der Herausforderer die Existenz eines solchen Pfades in $\mathfrak{A}_m$ nicht in m Zügen nachweisen kann, wenn die Duplikatorin in $\mathfrak{A}_m$ zwei Knoten mit hinreichend großem Abstand wählt.

Um diese Idee zu formalisieren, definieren wir zunächst die Distanz zwischen zwei Knoten sowie einen Begriff dafür, in welchen Fällen wir Distanzen als nicht unterscheidbar betrachten.

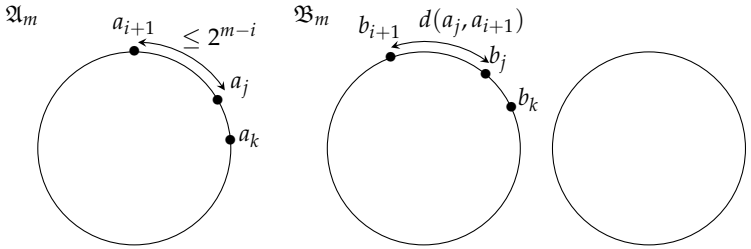
Für je zwei Knoten x, y sei die Distanz $d(x, y)$ die Länge eines kürzesten Pfades von x nach y, wenn ein solcher existiert, und $d(x, y) =$

∞, 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 $u, v \geq n$.

Behauptung. Die Duplikatorin kann so spielen, dass für alle $i \leq m$ und alle nach i Zügen ausgewählten Elemente $a_1, \ldots, a_i \in A_m$ und $b_1, \ldots, b_i \in B_m$ gilt: $d(a_j, a_k) =_{2^{m-i+1}} d(b_j, b_k)$.

Für $i = 0, 1$ ist dies trivial. Wir nehmen an, die Behauptung sei nach i Schritten erfüllt und behandeln den Induktionsschritt durch Fallunterscheidung. [4] 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 $d(a_j, a_{i+1}) < 2^{m-i}$. Dann wählt die Duplikatorin b_{i+1} so, dass $d(b_j, b_{i+1}) = d(a_j, a_{i+1})$.



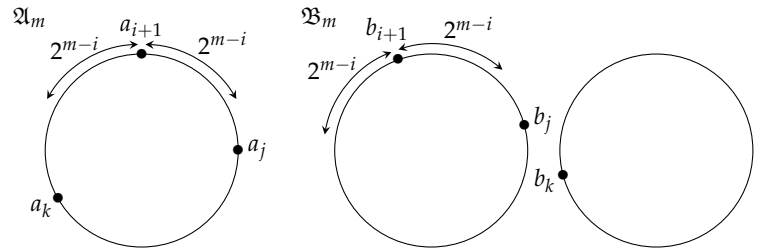
Da $d(a_j, a_k) =_{2^{m-i}} d(b_j, b_k)$, schließen wir:

- 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 $d(a_{i+1}, a_k) \geq 2^{m-i+1}$ und $d(b_{i+1}, b_k) \geq 2^{m-i+1}$, dann gilt $d(a_{i+1}, a_k) \geq 2^{m-i+1}/2 = 2^{m-i}$ und analog $d(b_{i+1}, b_k) \geq 2^{m-i}$.

Also gilt $d(a_{i+1}, a_j) = d(b_{i+1}, b_j)$ und $d(a_{i+1}, a_k) =_{2^{m-i}} d(b_{i+1}, b_k)$.

(b) Sei $d(a_{i+1}, a_j) \geq 2^{m-i}$. Die Duplikatorin wählt b_{i+1} so, dass $d(b_{i+1}, b_k) \geq 2^{m-i}$ für alle $k \leq i$.

[4] Dabei werden hier nur die wichtigsten Fälle betrachtet. Für alle weiteren Fälle verläuft der Beweis analog.



Am Ende des Spiels (nach m Zügen) gilt also $d(a_j, a_k) =_2 d(b_j, b_k)$ für alle $j, k \leq m$, d.h.:

$$a_j = a_k \text{ gdw. } b_k = b_k \text{ und}$$
$$(a_j, a_k) \in E \text{ gdw. } (b_j, b_k) \in E.$$

Also ist die Abbildung $a_1 \mapsto b_1, \ldots, a_m \mapsto b_k$ ein lokaler Isomorphismus von $\mathfrak{A}_m$ nach $\mathfrak{B}_m$, d.h. die Duplikatorin gewinnt $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$. Q.E.D.

4 Vollständigkeitssatz, Kompaktheitssatz und Unentscheidbarkeit der Prädikatenlogik

4.1 Der Sequenzenkalkül

Wie bereits in Abschnitt 1.6 für die Aussagenlogik beschrieben, können wir mit dem Sequenzenkalkül ein Verfahren angeben, das Beziehungen zwischen Formeln algorithmisch überprüft. Wir erweitern den Sequenzenkalkül nun auf die Prädikatenlogik.

Eine Schwierigkeit besteht dabei darin, Formeln mit freien Variablen zu behandeln, z.B. weil eine Variable sowohl frei als auch gebunden vorkommen kann. Durch Einführen neuer Konstantensymbole können wir uns auf die Betrachtung von Sätzen beschränken und so solche Komplikationen vermeiden. 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 $\psi(c_1, \ldots, c_n)$ ersetzen, 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 4.1. 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 *gültig*, 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 lautet:

$$(=) \quad \frac{\Gamma, t = t \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$$

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 $\mathrm{T}(\tau)$; $\psi(x)$ 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:

$$(\exists \Rightarrow) \quad \frac{\Gamma, \psi(c) \Rightarrow \Delta}{\Gamma, \exists x \psi(x) \Rightarrow \Delta}, \text{ wenn } c \text{ in } \Gamma, \Delta \text{ und } \psi \text{ nicht vorkommt.}$$

$$(\Rightarrow \exists) \quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma \Rightarrow \Delta, \exists x \psi(x)}$$

$$(\forall \Rightarrow) \quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, \forall x \psi(x) \Rightarrow \Delta}$$

$$(\Rightarrow \forall) \quad \frac{\Gamma \Rightarrow \Delta, \psi(c)}{\Gamma \Rightarrow \Delta, \forall x \psi(x)}, \text{ wenn } c \text{ in } \Gamma, \Delta \text{ und } \psi \text{ nicht vorkommt.}$$

Beispiel 4.2.

- 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:

$$\dfrac{\dfrac{\dfrac{\dfrac{Rcd \Rightarrow Rcd}{Rcd \Rightarrow \exists x Rxd}}{\forall y Rcy \Rightarrow \exists x Rxd}}{\forall y Rcy \Rightarrow \forall y \exists x Rxy}}{\exists x \forall y Rxy \Rightarrow \forall y \exists x Rxy}$$

- 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 4.1. Beweisen Sie die Korrektheit der Quantorenregeln. Zeigen Sie auch, dass in den Regeln $(\exists \Rightarrow)$ und $(\Rightarrow \forall)$ die Bedingung, dass c nicht in Γ, ψ und Δ vorkommt, nicht weggelassen werden kann.

Tabelle 4.1 fasst alle Regeln des Sequenzenkalküls nochmals zusammen. 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.

Da die Axiome des Sequenzenkalküls gültig sind, und die Schlussregeln gültige Sequenzen immer in gültige Sequenzen überführen, folgt, dass im Sequenzenkalkül nur gültige Sequenzen ableitbar sind.

Satz 4.3 (Korrektheitssatz für den Sequenzenkalkül)**.** Jede im Sequenzenkalkül ableitbare Sequenz ist gültig.

$$(=)\quad \frac{\Gamma, t = t \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$$

$$(S \Rightarrow)\quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, t \doteq t', \psi(t') \Rightarrow \Delta} \qquad (\Rightarrow S)\quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma, t \doteq t' \Rightarrow \Delta, \psi(t')}$$

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

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

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

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

$$(\exists \Rightarrow)\quad \frac{\Gamma, \psi(c) \Rightarrow \Delta}{\Gamma, \exists x \psi(x) \Rightarrow \Delta}\ {}^{*} \qquad (\Rightarrow \exists)\quad \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma \Rightarrow \Delta, \exists x \psi(x)}$$

$$(\forall \Rightarrow)\quad \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, \forall x \psi(x) \Rightarrow \Delta} \qquad (\Rightarrow \forall)\quad \frac{\Gamma \Rightarrow \Delta, \psi(c)}{\Gamma \Rightarrow \Delta, \forall x \psi(x)}\ {}^{*}$$

*wenn c in Γ, Δ und ψ nicht vorkommt

Tabelle 4.1. Die Regeln des Sequenzenkalküls

4.2 Der Vollständigkeitssatz

Die Vollständigkeit des Sequenzenkalküls ist nachgewiesen, wenn bewiesen ist, dass jede gültige Sequenz ableitbar ist.

Stattdessen können wir allerdings auch die etwas natürlichere Formulierung über die Ableitbarkeit von Sätzen oder Sequenzen aus einer Menge von Hypothesen (z.B. den Axiomen einer Theorie) betrachten. Die Frage ist dann, welche Aussagen sich aus gegebenen Voraussetzungen im Sequenzenkalkül beweisen lassen. Mit dem Vollständigkeitssatz wird bewiesen, dass das gerade die Aussagen sind, die semantisch aus den Voraussetzungen folgen.

Ableitbarkeit in Theorien. Aus dem Sequenzenkalkül erhält man den folgenden Ableitungsbegriff für Sätze oder Sequenzen aus einer Hypothesenmenge.

Definition 4.4. 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 4.5. 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*. Nach Definition ist Φ genau dann konsistent, 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, da der Sequenzenkalkül rein syntaktische Ersetzungen ausführt. 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 4.6 (Vollständigkeitssatz für den Sequenzenkalkül)**.** Für jede Satzmenge $\Phi \subseteq \mathrm{FO}(\sigma)$ und jeden Satz $\psi \in \mathrm{FO}(\sigma)$ gilt:

(i) $\Phi \models \psi$ gdw. $\Phi \vdash \psi$;

(ii) Φ ist genau dann konsistent, wenn Φ erfüllbar ist.

4.3 Der Beweis des Vollständigkeitssatzes

Man beweist den Vollständigkeitssatz, indem man für jede beliebige, nicht aus Φ ableitbare Sequenz $\Gamma \Rightarrow \Delta$ ein Modell $\mathfrak{A}$ von $\Phi \cup \Gamma \cup \neg\Delta$ konstruiert. Dabei ist $\neg\Delta := \{\neg\psi : \psi \in \Delta\}$. Daraus erhält man sofort die beiden Aussagen des Vollständigkeitssatzes:

(i) Wir wissen wegen der Korrektheit des Sequenzenkalküls bereits, dass $\Phi \models \psi$ aus $\Phi \vdash \psi$ folgt. Wir zeigen die Kontraposition der anderen Richtung. Wenn $\Phi \nvdash \psi$, dann ist insbesondere die Sequenz $\emptyset \Rightarrow \psi$ 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.

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.

Herbrandstrukturen und kanonische Modelle

Als Vorbereitung für die Modellkonstruktion behandeln wir Mengen von atomaren Sätzen. Für jede Menge von atomaren Sätzen, die unter Substitution abgeschlossen ist (d.h. alle semantisch folgenden atomaren Aussagen bereits syntaktisch enthält) konstruieren wir das sogenannte *kanonische Modell*. Dafür definieren wir zunächst den Begriff einer *Herbrandstruktur*.

Eine Herbrandstruktur besitzt genau die Elemente, die durch Terme der gegebenen Signatur definierbar sind, und damit genau die Elemente, die in jedem Modell jeder Satzmenge der Signatur existieren müssen. Später werden die Relationen gerade entsprechend der gegebenen atomaren Sätze definiert.

Lediglich Gleichheiten definierbarer Elemente werden in unserer Herbrandstruktur noch nicht erfüllt. Das kanonische Modell entsteht daher als *Faktorstruktur* durch herausfaktorisieren der Gleichheiten.

Definition 4.7. Eine *Herbrandstruktur* zu einer Signatur τ (die mindestens ein Konstantensymbol enthält) 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 $f^{\mathfrak{H}}(t_1, \ldots, t_n) := f t_1 \cdots t_n$. Die Interpretation der Relationssymbole aus τ ist beliebig.

Eine Herbrandstruktur $\mathfrak{H}$ ist eine Struktur, deren Redukt auf die Funktionssymbole gerade die Termalgebra über der leeren Variablenmenge ist, also die die Menge der Terme zusammen mit den Operationen zur syntaktischen Konstruktion von Termen. Man beachte, dass in $\mathfrak{H}$ jeder Grundterm durch sich selbst interpretiert ist: $t^{\mathfrak{H}} = t$.

Beispiel 4.8. Sei $\tau = \{c, f\}$ für ein Konstantensymbol c und ein einstelliges Funktionssymbol f. Eine Herbrandstruktur zur Signatur τ enthält dann die Elemente c, fc, ffc usw., also alle Zeichenketten $f^n c$ für $n \in \mathbb{N}$.

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

$$R^{\mathfrak{H}(\Sigma)} = \{(t_1, \ldots, t_n) : R t_1 \cdots t_n \in \Sigma\}.$$

$\mathfrak{H}(\Sigma)$ erfüllt also bereits alle Sätze der Form $R t_1 \cdots t_n$ in Σ.

Im Allgemeinen ist $\mathfrak{H}(\Sigma)$ allerdings *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 daher notwendig, Gleichheiten *herauszufaktorisieren*.

Wir konstruieren deshalb aus der Herbrandstruktur $\mathfrak{H}(\Sigma)$ eine Struktur, in der all jene Terme zusammengefasst werden, die gemäß einem Satz in Σ gleich interpretiert werden sollen. Um die Relationen und Funktionen der Herbrandstruktur zu erhalten, werden die Elemente entsprechend einer Kongruenzrelation zusammengefasst.

Definition 4.9. Sei $\mathfrak{A}$ eine τ-Struktur. Eine *Kongruenzrelation auf* $\mathfrak{A}$ ist eine Äquivalenzrelation $\sim$ auf A, welche in folgendem Sinn mit den Relationen und Funktionen von $\mathfrak{A}$ kompatibel ist:

(1) Ist $f \in \tau$ ein n-stelliges Funktionssymbol und $a_1, \dots, a_n, b_1 \dots, b_n \in A$ mit $a_1 \sim b_1, \dots, a_n \sim b_n$, so gilt:

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

(2) Ist $R \in \tau$ ein n-stelliges Relationssymbol und $a_1, \dots, a_n, b_1, \dots, b_n \in A$ mit $a_1 \sim b_1, \dots, a_n \sim b_n$, so gilt:

$$(a_1, \dots, a_n) \in R^{\mathfrak{A}} \text{ gdw. } (b_1, \dots, b_n) \in R^{\mathfrak{A}}\,.$$

Ist $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$, so bezeichnen wir mit $[a] := \{b \in A : a \sim b\}$ die *Kongruenzklasse von a unter* $\sim$.

Wir wollen in der Herbrandstruktur die Elemente jeder Kongruenzklasse zusammenfassen. Die dabei entstehende Struktur ist wie folgt definiert:

Definition 4.10. Sei $\mathfrak{A}$ eine τ-Struktur und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Die *Faktorstruktur* $\mathfrak{A}/\sim$ ist die τ-Struktur mit Universum $\{[a] : a \in A\}$ (der Menge der Kongruenzklassen von $\sim$) und der folgenden Interpretation der Relations- und Funktionssymbole.

(1) Ist $f \in \tau$ ein n-stelliges Funktionssymbol und $a_1, \dots, a_n \in A$, so gilt:

$$f^{\mathfrak{A}/\sim}([a_1], \dots, [a_n]) = [f^{\mathfrak{A}}(a_1, \dots, a_n)]\,.$$

(2) Ist $R \in \tau$ ein n-stelliges Relationssymbol und $a_1, \dots, a_n \in A$, so gilt:

$$([a_1], \dots, [a_n]) \in R^{\mathfrak{A}/\sim} \text{ gdw. } (a_1, \dots, a_n) \in R^{\mathfrak{A}}\,.$$

Man beachte, dass $f^{\mathfrak{A}/\sim}$ und $R^{\mathfrak{A}/\sim}$ wohldefiniert sind, da $\sim$ eine Kongruenzrelation ist.

Beispiel 4.11. Sei $\mathfrak{A} = (\mathbb{N}, +)$, $n \in \mathbb{N}$ und $\sim$ die Relation mit $a \sim b$ genau dann, wenn n ein Teiler von $a - b$ ist. Dann ist $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Die Faktorstruktur $\mathfrak{A}/\sim$ ist isomorph zu $(\{0, \dots, n-1\}, +_n)$, wobei $+_n$ die Addition modulo n bezeichnet.

Wir können also für jede Kongruenzrelation die Faktorstruktur bilden. In der Herbrandstruktur $\mathfrak{H}(\Sigma)$ sollen Gleichheiten herausfaktorisiert werden, also werden wir eine dafür passende Kongruenzrelation angeben. Dafür muss bekannt sein, welche Gleichheiten in der Faktorstruktur gelten sollen. Aus der Menge Σ von atomaren Sätzen folgen möglicherweise auch Gleichheiten, die nicht explizit enthalten sind. Daher erweitern wir zunächst die Menge Σ so, dass sie alle Gleichheiten enthält, die aus Σ folgen. Der Abschluss unter Substitution ist eine syntaktische Operation, die genau das gewährleistet:

Definition 4.12. Eine Menge Σ von atomaren Sätzen in $\mathrm{FO}(\tau)$ ist *abgeschlossen unter Substitution*, wenn für jede atomare Formel $\psi(x)$ und alle Grundterme $t, t' \in \mathrm{T}(\tau)$ gilt:

(i) Σ enthält die Gleichung $t = t$.
(ii) Wenn $t = t'$ und $\psi(t)$ zu Σ gehören, dann auch $\psi(t')$.

Beispiel 4.13. 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, da jeder atomare Satz, der beim Abschluss unter Substitution entsteht, bereits von $\mathfrak{A}$ erfüllt wird.

Wenn Σ unter Substitution abgeschlossen ist, können wir auf der Herbrandstruktur $\mathfrak{H}(\Sigma)$ mithilfe der enthaltenen Gleichheiten eine Kongruenzrelation bilden.

Für beliebige Grundterme $t, t' \in \mathrm{T}(\tau)$ setzen wir:

$$t \sim t' \text{ gdw. } \Sigma \text{ enthält die Formel } t = t'.$$

Wir zeigen nun, dass $\sim$ für unter Substitution abgeschlossene Satzmengen tatsächlich eine Kongruenzrelation ist, sodass wir die Faktorstruktur bilden können.

Lemma 4.14. 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 4.12 ist $\sim$ reflexiv. Sei nun $t \sim t'$ und damit $t = t' \in \Sigma$. Wenn $\psi(x)$ die Formel $x = t$ ist, dann ist $\psi(t)$ die

Gleichung $t = t$ und somit in Σ. Nach Bedingung (ii) von Definition 4.12 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 $fs_1 \cdots s_n = ft_1 \cdots t_{i-1} x s_{i+1} \cdots s_n$ 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:

$$\mathfrak{H}(\Sigma) \models Rs_1 \cdots s_n \text{ gdw. } \mathfrak{H}(\Sigma) \models Rt_1 \cdots t_n.$$

Die Argumentation ist wie bei den Funktionssymbolen, unter Verwendung der Formeln $\psi_i(x) := Rt_1 \cdots t_{i-1} x s_{i+1} \cdots s_n$. Q.E.D.

Wir können also die Faktorstruktur $\mathfrak{A}(\Sigma) := \mathfrak{H}(\Sigma)/\sim$ bilden. Offensichtlich wird in $\mathfrak{A}(\Sigma)$ jeder Grundterm t durch seine Kongruenzklasse interpretiert: $t^{\mathfrak{A}(\Sigma)} = [t]$. Somit erfüllt $\mathfrak{A}(\Sigma)$ die in Σ enthaltenen Gleichheiten. Da bereits $\mathfrak{H}(\Sigma)$ nach Definition genau die in Σ definierten relationalen Aussagen erfüllt, folgt:

Lemma 4.15. Für jeden atomaren Satz ψ aus FO(τ) gilt: $\mathfrak{A}(\Sigma) \models \psi$ gdw. $\psi \in \Sigma$.

$\mathfrak{A}(\Sigma)$ heißt das *kanonische Modell* von Σ. Leider lässt sich Lemma 4.15 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 $R^{\mathfrak{A}(\Sigma)} = \emptyset$ und somit $\mathfrak{A}(\Sigma) \not\models \exists x Rx$. 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.

Hintikka-Mengen und der Modell-Existenz-Satz

Bisher können wir das kanonische Modell für eine Menge von atomaren Sätzen konstruieren. Das Ziel ist weiterhin, für eine beliebige nicht aus Φ ableitbare Sequenz $\Gamma \Rightarrow \Delta$ ein Modell von $\Phi \cup \Gamma \cup \neg\Delta$ zu erhalten. Dazu erweitern wir diese Menge so, dass sie bestimmte Abschlusseigenschaft besitzt, die garantieren, dass das kanonische Modell der vorkommenden atomaren Sätze auch Modell der gesamten Satzmenge ist.

Genauer gesagt werden wir eine unendliche, aufsteigende Folge von nicht aus Φ ableitbaren Sequenzen $\Gamma_n \Rightarrow \Delta_n$ konstruieren. Dabei soll jede Formel aus Φ in einer Menge Γ_n enthalten sein. Betrachten wir die Vereinigung aller Γ_n bzw. Δ_n, so werden in diesen Mengen bereits alle möglichen Ableitungen im Sequenzenkalkül „simuliert“: Wann immer eine Teilformel im Antezedens (bzw. Sukzedens) der Prämisse einer anwendbaren Schlussregel vorkommt, ist sie auch in einem Γ_n (bzw. Δ_n) enthalten. So können wir später aus der Nichtableitbarkeit der Sequenzen folgern, dass ein Modell der enthaltenen atomaren Sätze (die in Blättern von Ableitungsbäumen vorkommen) auch Modell aller weiteren vorkommenden Sätze 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 nichtableitbare 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 $\psi \to \varphi$ und $\forall x \psi(x)$ ist analog.

Umgekehrt ist ein Modell von $\Gamma \cup \neg\Delta$ natürlich auch ein Modell von $\Gamma' \cup \neg\Delta'$ und erbringt damit den Nachweis, dass $\Gamma' \Rightarrow \Delta'$ nicht korrekt ist.

Bei der Konstuktion der Mengen Γ_n, Δ_n sollen allen Sätze über der gegebenen Signatur berücksichtigt werden, wobei in jedem Schritt eine neue Formel einfließt. Dazu legen wir eine Aufzählung von Formeln fest, anhand derer die jeweils nächste zu behandelnde Formel bestimmt wird.

Sei nun $\Phi \subseteq \mathrm{FO}(\sigma)$, und sei $\tau = \sigma \cup C$ für eine abzählbar unendliche Menge C von neuen Konstantensymbolen. Wir fixieren 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, sowie 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 wäre mit der Regel $(S \Rightarrow)$ auch $\Gamma_n, t = t', \psi_m(t') \Rightarrow \Delta_n$ ableitbar. 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 wäre (da c in Φ, Γ_n und Δ_n nicht vorkommt) mit der Regel $(\exists \Rightarrow)$ auch $\Gamma_n, \exists x \psi(x) \Rightarrow \Delta_n$ und damit $\Gamma_n \Rightarrow \Delta_n$ aus Φ ableitbar.
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 anderen Fällen sei $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} := \Delta_n$. Man beachte, dass aufgrund von Schritt (a) der Konstruktion $\Phi \subseteq \bigcup_{n\in\mathbb{N}} \Gamma_n$ gilt.

Wir zeigen nun, dass die Folge der $\Gamma_n \Rightarrow \Delta_n$ wie oben beschrieben die Schlussregeln des Sequenzenkalküls simuliert, und das kanonische Modell der enthaltenen atomaren Sätze definiert werden kann.

Lemma 4.16. 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 Definition 4.12).
(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 sowie 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 $\varphi_0, \varphi_1, \ldots$ 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 $\psi(t_n) \in \Delta_{n+1}$. Q.E.D.

Definition 4.17. Sei Γ^*, Δ^* ein Paar von Satzmengen welches die Eigenschaften (1) – (5) erfüllt. Dann heißt $\Gamma^* \cup \neg\Delta^*$ eine *Hintikka-Menge*.

Die Sequenzen $\Gamma_n \Rightarrow \Delta_n$ wurden als Erweiterung der nicht aus Φ ableitbaren Sequenz $\Gamma \Rightarrow \Delta$ konstruiert. Das Ziel, ein Modell von $\Phi \cup \Gamma \cup \neg\Delta$ zu konstruieren, ist also erreicht, wenn wir ein Modell der Hintikka-Menge angeben können.

Satz 4.18 (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:

- Ist $\varphi \in \Gamma^*$, so gilt $\mathfrak{A}(\Sigma) \models \varphi$;
- Ist $\varphi \in \Delta^*$, so gilt $\mathfrak{A}(\Sigma) \models \neg\varphi$.

(i) Für atomare Sätze ist dies bereits bewiesen (Lemma 4.15).
(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 für alle t $\psi(t) \in \Delta^*$ und daher per Induktionsvoraussetzung $\mathfrak{A}(\Sigma) \models \neg\psi(t)$. Da jedes Element von $\mathfrak{A}(\Sigma)$ einen Grundterm interpretiert, folgt $\mathfrak{A}(\Sigma) \models \neg\exists x\psi(x)$. Q.E.D.

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 so 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 Hintikka-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 Mathematische Logik*, 5. Auflage, Spektrum Akademischer Verlag, 2007, Kapitel 5).

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 4.19 (Absteigender Satz von 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 Verfügung 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.

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 anderen 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-Eliminationssatz*, 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.

4.4 Der Kompaktheitssatz, Axiomatisierbarkeit und Größe von Modellen

Der Vollständigkeitssatz schafft eine Brücke zwischen Syntax und Semantik 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.

Nach dem (mithilfe des Vollständigkeitssatzes) sehr einfachen Beweis werden wir einige Folgerungen des Kompaktheitssatzes betrachten. Insbesondere ergeben sich einige Techniken zum Beweis der Nicht-Axiomatisierbarkeit, die wir in diesem Abschnitt erläutern.

Satz 4.20 (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 genau dann erfüllbar, wenn jede endliche Teilmenge 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 genau dann konsistent, wenn jede endliche Teilmenge von Φ konsistent ist.

Da nach dem Vollständigkeitssatz eine Formelmenge genau dann erfüllbar ist, wenn sie konsistent ist, und die Folgerungsbeziehung $\models$ mit der

Ableitungsbeziehung $\vdash$ zusammenfällt, ergeben sich die semantischen Aussagen des Kompaktheitssatzes. Q.E.D.

In Kapitel 3.1 haben wir gesehen, dass die Klasse aller Körper mit Charakteristik p durch den Satz $\psi_{\text{Körper}} \wedge \chi_p$ endlich axiomatisiert wird, 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 4.21. Die Klasse der Körper der Charakteristik 0 ist nicht endlich axiomatisierbar.

Beweis. Sei $\psi \in \text{FO}(\tau_{\text{ar}})$ 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 somit nicht die Körper der Charakteristik 0. Q.E.D.

Weitere Überlegungen, wieder mit Hilfe des Kompaktheitssatzes, erlauben uns, Aussagen über die Existenz von unendlichen und sogar beliebig großen Modellen eines Axiomensystems zu treffen. Dazu definieren wir zunächst Begriffe, die den Vergleich von Größen von Modellen erlauben.

Definition 4.22. Seien A, B zwei Mengen. Wir sagen, dass A *mindestens so mächtig* wie B ist (kurz: $|A| \geq |B|$), wenn eine *injektive* Funktion $f : B \to A$ existiert. Weiter sagen wir, dass A und B *gleich mächtig* sind (kurz: $|A| = |B|$), wenn eine *bijektive* Funktion $f : A \to B$ existiert.

Für eine Menge A bezeichnen wir mit $\text{Pot}(A) := \{B : B \subseteq A\}$ die *Potenzmenge* von A.

Satz 4.23. Keine Menge ist gleich mächtig zu ihrer Potenzmenge.

Beweis. Wir zeigen, dass keine Funktion $f : A \to \text{Pot}(A)$ 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

$$b \in f(b) \text{ gdw. } b \in B_f \text{ gdw. } b \notin f(b)\,.$$

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

Satz 4.24 (Aufsteigender Satz von Löwenheim-Skolem)**.** Sei $\Phi \subseteq \text{FO}(\tau)$ eine Satzmenge.

(i) Φ besitze beliebig große endliche Modelle (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.

(ii) 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. (i) Sei $\Theta := \Phi \cup \{\varphi_{\geq n} : n \in \mathbb{N}\}$, wobei

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

Die Modelle von Θ sind 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 $\Theta_0 \subseteq \Theta$ gibt es aber ein $n_0 \in \mathbb{N}$, so dass $\Theta_0 \subseteq \Phi \cup \{\varphi_{\geq n} : n < n_0\}$. Da nach Voraussetzung Φ beliebig große endliche Modelle hat, ist Θ_0 erfüllbar.

(ii) 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 unendliches Modell $\mathfrak{B} \models \Phi$. 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 $\mathfrak{D} \models \Phi$.

Q.E.D.

Folgerung 4.25. Die Klasse aller endlichen τ-Strukturen ist nicht FO-axiomatisierbar.

Ebenso folgt, dass die Klasse aller endlichen Gruppen, die Klasse aller endlichen Körper, die Klassen aller endlichen Graphen etc. nicht FO-axiomatisierbar sind.

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 die gleiche Theorie haben.

Lemma 4.26. $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\}$ 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 somit 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 $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\} \subseteq \mathrm{Mod}(\Phi)$. Q.E.D.

Nach dem Isomorphielemma sind isomorphe Strukturen auch elementar äquivalent. Die Umkehrung gilt für unendliche Strukturen im Allgemeinen nicht.

Satz 4.27. 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 $\mathrm{Pot}(A)$ von A hat. Nach Satz 4.23 ist $\mathfrak{B}$ nicht gleich mächtig 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. Q.E.D.

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 τ_{ar}-Struktur, die zu $\mathfrak{N}$ zwar elementar äquivalent aber nicht isomorph ist.

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 4.28 (Skolem)**.** Es gibt ein abzählbares Nichtstandardmodell der Arithmetik.

Beweis. Sei $\Phi := \mathrm{Th}(\mathfrak{N}) \cup \{c \neq \underline{n} : n \in \mathbb{N}\}$, wobei c ein neues Konstantensymbol ist, $\underline{0} := 0$ und $\underline{n} := \underbrace{1 + \cdots + 1}_{n\text{-mal}}$ 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 $\mathfrak{C} = \mathfrak{B} \restriction \tau_{\text{ar}}$ (das durch Weglassen von $c^{\mathfrak{B}}$ definierte Redukt von $\mathfrak{B}$). Da $\mathfrak{B} \models \text{Th}(\mathfrak{N})$, ist $\mathfrak{N} \equiv \mathfrak{C}$.

Es bleibt zu zeigen, dass kein Isomorphismus $\pi : \mathfrak{N} \to \mathfrak{C}$ existiert. Für jeden solchen Isomorphismus π müsste gelten, dass $\pi(n) = \pi(\underline{n}^{\mathfrak{N}}) = \underline{n}^{\mathfrak{B}}$ für alle $n \in \mathbb{N}$ gilt. Da π surjektiv ist, gibt es ein $k \in \mathbb{N}$, so dass $c^{\mathfrak{B}} = \pi(k) = \underline{k}^{\mathfrak{B}}$. Damit erhalten wir einen Widerspruch: Einerseits gilt $\mathfrak{B} \models c = \underline{k}$, aber andererseits, da die Formel $c \neq \underline{k}$ in Φ enthalten ist, auch $\mathfrak{B} \models c \neq \underline{k}$. Q.E.D.

Übung 4.2. 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 $\text{Th}(\mathfrak{N}, <)$ 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 4.3. Zeigen Sie, dass es überabzählbar viele paarweise nichtisomorphe abzählbare Modelle der Arithmetik gibt.

Hinweis: Sei $\varphi(x, y) := \exists z(x \cdot z = y)$. Die Primteiler eines Elements a eines Nichtstandardmodells $\mathfrak{A}$ der Arithmetik seien die Primzahlen $p \in \mathbb{N}$, so dass $\mathfrak{A} \models \varphi[\underline{p}, a]$. 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 Kompaktheitssatz 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 $\mathcal{O}_\psi := \{T \in S : \psi \in T\}$ 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 $S \setminus \mathcal{O}_\psi = \{T \in S : \psi \notin T\} = \{T \in S : \neg\psi \in T\} = \mathcal{O}_{\neg\psi}$.

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 $\mathcal{O}_\psi \cap \mathcal{O}_{\neg\psi} = \emptyset$.

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 $\Phi \subseteq \text{FO}(\tau)$).

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 $\Phi \subseteq \text{FO}(\tau)$). Also ist $\emptyset = S \setminus \bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi = \bigcap_{\varphi \in \Phi} \mathcal{O}_{\neg\varphi}$.

Daher lässt sich die Satzmenge $\{\neg\varphi : \varphi \in \Phi\}$ nicht zu einer vollständigen Theorie erweitern und ist somit unerfüllbar. Nach dem Kompaktheitssatz ist bereits $\{\neg\varphi : \varphi \in \Phi_0\}$ für ein endliches $\Phi_0 \in \Phi$ unerfüllbar. Folglich ist $S = S \setminus \bigcap_{\varphi \in \Phi_0} \mathcal{O}_{\neg\varphi} = \bigcup_{\varphi \in \Phi_0} \mathcal{O}_\varphi$.

4.5 Unentscheidbarkeit der Prädikatenlogik

Das klassische Entscheidungsproblem 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 genau dann erfüllbar, wenn $\neg\psi$ nicht allgemeingültig ist, und nach dem Vollständigkeitssatz ist eine Formel genau dann allgemeingültig, wenn sie ableitbar ist.

Das klassische Entscheidungsproblem wurde zu Beginn des 20ten Jahrhunderts 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 4.4. 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 $m \cdot 2^q$ Elementen besitzt.

Übung 4.5. Zeigen sie, dass das Erfüllbarkeitsproblem für Formeln der Gestalt $\exists x_1 \ldots \exists x_r \forall y_1 \ldots \forall y_s \varphi$ entscheidbar ist, wobei φ quantorenfrei und relational sein soll.

Hinweis: Zeigen Sie, dass jeder erfüllbare Satz dieser Gestalt ein Modell mit höchstens r Elementen besitzt.

Übung 4.6. Zeigen Sie, dass das Erfüllbarkeitsproblem für existentielle Formeln (mit beliebiger Signatur) entscheidbar ist.

1936/37 haben Church und Turing unabhängig voneinander bewiesen, dass das Entscheidungsproblem nicht algorithmisch lösbar ist. Im Gegensatz zur Aussagenlogik ist das Erfüllbarkeitsproblem für die Prädikatenlogik also unentscheidbar.

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). Unter dem PCP versteht man das folgende Entscheidungsproblem.

Gegeben: Eine Folge $F = (u_1, v_1), \ldots, (u_k, v_k)$ von Wortpaaren mit $u_i, v_i \in \{0,1\}^*$.

Frage: Gibt es eine Indexfolge $i_1, \ldots, i_l$ so dass $u_{i_1} \cdots u_{i_l} = v_{i_1} \cdots v_{i_l}$? (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 4.29 (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 genau dann eine Lösung zulässt, 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 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 4.30 (Church, Turing)**.** Das Gültigkeitsproblem (und damit auch das Erfüllbarkeitsproblem) der Prädikatenlogik ist unentscheidbar.

Beweis. Wir zeigen, dass man zu jeder Eingabe $F = (u_1, v_1), \ldots, (u_k, v_k)$ für das PCP effektiv einen FO-Satz ψ_F konstruieren kann, so dass gilt:

ψ_F ist allgemeingültig gdw. es gibt eine Lösung für F.

Die Signatur τ von ψ_F besteht aus einem Konstantensymbol c, einstelligen Funktionssymbolen f_0 und f_1 und einem zweistelligen Relationssymbol P.

In jeder τ-Struktur interpretieren wir c als das leere Wort ε, und $f_0 w$ (bzw. $f_1 w$) als das Wort, das durch Anhängen von 0 bzw. 1 am Wortanfang entsteht (also $0w$ bzw. $1w$). So kann 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 werden. Dabei ist garantiert, dass jede τ-Struktur für jedes endliche Wort über $\{0,1\}$ ein Element enthält (im Allgemeinen sind diese Elemente natürlich nicht zwingend verschieden). Um, im Fall dass ψ_F allgemeingültig ist, eine Lösung der PCP-Instanz zu konstruieren, werden wir allerdings eine Struktur verwenden, deren Elemente *genau* die endlichen $\{0,1\}$-Wörter sind.

P soll entsprechend dieser Zuordnung alle Paare von Wörtern (u, v) enthalten, die mit den Paaren (u_i, v_i) gebildet werden können.

Die Formel

$$\varphi := \bigwedge_{i=1}^{k} P(t_{u_i} c, t_{v_i} c)$$

sagt somit aus, dass jedes vorgegebene Wortpaar (u_i, v_i) gebildet werden kann.

Die Bedingung folgt dann mit

$$\vartheta := \forall x \forall y (Pxy \to \bigwedge_{i=1}^{k} P(t_{u_i} x, t_{v_i} y)),$$

denn ϑ bedeutet, dass, wenn ein Wortpaar (x, y) aus den (u_j, v_j) gebildet werden kann, dann auch das Paar $(u_i x, v_i y)$, das durch Anhängen an (u_i, v_i) entsteht.

Die PCP-Instanz besitzt in dieser Darstellung eine Lösung, genau dann, wenn auf diese Art auch ein Wortpaar (x, x) gebildet werden kann. Die Lösbarkeitsbedingung wird dann durch die Formel

$$\psi_F := (\varphi \wedge \vartheta) \to \exists x Pxx$$

ausgedrückt.

Nehmen wir zunächt an ψ_F sei gültig. Dann gilt ψ_F in jeder zu der Formel passenden Struktur, insbesondere also in $\mathfrak{A} = (A, c, f_0, f_1, P)$ mit

$$\begin{aligned}
A &:= \{0,1\}^*, \\
c &:= \varepsilon \text{ (das leere Wort)}, \\
f_0(w) &:= 0w \text{ für alle } w \in \{0,1\}^*, \\
f_1(w) &:= 1w \text{ für alle } w \in \{0,1\}^* \text{ und} \\
P &:= \{(u, v) : \text{ es gibt } i_1, \ldots, i_l \text{ mit} \\
&\qquad\qquad u = u_{i_1} \cdots u_{i_l} \text{ und } v = v_{i_1} \cdots v_{i_l}\}.
\end{aligned}$$

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 $i_1, \ldots, i_l$ mit $z = u_{i_1} \cdots u_{i_l} = v_{i_1} \cdots v_{i_l}$, d.h. $i_1, \ldots, i_l$ ist eine Lösung für F.

Nehmen wir nun umgekehrt an, dass F eine Lösung $i_1, \ldots, i_l$ 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 $h(\varepsilon) = c$, $h(0w) = f_0(h(w))$ und $h(1w) = f_1(h(w))$.

Da $\mathfrak{A} \models \varphi$, gilt $(h(u_i), h(v_i)) \in P$ für $i = 1, \ldots, k$. Wegen $\mathfrak{A} \models \vartheta$ gilt für $i = 1, \ldots, k$, dass aus $(x, y) \in P$ auch $(h(u_i x), h(v_i y)) \in P$ folgt. Per Induktion schließen wir, dass $(h(u_{i_1} \cdots u_{i_l}), h(v_{i_1} \cdots v_{i_l})) \in P$ gilt, d.h. für die Lösung $w = u_{i_1} \cdots u_{i_l} = v_{i_1} \cdots v_{i_l}$ folgt $(h(w), h(w)) \in P$. Damit ist gezeigt, dass $\mathfrak{A} \models \exists x P x x$ und somit $\mathfrak{A} \models \psi_F$. Q.E.D.

5 Modallogik, temporale Logiken und monadische Logik

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.

5.1 Syntax und Semantik der Modallogik

Modallogiken formalisieren Aussagen über Transitionssysteme von einer internen, lokalen Perspektive her. 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 alle a aus einer Menge von *Aktionen*.

Definition 5.1. 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 $(\psi \to \varphi)$.
- Wenn $\psi \in$ ML und $a \in A$, dann gehören auch $\langle a \rangle \psi$ und $[a]\psi$ zu ML.

Notation. 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 5.2. 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 5.3. 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) $\mathcal{K}, v \models P_i$ gdw. $v \in P_i$.
(2) Die Bedeutungen von $\neg\psi$, $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $(\psi \to \varphi)$ 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) $\mathcal{K}, v \models [a]\psi$, 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 5.3 gegeben Regeln äquivalent sind):

(1) $[\![P_i]\!]^{\mathcal{K}} = P_i$.
(2) $[\![\neg\psi]\!]^{\mathcal{K}} := V \setminus [\![\psi]\!]^{\mathcal{K}}$
$[\![\psi \wedge \varphi]\!]^{\mathcal{K}} := [\![\psi]\!]^{\mathcal{K}} \cap [\![\varphi]\!]^{\mathcal{K}}$
$[\![\psi \vee \varphi]\!]^{\mathcal{K}} := [\![\psi]\!]^{\mathcal{K}} \cup [\![\varphi]\!]^{\mathcal{K}}$
$[\![\psi \to \varphi]\!]^{\mathcal{K}} := (V \setminus [\![\psi]\!]^{\mathcal{K}}) \cup [\![\varphi]\!]^{\mathcal{K}}$.
(3) $[\![\langle a\rangle\psi]\!]^{\mathcal{K}} := \{v : vE_a \cap [\![\psi]\!]^{\mathcal{K}} \neq \emptyset\}$.
(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 5.4. FO^2, das *Zwei-Variablen-Fragment* von FO, ist die Menge aller relationalen FO-Formeln, welche nur zwei Variablen x und y enthalten.

Beispiel 5.5. Wir wollen ausdrücken, dass es (in einem gegebenen Transitionssystem) 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

$$\psi(x) := \exists y_1 \cdots \exists y_5 (E_a x y_1 \wedge \bigwedge_{i=1}^{4} E_a y_i y_{i+1} \wedge P y_5),$$

welche sechs Variablen verwendet. 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 5.6. Zu jeder Formel $\psi \in \mathrm{ML}$ gibt es eine Formel $\psi^*(x)$ in FO^2, so dass für alle Transitionssysteme $\mathcal{K}$ und alle Zustände v von $\mathcal{K}$ gilt:

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

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

$$\begin{aligned}
P_i &\mapsto P_i x \\
\neg\psi &\mapsto \neg\psi^*(x) \\
(\psi \circ \varphi) &\mapsto (\psi^*(x) \circ \varphi^*(x)) \text{ für } \circ \in \{\wedge, \vee, \rightarrow\} \\
\langle a\rangle\psi &\mapsto \exists y(E_a xy \wedge \psi^*(y)) \\
[a]\psi &\mapsto \forall y(E_a xy \rightarrow \psi^*(y))
\end{aligned}$$

Q.E.D.

Erfüllbarkeit, Gültigkeit, Äquivalenz. Analog zu Aussagenlogik und Prädikatenlogik definieren wir: Eine Formel $\psi \in \mathrm{ML}$ 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 5.7. Für alle Formeln $\psi \in \mathrm{ML}$ 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 $\psi \in \mathrm{ML}$ 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 5.1. Gilt für ML das Analogon des Satzes über die Pränex-Normalform?

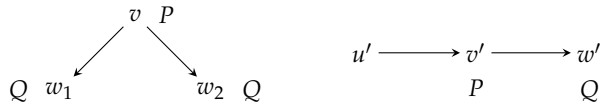
5.2 Bisimulation

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

(1) $v \in P_i$ gdw. $v' \in P'_i$ 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 5.9. $Z = \{(v, v'), (w_1, w'), (w_2, w')\}$ ist eine Bisimulation zwischen den beiden folgenden Transitionssystemen:



Definition 5.10. 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: $v \in P_i$ gdw. $v' \in P_i'$ 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 5.11. II gewinnt genau dann das Bisimulationsspiel auf $\mathcal{K}, \mathcal{K}'$ von (u, u'), wenn $\mathcal{K}, u \sim \mathcal{K}', u'$.

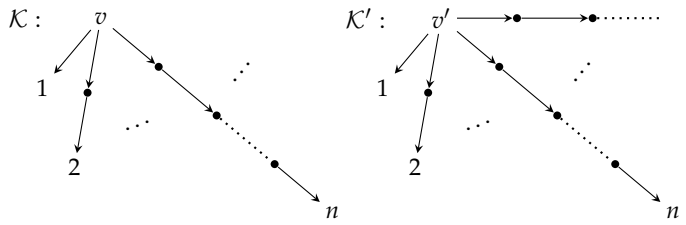
Wir können die Analyse noch etwas verfeinern, wenn wir die Anzahl der Züge in einem Bisimulationsspiel in Betracht ziehen. Wir sagen, II gewinnt das n-Züge-Bisimulationsspiel, wenn sie eine Strategie hat, um n Züge lang zu spielen ohne zu verlieren. Analog dazu betrachten wir den Begriff der *n-Bisimilarität*,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

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

Es gilt für alle $n \in \mathbb{N}$, dass II genau dann das n-Züge-Bisimulationsspiel von (v, v') aus gewinnt, wenn $\mathcal{K}, v \sim_n \mathcal{K}', v'$ gilt.

Satz 5.12. 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 $\mathcal{K}, v \nsim \mathcal{K}', v'$. 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. Q.E.D.

Bisimulationsinvarianz von modallogischen Formeln. Die grundlegende Bedeutung von Bisimulationen besteht darin, 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 5.13. Die *Modaltiefe* einer Formel $\psi \in \mathrm{ML}$ ist induktiv definiert durch:

(1) $\mathrm{md}(\psi) = 0$ für aussagenlogische Formeln ψ,
(2) $\mathrm{md}(\neg\psi) = \mathrm{md}(\psi)$,
(3) $\mathrm{md}(\psi \circ \varphi) = \max(\mathrm{md}(\psi), \mathrm{md}(\varphi))$ für $\circ \in \{\wedge, \vee, \to\}$,
(4) $\mathrm{md}(\langle a\rangle\psi) = \mathrm{md}([a]\psi) = \mathrm{md}(\psi) + 1$.

Definition 5.14. 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 $\psi \in$ ML gilt:
$\mathcal{K}, v \models \psi$ gdw. $\mathcal{K}', v' \models \psi$.
(2) $\mathcal{K}, v \equiv^n_{\mathrm{ML}} \mathcal{K}', v'$, wenn für alle $\psi \in$ ML mit $\mathrm{md}(\psi) \leq n$ gilt:
$\mathcal{K}, v \models \psi$ gdw. $\mathcal{K}', v' \models \psi$.

Satz 5.15. Für Kripkestrukturen $\mathcal{K}$, $\mathcal{K}'$ und $u \in \mathcal{K}$, $u' \in \mathcal{K}'$ gilt:

(1) Aus $\mathcal{K}, u \sim \mathcal{K}', u'$ folgt $\mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'$;
(2) Aus $\mathcal{K}, u \sim_n \mathcal{K}', u'$ folgt $\mathcal{K}, u \equiv^n_{\mathrm{ML}} \mathcal{K}', u'$.

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 $\psi \in$ ML gilt:

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

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. Q.E.D.

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

Wenn $\mathcal{K}, v \models \psi$ und $\mathcal{K}, v \sim \mathcal{K}', v'$, 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 Beweis von Satz 5.12. 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 5.16. 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 5.17. Seien $\mathcal{K}, \mathcal{K}'$ endlich verzweigte Transitionssysteme. Dann gilt $\mathcal{K}, u \sim \mathcal{K}', u'$ genau dann, wenn $\mathcal{K}, u \equiv_{\mathrm{ML}} \mathcal{K}', u'$ gilt.

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 $v \in P_i$ gdw. $v' \in P'_i$, 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

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

  Es reicht zu zeigen, dass ein $w' \in v'E_a \setminus X_w$ existiert, denn dann ist $(w, w') \in Z$ und die Hin-Eigenschaft erfüllt. Dazu wählen wir für jedes $z' \in X_w$ eine Formel $\varphi_{z'} \in$ 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 $\varphi \in$ 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 verläuft analog mit vertauschten Rollen von $\mathcal{K}, v$ und $\mathcal{K}', v'$. Q.E.D.

5.3 Abwicklungen und Baummodell-Eigenschaft

Eine Menge von Formeln (irgendeiner Logik, etwa der Modallogik oder der Prädikatenlogik), welche auf Transitionssystemen interpretiert wird, hat die *Baummodell-Eigenschaft* (BME), wenn jede erfüllbare Formel in Φ ein Modell hat, welches ein Baum ist.

Definition 5.18. 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) $E_a \cap E_b = \emptyset$ für alle Aktionen $a \neq b$,
(2) für $E = \bigcup_{a\in A} E_a$ der Graph (V, E) ein (gerichteter) Baum mit Wurzel w im Sinn der Graphentheorie ist (siehe auch Kapitel 1.4).

Wir werden zeigen, dass die Modallogik die Baumodell-Eigenschaft besitzt. 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 5.19. 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

$$
\begin{aligned}
V^{\mathcal{T}} &= \{\bar{v} = v_0 a_0 v_1 a_1 v_2 \dots v_{m-1} a_{m-1} v_m : m \in \mathbb{N},\\
&\qquad v_0 = v,\ v_i \in V^{\mathcal{K}},\ a_i \in A,\ (v_i, v_{i+1}) \in E_{a_i}^{\mathcal{K}} \text{ für alle } i < m\},\\
E_a^{\mathcal{T}} &= \{(\bar{v}, \bar{w}) \in V^{\mathcal{T}} \times V^{\mathcal{T}} : \bar{w} = \bar{v}aw \text{ für ein } w \in V^{\mathcal{K}}\} \text{ und}\\
P_i^{\mathcal{T}} &= \{\bar{v} = v_0 a_0 \dots v_m \in V^{\mathcal{T}} : v_m \in P_i^{\mathcal{K}}\}
\end{aligned}
$$

Mit $\mathrm{End}(\bar{v})$ bezeichnen wir den letzten Knoten auf dem Pfad $\bar{v}$. Damit ist $\bar{v} \in P_i^{\mathcal{T}}$ gdw. $\mathrm{End}(\bar{v}) \in P_i^{\mathcal{K}}$.

Lemma 5.20. Es gilt $\mathcal{K}, v \sim \mathcal{T}_{K,v}, v$.

Beweis. $Z := \{(w, \bar{w}) \in V^{\mathcal{K}} \times V^{\mathcal{T}} : \mathrm{End}(\bar{w}) = w\}$ ist eine Bisimulation von $\mathcal{K}$ nach $\mathcal{T}_{\mathcal{K},v}$ mit $(v, v) \in Z$. Q.E.D.

Satz 5.21. 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. Q.E.D.

Dasselbe Argument zeigt, dass *jede* Klasse von bisimulationsinvarianten Formeln die Baummodell-Eigenschaft besitzt.

5.4 Temporale Logiken

ML ist keine besonders ausdrucksstarke Logik. Eine wesentliche Schwäche ist, dass der Wahrheitswert einer an einem Zustand v ausgewerteten Formel nur von einer beschränkten Umgebung von v abhängen kann. Zu den wichtigsten Aussagen in einer Reihe von Anwendungen (insbesondere in der Verifikation) gehören *Erreichbarkeitsaussagen* (ein „guter" Zustand wird auf jeden Fall irgendwann erreicht) oder *Sicherheitsbedingungen* (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 Transitionssystem „hineinsehen" kann. Wie wir gesehen haben, sind Erreichbarkeitsaussagen in Transitionssystemen auch in FO nicht formalisierbar.

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 die temporalen Logiken LTL („linear time temporal logic“) und CTL („computation tree logic“ oder auch „branching time temporal logic“), welche die Modallogik ML erweitern und in der (Hardware-)Verifikation sehr populär sind.

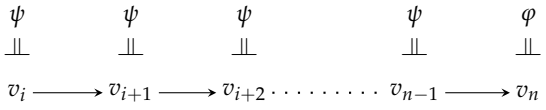
Syntax und Semantik von LTL

Die temporale Logik LTL wird auf endlichen oder unendlichen Wörtern oder Pfaden ausgewertet, also auf Folgen $v_0 v_1 \dots v_{n-1}$ bzw. $v_0 v_1 \dots$ mit atomaren Aussagen P_i. Die Idee von LTL ist, aussagenlogische Formeln über den atomaren Aussagen P_i durch temporale Operatoren (wie „next“, „until“, „eventually“ und „globally“) zu erweitern.

Definition 5.22 (Syntax von LTL)**.** Die Formeln von LTL sind induktiv wie folgt definiert:

- Alle aussagenlogischen Formeln über $\{P_i : i \in I\}$ gehören zu LTL.
- LTL ist abgeschlossen unter den Booleschen Operatoren $\wedge$, $\vee$, $\to$ und $\neg$.
- Wenn ψ, $\varphi \in$ LTL, dann sind auch die Ausdrücke $\mathrm{X}\psi$ und $(\psi \,\mathrm{U}\, \varphi)$ Formeln von LTL.

Die Intuition bei der Modellbeziehung ist folgende: Wie die Modallogik ML wird auch LTL an einzelnen Punkten ausgewertet. Ob eine Formel ψ an einem Punkt v_i gilt, kurz $\mathcal{W}, v_i \models \psi$, hängt von dem Teilwort $v_i v_{i+1} \dots$ ab, welches bei v_i beginnt. Der Ausdruck $\mathrm{X}\psi$ („next ψ“) bedeutet, dass am unmittelbar folgenden Element v_{i+1} die Formel ψ gilt, und der Ausdruck $\psi \,\mathrm{U}\, \varphi$ („ψ until φ“) besagt, dass an irgendeinem „späteren“ Element v_n φ gilt und davor immer ψ wahr ist:



Definition 5.23 (Semantik von LTL)**.** Sei $\mathcal{W}$ eine endliche oder unendliche Folge von Elementen $v_0 \dots v_{n-1}$ oder $v_0 v_1 \dots$ und atomaren

Relationen P_i für $i \in I$. Die Bedeutung der Formeln P_i und der aussagenlogischen Junktoren ist auf die übliche Weise definiert. Außerdem gilt:

- $\mathcal{W}, v_i \models \mathrm{X}\psi$ genau dann, wenn v_i nicht das letzte Element von $\mathcal{W}$ ist und $\mathcal{W}, v_{i+1} \models \psi$;
- $\mathcal{W}, v_i \models (\psi \,\mathrm{U}\, \varphi)$, wenn ein $n \geq i$ existiert, so dass $\mathcal{W}, v_n \models \varphi$ und $\mathcal{W}, v_m \models \psi$ für alle m mit $i \leq m < n$.

Notation. Zwei wichtige Abkürzungen sind:

$$\mathrm{F}\psi := (1 \,\mathrm{U}\, \psi) \qquad \text{(irgendwann wird } \psi \text{ gelten)}$$
$$\mathrm{G}\psi := \neg\mathrm{F}\neg\psi \qquad \text{(immer wird } \psi \text{ gelten)}$$

Beispiel 5.24.

- In LTL kann man ausdrücken, dass in einem unendlichen Wort $\mathcal{W}$ eine Formel φ an unendlichen vielen Positionen gilt. In der Tat besagt $\mathrm{GF}\varphi$, dass für jedes i ein $j \geq i$ existiert, so dass $\mathcal{W}, v_j \models \varphi$, und dies ist genau dann der Fall, wenn φ an unendlich vielen Positionen v_j gilt.
- Entsprechend gilt die Formel $\mathrm{FG}\neg\varphi$ ausgewertet über einem unendlichen Wort $\mathcal{W}$ genau dann, wenn φ nur an endlich vielen Positionen gilt.
- Die Formel $\mathrm{G}(\varphi \to (\varphi \,\mathrm{U}\, \psi))$ besagt, dass zu jeder Position an der φ gilt eine spätere Position existiert an der ψ gilt, und dass zwischen beiden Positionen immer φ gilt.

Wir haben gesehen, dass die Modallogik ML in die Prädikatenlogik FO eingebettet werden kann. Gilt dies auch für LTL? Dies hängt davon ab, wie wir Wörter bzw. Pfade als Strukturen formalisieren; anders ausgedrückt, ob wir FO-Formeln betrachten, welche die Ordnungsrelation auf den Elementen benutzen, oder ob nur die Nachfolgerrelation zur Verfügung steht. Stellen wir (endliche oder unendliche) Wörter als Strukturen der Form

$$\mathcal{W} = (V, <, (P_i)_{i \in I})$$

mit Universum $V = \omega$ (die Menge der natürlichen Zahlen) oder $V = \{0, \dots, n-1\}$ sowie der üblichen linearen Ordnung $<$ auf V und mit einstelligen Relationen $P_i \subseteq V$ dar, so lässt sich LTL in FO einbetten.

Satz 5.25. Zu jeder LTL-Formel ψ existiert eine FO-Formel $\psi^*(x)$ der Signatur $\{<\} \cup \{P_i : i \in I\}$, so dass für alle $\mathcal{W}, v$ gilt:

$$\mathcal{W}, v \models \psi \quad \text{gdw.} \quad \mathcal{W} \models \psi^*(v).$$

Beweis. Der Beweis ist analog zum Beweis der Einbettung von ML in FO, mit folgenden Änderungen: Formeln der Form $\psi = X\varphi$ werden übersetzt in

$$\psi^*(x) := \exists y(x < y \wedge \neg\exists z(x < z \wedge z < y) \wedge \varphi^*(y)),$$

und Formeln der Form $\psi = (\varphi \,\mathrm{U}\, \vartheta)$ werden übersetzt in

$$\psi^*(x) := \exists y(x < y \wedge \vartheta^*(y) \wedge \forall z((x \leq z \wedge z < y) \to \varphi^*(z))).$$

Q.E.D.

Wenn aber auf dem Universum V statt der Ordnungsrelation $<$ nur die Nachfolgerrelation $E = \{(v_i, v_j) \in V \times V : j = i + 1\}$ zur Verfügung steht, dann kann man mit FO-Formeln nicht alle LTL-Eigenschaften ausdrücken. Mit Hilfe von Ehrenfeucht-Fraïssé-Spielen kann man beweisen, dass bereits Formeln der Form GFP keine äquivalente FO-Formel ohne Ordnungsrelation zulassen.

Temporale Logiken auf Transitionssystemen. In vielen Anwendungen werden LTL (und andere temporale Logiken) zur Verifikation von Eigenschaften von Transitionssystemen verwendet. Wir betrachten dabei Transitionssysteme mit nur einer Transitionsrelation, d.h. Strukturen der Form $\mathcal{K} = (V, E, (P_i)_{i\in I})$ und setzen der Einfachheit halber voraus, dass E nicht terminiert, d.h. zu jedem $u \in V$ existiert ein v, so dass $(u, v) \in E$. Für eine LTL-Formel ψ sagen wir, dass ψ am Zustand v von $\mathcal{K}$ gilt, kurz $\mathcal{K}, v \models \psi$, wenn ψ auf *allen* unendlichen Pfaden durch $\mathcal{K}$, welche bei v beginnen, gilt.

Syntax und Semantik von CTL

Eine andere Möglichkeit, Aussagen über das mögliche Verhalten eines Transitionssystem zu machen, führt auf die „branching time logic“ CTL. Die Idee von CTL ist, ML um Pfadquantoren und temporale Operatoren auf Pfaden zu erweitern.

Definition 5.26 (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 Booleschen Operatoren $\wedge$, $\vee$, $\to$ und $\neg$.
- Wenn $\psi, \varphi \in$ CTL, dann sind auch die Ausdrücke EXψ, AXψ, E$(\psi \,\mathrm{U}\, \varphi)$ und A$(\psi \,\mathrm{U}\, \varphi)$ Formeln von CTL.

Die Intuition bei der Modellbeziehung ist folgende: Sei $\mathcal{K}$ ein Transitionssystem und v ein Zustand von $\mathcal{K}$. Dann quantifizieren E und A über unendliche Pfade $v = v_0v_1v_2\dots$ in $\mathcal{K}$, welche bei v beginnen und auf denen die temporalen Operatoren dann ausgewertet werden.

Definition 5.27 (Semantik von CTL)**.** Sei $\mathcal{K} = (V, E, (P_i)_{i\in I})$ eine Kripkestruktur und $v \in V$. Dann gilt:

- EX$\psi :\equiv \Diamond\psi$;
- AX$\psi :\equiv \Box\psi$;
- Es gilt $\mathcal{K}, v \models$ E$(\psi \,\mathrm{U}\, \varphi)$, wenn ein Pfad $v_0v_1v_2\dots$ mit $v = v_0$ 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 gilt $\mathcal{K}, v \models$ A$(\psi \,\mathrm{U}\, \varphi)$, wenn für alle unendlichen Pfade $v_0v_1v_2\dots$ mit $v_0 = v$ ein $n \geq 0$ existiert, so dass $\mathcal{K}, v_n \models \varphi$ und $\mathcal{K}, v_m \models \psi$ für alle m mit $0 \leq m < n$.

Analog zu LTL definieren wir die folgenden abkürzenden Schreibweisen:

EF$\psi :\equiv$ E$(1 \,\mathrm{U}\, \psi)$	(ex. ein Pfad, auf dem irgendwann ψ gilt)
AF$\psi :\equiv$ A$(1 \,\mathrm{U}\, \psi)$	(auf allen Pfaden gilt irgendwann ψ)
EG$\psi :\equiv \neg$AF$\neg\psi$	(ex. ein Pfad, auf dem immer ψ gilt)

$\mathrm{AG}\psi :\equiv \neg\mathrm{EF}\neg\psi$ (auf allen Pfaden gilt immer ψ)

Beispiel 5.28.

- In CTL ist Erreichbarkeit definierbar: $\mathrm{EF}\psi$ bedeutet, dass ein Zustand erreicht werden kann, an dem ψ gilt.
- $\mathrm{AG}\neg(P \wedge Q)$ drückt aus, dass sich P und Q in allen erreichbaren Zuständen ausschließen.
- $\mathrm{AGAF}\psi$ 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 5.2. 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 bezüglich der Länge der Formel wie der Größe des Transitionssystems).

Satz 5.29. 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.

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 (da z.B. Erreichbarkeit nicht FO-definierbar ist).

5.5 Monadische Logik

Eine wichtige 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

$$\forall X((Xs \wedge \forall y \forall z(Xy \wedge Eyz \to Xz)) \to Xt)$$

aus, dass im Graphen (V, E) ein Pfad von s nach t existiert.

Übung 5.3. Zeigen Sie, dass jede CTL-Formel in eine äquivalente Formel in MSO übersetzt werden kann.

> 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*

Symbole

AL Menge aller aussagenlogischen Formeln. 4

$\neg$ Negation (logischer Junktor), „nicht“. 4, 53

$\vee$ Disjunktion (logischer Junktor), „oder“. 4, 53

$\wedge$ Konjunktion (logischer Junktor), „und“. 4, 53

$\rightarrow$ Implikation (logischer Junktor). 4, 53

$\tau(\psi)$ Menge der in der aussagenlogischen Formel ψ vorkommenden Aussagenvariablen. 6

$[\![\psi]\!]^{\mathfrak{I}}$ Wahrheitswert der Formel ψ (in AL bzw. FO) unter der Interpretation $\mathfrak{I}$ (Semantik von ψ). 6, 52

$\models$ (1) Modellbeziehung. Relation zwischen einer Interpretation und einer Formel oder Formelmenge
(2) Semantische Folgerungsbeziehung. Relation zwischen einer Formelmenge und einer Formel
7, 18, 53, 55

$\equiv$ (1) logische Äquivalenz von Formeln
(2) elementare Äquivalenz von Strukturen
8, 55, 82, 124

$\overline{Y}$ Komplement des Literals Y. 11

$\Rightarrow$ Sequenzpfeil. 31, 93

$\vdash$ Ableitbarkeit aus einer Hypothesenmenge im Sequenzenkalkül. 33, 97

$|\ f|A$ ist die Restriktion der Funktion f auf die Menge A. 42

$\mathfrak{B} \restriction \sigma$ Redukt der Struktur $\mathfrak{B}$ auf die Signatur σ. 42

$\mathrm{T}(\tau)$ Menge aller Terme über der Signatur τ. 48

$\mathrm{FO}(\tau)$ Menge aller prädikatenlogischen Formeln mit Signatur τ. 49

$\exists$ Existenzquantor. 49, 53

$\forall$ Allquantor. 49, 53

$[\![t]\!]^{\mathfrak{I}}$ Wert eines Terms (in FO) unter der Interpretation $\mathfrak{I}$. 52

$[x/a]$ Ersetzung der Variablen x durch das Element a aus dem Universum der Struktur $\mathfrak{A}$ in einer Variablenbelegung β oder Interpretation $(\mathfrak{A}, \beta)$. 53

$\mathrm{MC}(\mathfrak{A}, \psi)$ Auswertungsspiel für die Struktur $\mathfrak{A}$ und die prädikatenlogische Formel ψ. 65

$\cong$ Isomorphie von Strukturen. 78

$\xrightarrow{\sim} \pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$ ist ein Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$. 78

$1_{\mathfrak{A}}$ Identitätsabbildung der Struktur $\mathfrak{A}$. 78

$\mathrm{Aut}(\mathfrak{A})$ Automorphismengruppe der Struktur $\mathfrak{A}$. 78

$\mathrm{Th}(\mathfrak{A})$ Theorie der Struktur $\mathfrak{A}$. 81

$\mathrm{qr}(\psi)$ Quantorenrang der prädikatenlogischen Formel ψ. 82

$\equiv_m$ m-Äquivalenz von Strukturen. 83

$\mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ Menge der lokalen Isomorphismen von $\mathfrak{A}$ nach $\mathfrak{B}$. 84

$G_m(\mathfrak{A}, \mathfrak{B})$ Ehrenfeucht-Fraïssé-Spiel mit m Zügen auf den Strukturen $\mathfrak{A}$ und $\mathfrak{B}$. 84

$G(\mathfrak{A}, \mathfrak{B})$ Ehrenfeucht-Fraïssé-Spiel ohne feste Beschränkung der Anzahl Züge auf den Strukturen $\mathfrak{A}$ und $\mathfrak{B}$. 85

$\mathfrak{H}(\Sigma)$ Herbrandstruktur zur Menge Σ von atomaren FO-Sätzen. 99

$\mathfrak{A}(\Sigma)$ kanonisches Modell der Menge Σ von atomaren FO-Sätzen. 102

ML Menge aller Formeln der Modallogik. 121

$\langle a \rangle$ „möglicherweise“-Operator der Modallogik für Kantenrelation E_a. 121, 123

$[a]$ „notwendigerweise“-Operator der Modallogik für Kantenrelation E_a. 121, 123

$\Diamond$ Diamond- oder „möglicherweise“-Operator der Modallogik. 121

$\Box$ Box- oder „notwendigerweise“-Operator der Modallogik. 121

$[\![\psi]\!]^{\mathcal{K}}$ Menge aller Zustände im Transitionssystem $\mathcal{K}$, an denen die modallogische Formel ψ gilt (Extension). 122

$\sim$ Bisimulation. Relation zwischen zwei Kripkestrukturen mit jeweils einem ausgezeichneten Knoten. 125

$\sim_n$ n-Bisimulation. Relation zwischen zwei Kripkestrukturen mit jeweils einem ausgezeichneten Knoten. 126

$\mathrm{md}(\psi)$ Modaltiefe der modallogischen Formel ψ. 128

$\equiv_{\mathrm{ML}}$ modallogische Äquivalenz zwischen Kripkestrukturen mit ausgezeichneten Knoten. 128

$\equiv^n_{\mathrm{ML}}$ modallogische Äquivalenz bis Modaltiefe n zwischen Kripkestrukturen mit ausgezeichneten Knoten. 128

LTL linear temporal logic. 132

CTL computation tree logic, branching time temporal logic. 132

U „until“-Operator in LTL und CTL. 132, 135

$\mathrm{F}\psi$ Abkürzung für $(1\,\mathrm{U}\,\psi)$ in temporaler Logik („finally“). 133

$\mathrm{G}\psi$ Abkürzung für $\neg\mathrm{F}\neg\psi$ in temporaler Logik („globally“). 133

E Operator in CTL, äquivalent zu $\Diamond$. 135

A Operator in CTL, äquivalent zu $\Box$. 135

MSO monadische Logik zweiter Stufe. 137