Mathematische Logik
WS 97/98

Erich Grädel

Inhaltsverzeichnis

Kapitel 1

Strukturen und Homomorphismen

In diesem Kapitel entwickeln wir den Begriff einer mathematischen *Struktur*. Er ist hinreichend allgemein um fast alle in Mathematik und Informatik auftretenden Strukturen zu erfassen (z.B. algebraische und geometrische Strukturen, Räume, Datenstrukturen, Datenbanken, etc.). Wir behandeln wichtige Beziehungen zwischen Strukturen und werden zahlreiche Beispiele beschreiben.

Ausserdem führen wir Abildungen zwischen Strukturen ein, welche (in unterschiedlichem Masse) *strukturerhaltend* sind. Wir definieren *Kongruenzrelationen* auf Strukturen und *Quotientenstrukturen*. Schliesslich diskutieren wir *Äquivalenzen* (Ununterscheidbarkeitsrelationen) zwischen Strukturen. Die wichtigste und bekannteste ist natürlich die *Isomorphie*. Für die mathematische Logik sind aber auch andere, schwächere Äquivalenzen wichtig, insbesondere die *endliche Isomorphie*. Wie wir später sehen werden, entspricht diese der Ununterscheidbarkeit von Strukturen durch Sätze der Prädikatenlogik.

1.1 Einige Grundbegriffe

Kartesische Produkte. Seien A und B Mengen. Dann ist

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

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

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

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

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

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

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

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

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

Lemma 1.1. *Jede abzählbare Menge ist entweder endlich oder gleichmächtig zu* $\mathbb{N}$.

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

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

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

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

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

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

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

Satz 1.2. *Keine Menge ist gleichmächtig zu ihrer Potenzmenge.*

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

$$b \in f(b) \qquad \Longleftrightarrow \qquad b \in B_f \qquad \Longleftrightarrow \qquad b \notin f(b).$$

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

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

	0	1	2	3	$\dots$
A_0	1	0	0	1	$\dots$
A_1	0	1	0	0	$\dots$
A_2	1	1	0	0	$\dots$
A_3	1	0	0	0	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

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

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

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

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

Übung 1.1. Beweisen Sie die folgenden Aussagen.

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

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

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

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

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

aller (endlichen) Wörter über dem Alphabet A.

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

1.2 Strukturen

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

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

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

Definition 1.3. Eine *Signatur* τ ist eine Menge von Funktions- und Relationssymbolen. Jedes dieser Symbole hat eine feste endliche Stelligkeit. Formal:

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

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

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

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

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

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

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

Notation. Normalerweise verwenden wir

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

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

Definition 1.4. Eine τ-*Struktur* $\mathfrak{A}$ besteht aus

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

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

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

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

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

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

Definition 1.5. $\mathfrak{A}, \mathfrak{B}$ seien τ-Strukturen. $\mathfrak{A}$ ist *Substruktur* von $\mathfrak{B}$, (kurz: $\mathfrak{A} \subseteq \mathfrak{B}$), wenn

(1) $A \subseteq B$,

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

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

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

Ist $\mathfrak{A}$ eine Substruktur der τ-Struktur $\mathfrak{B}$, so ist A *τ-abgeschlossen*, d.h., für alle $f \in F^n(\tau)$ und alle $a_1, \dots, a_n \in A$ 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 1.6. 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 $\tau - \sigma$ 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 $(\mathbb{R}, +, \cdot, 0, 1)$.

1.3 Ein Zoo von Strukturen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(6) **Gruppen.** Wie können Gruppen (im Sinne der Algebra) durch Strukturen gemäss Definition 1.4 formalisiert werden? Dafür gibt es mehrere Möglichkeiten, abhängig davon, welche in Gruppen vorkommenden Funktionen und Relationen explizit (d.h. in der Signatur) vorkommen sollen. Mit den üblichen Bezeichnungen $\circ$ für die Gruppenoperation, e für das neutrale Element, g^{-1} für das zu g inverse Element ergeben sich sofort die Möglichkeiten

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

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

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

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

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

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

(8) **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. Ein solches Transitionssystem wird beschrieben durch eine Struktur mit Universum S, und einer Menge $\{E_a : a \in A\}$ von binären Relationen auf S. Dabei soll die Relation E_a 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.

(9) **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 $(a_1, \dots, a_n) \in D_1 \times \cdots \times D_n$ wobei $D_1, \dots, D_n$ die den einzelnen Spalten (im Datenbank-Jargon: den Attributen) zugeordneten Domains sind (z.B. Integers, Strings, ...). Sei D die Vereinigung aller in der Datenbank vorkommenden Domains. Die Tabelle R kann dann als eine n-stellige Relation über D aufgefasst werden: $R \subseteq D^n$.

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

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

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

Da alle Relationen R_i endlich sind, ist auch $\mathrm{ad}(\mathfrak{D})$ endlich und die endliche Substruktur $(\mathrm{ad}(\mathfrak{D}), R_1, \ldots, R_m)$ 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.

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

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

Man kann aber einen Vektorraum V über K auch als eine Struktur über dem Universum $U = V \cup K$ formalisieren. Innerhalb dieses Universums werden Vektoren und Skalare durch einstellige Relationen $V, K \subseteq U$ identifiziert. Somit kann der Vektorraum etwa durch eine Struktur $(U, V, K, R_V^+, 0_V, R_K^+, R_K^*, 0_K, 1_K, R_{KV}^\circ)$ formalisiert werden, wobei Addition auf V, die Körperoperationen auf K und die Skalarmultiplikation durch ihre Graphen repräsentiert werden.

Man erkennt hier einige Probleme, die bei der Formalisierung von mathematischen Objekten durch Strukturen nach Definition 1.4 auftreten können:

- Es können in einer Struktur Objekte verschiedener Art auftreten (z.B. Vektoren und Skalare, Zahlen und Mengen von Zahlen, etc.)
- Funktionen sind oft *partiell*, d.h. nicht überall definiert.

Diese Probleme bereiten aber keine grundsätzlichen Schwierigkeiten. Sie werden gelöst durch Ad-Hoc-Konstruktionen (Identifikation der einzelnen Sorten durch einstellige Relationen, Beschreibung von partiellen Funktionen durch ihre Graphen) oder durch naheliegende Verallgemeinerungen der Struktur-Definition, indem z.B. partielle Funktionen zugelassen werden oder durch Übergang zu *mehrsortigen Strukturen*, d.h. Strukturen mit mehreren Trägermengen und 'getypten' Funktionen und Relationen.

Insgesamt hat sich Definition 1.4 aber als ausreichend und sehr nützlich erwiesen.

1.4 Homomorphismen und Isomorphismen

Homomorphismen sind *strukturerhaltende Abbildungen.*

Definition 1.7. $\mathfrak{A}$ und, $\mathfrak{B}$ seien τ-Strukturen. Eine Abbildung $\pi : A \to B$ ist ein *Homomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ wenn folgende Bedingungen erfüllt sind:

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

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

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

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

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

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

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

Definition 1.8. Ein *starker Homomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ ist ein Homomorphismus $\pi : \mathfrak{A} \to \mathfrak{B}$, welcher die folgende, stärkere Version von (1) erfüllt:

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

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

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

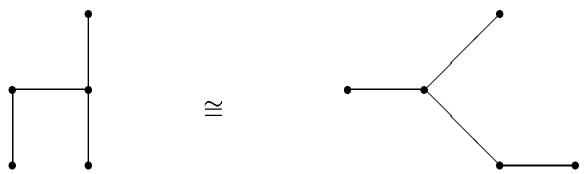
Definition 1.9. Eine *Einbettung* von $\mathfrak{A}$ in $\mathfrak{B}$ in ein injektiver starker Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$. Ein *Isomorphismus* ist ein bijektiver, starker Homomorphismus (also eine surjektive Einbettung). Zwei τ-Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ sind *isomorph* (kurz: $\mathfrak{A} \cong \mathfrak{B}$), wenn ein Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ existiert. Ein Isomorphismus $\pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{A}$ heisst *Automorphismus* von $\mathfrak{A}$.

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

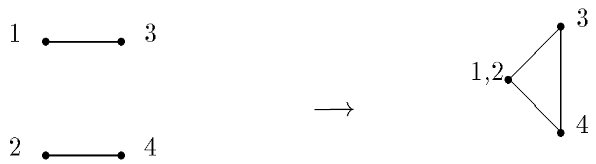
Die Menge aller Automorphismen einer Struktur $\mathfrak{A}$ bilden bzgl. Hintereinanderausführen eine Gruppe mit neutralem Element $1_{\mathfrak{A}}$. Wir nennen sie die *Automorphismengruppe* oder *Symmetriegruppe* von $\mathfrak{A}$ und bezeichnen sie mit $\mathrm{Aut}(\mathfrak{A})$. Eine Struktur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

Beispiele. (1) Unter der in Abschnitt 1.3 (10) zugrundegelegten Formalisierung von Vektorräumen sind die Homomorphismen zwischen Vektorräumen genau die linearen Abbildungen.

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



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



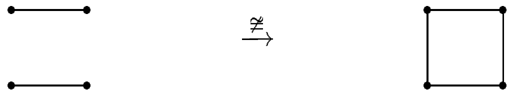
(4) Mit K_n bezeichnet man den vollständigen Graphen mit n Punkten, d.h. $K_n = (\{1, \ldots, n\}, E)$ mit $E = \{(i, j) : i \neq j\}$. Offensichtlich ist jede Permutation von $\{1, \ldots, n\}$ ein Automorphismus von K_n, d.h. $\mathrm{Aut}(K_n) = S_n$ (mit S_n bezeichnet man die Permutationsgruppe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

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

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

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

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



1.5 Kongruenzrelationen und Quotientenstrukturen

Definition 1.10. Eine binäre Relation $E \subseteq A \times A$ ist eine *Äquivalenzrelation* auf A, falls sie folgende Bedingungen erfüllt:

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

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

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

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

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

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

Sei E eine Äquivalenzrelation auf A. Dann ist

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

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

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

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

Definition 1.11. Sei $\mathfrak{A}$ eine τ-Struktur. Eine *Kongruenzrelation* auf $\mathfrak{A}$ ist eine Äquivalenzrelation $\sim$ auf dem Universum A von $\mathfrak{A}$ welche in folgendem Sinn mit den Relationen und Funktionen von $\mathfrak{A}$ kompatibel ist.

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

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

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

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

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

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

Definition 1.12. $\mathfrak{A}$ sei eine τ-Struktur und $\sim$ eine Kongruenzrelation auf $\mathfrak{A}$. Die *Quotienten-* oder *Faktor-Struktur* $\mathfrak{A}/_\sim$ ist die τ-Struktur welche wie folgt definiert ist:

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

(2) Für $f \in F^n(\tau)$ ist

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

(3) Für $R \in R^n(\tau)$

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

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

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

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

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

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

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

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

1.6 Endliche Isomorphie

Isomorphe Strukturen werden in der Mathematik in aller Regel nicht unterschieden. Wir definieren in diesem Abschnitt andere, schwächere Äquivalenzbegriffe zwischen Strukturen, nämlich die *m-Isomorphie* und die *endliche Isomorphie*. Wir werden später sehen, dass die endliche Isomorphie der Ununterscheidbarkeit durch Sätze der Prädikatenlogik entspricht.

Der Einfachheit halber betrachten wir in diesem Abschnitt nur relationale Strukturen.

Definition 1.13. Sei τ eine relationale Signatur und $\mathfrak{A}$, $\mathfrak{B}$ τ-Strukturen. Ein *lokaler* (oder *partieller) Isomorphismus* von $\mathfrak{A}$ nach $\mathfrak{B}$ ist eine injektive Abbildung $p : \mathrm{Def}(p) \to B$ wobei $\mathrm{Def}(p) \subseteq A$, so dass für alle $n \in \mathbb{N}$, alle Relationssymbole $R \in R^n(\tau)$ und alle $a_1, \ldots, a_n \in \mathrm{Def}(p)$ gilt:

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

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

Das Bild von p ist $\mathrm{Bild}(p) := \{pa : a \in \mathrm{Def}(p)\}$. Die *leere Abbildung* p mit $\mathrm{Def}(p) = \mathrm{Bild}(p) = \varnothing$ ist trivialerweise ein lokaler Isomorphismus. Ein nicht-leerer lokaler Isomorphismus ist ein Isomorphismus zwischen den von $\mathrm{Def}(p)$ und $\mathrm{Bild}(p)$ induzierten Substrukturen von $\mathfrak{A}$ und $\mathfrak{B}$. Wir identifizieren einen lokalen Isomorphismus p oft mit seinem Graphen, d.h. mit der Menge $\{(a, pa)) : a \in \mathrm{Def}(p)\}$. Insbesondere nennen wir p endlich, wenn sein Graph endlich ist.

Beispiele. (1) Betrachte die Graphen

$p = \{(2, a), (3, b), (4, d)\}$ ist ein lokaler Isomorphismus.

(2) Seien $(\mathfrak{A}, <^{\mathfrak{A}})$ und $\mathfrak{B} = (B, <^{\mathfrak{B}})$ lineare Ordnungen und $a_1, \ldots, a_n$ 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 $b_{s(1)} <^{\mathfrak{B}} b_{s(2)} <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_{s(n)}$.

Zur Motivation der folgenden Überlegungen behandeln wir einen klassischen Satz von Cantor.

Satz 1.14 (Cantor). *Je zwei abzählbare dichte Ordnungen ohne erstes und letztes Element sind isomorph.*

Beweis. Seien $\mathfrak{A} = (A, <^{\mathfrak{A}})$ und $\mathfrak{B} = (B, <^{\mathfrak{B}})$ abzählbare dichte Ordnungen ohne Endpunkte. Fixiere Aufzählungen $A = \{f(n) : n = 0, 1, 2, \ldots\}$, $B = \{g(n) : n = 0, 1, 2, \ldots\}$.

Wir definieren induktiv eine Folge $p_0 \subseteq p_1 \subseteq p_2 \subseteq \cdots$ von lokalen Isomorphismen von $\mathfrak{A}$ nach $\mathfrak{B}$ und werden daraus einen Isomorphismus $p := \bigcup_{n \in \mathbb{N}} p_n$ gewinnen können.

Setze $p_0 = \varnothing$. Sei nun $p_n = \{(a_1, b_1), \ldots, (a_n, b_n)\}$ bereits definiert, mit paarweise verschiedenen $a_1, \ldots, a_n$ (und daher auch $b_1, \ldots, b_n$). Da p_n ein lokaler Isomorphismus ist, gibt es eine Permutation s der Indizes $1, \dots, n$ so, dass $a_{s(1)} <^{\mathfrak{A}} a_{s(2)} <^{\mathfrak{A}} \cdots <^{\mathfrak{A}} a_{s(n)}$ und $b_{s(1)} <^{\mathfrak{B}} b_{s(2)} <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_{s(n)}$.

Wir definieren nun p_{n+1} wie folgt. Bei geradem n wählen wir das erste Element $f(k)$ in der Aufzählung von A, das verschieden ist von $a_1, \dots, a_n$ und setzen $a_{n+1} := f(k)$. Entweder ist $a_{n+1} <^{\mathfrak{A}} a_{s(1)}$, oder $a_{s(n)} <^{\mathfrak{A}} a_{n+1}$, oder $a_{s(i)} <^{\mathfrak{A}} a_{n+1} <^{\mathfrak{A}} a_{s(i+1)}$ für ein geeignetes i. Da $(B, <^{\mathfrak{B}})$ dicht ist und weder ein kleinstes noch ein grösstes Element besitzt, gibt es in jedem dieser Fälle ein geeignetes b_{n+1}, das in die Kette $b_{s(1)} <^{\mathfrak{B}} b_{s(2)} <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_{s(n)}$ so eingefügt werden kann, dass $p_{n+1} := p_n \cup \{(a_{n+1}, b_{n+1})\}$ ein lokaler Isomorphismus ist.

Für ungerades n gehen wir analog vor, mit vertauschten Rollen von $\mathfrak{A}$ und $\mathfrak{B}$. Wir wählen für b_{n+1} das erste Element der Aufzählung von B, das in p_n noch nicht vorkommt und finden, da auch $(A, <^{\mathfrak{A}})$ dicht und ohne Endpunkte ist, ein geeignetes a_{n+1}.

Es ist nun sofort einzusehen, dass die Vereinigung $p = \bigcup_{n \in \mathbb{N}} p_n$ ein Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ ist. □

Die wesentliche Tatsache, die in diesem Beweis benutzt wird, ist die beliebige Erweiterbarkeit von lokalen Isomorphismen:

Zu jedem $p = \{(a_1, b_1), \dots, (a_n, b_n)\} \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ und jedem $a \in A$ (bzw. $b \in B$) findet man ein $b \in B$ (bzw. ein $a \in A$) so dass $p \cup \{(a, b)\}$ wieder ein lokaler Isomorphismus ist. Diese Eigenschaft nennt man die *Hin-* bzw. *Her-Eigenschaft*.

Definition 1.15. Sei $I \subseteq \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ eine Menge von lokalen Isomorphismen. Ein lokaler Isomorphismus p von $\mathfrak{A}$ nach $\mathfrak{B}$ hat die *Hin- und Her-Eigenschaft* bzgl. I wenn gilt:

Hin: Für alle $a \in A$ gibt es ein $b \in B$ so dass $p \cup \{(a, b)\} \in I$.

Her: Für alle $b \in B$ gibt es ein $a \in A$ so dass $p \cup \{(a, b)\} \in I$.

Für gegebene τ-Strukturen $\mathfrak{A}$, $\mathfrak{B}$ definieren wir nun eine Folge

$$I_0(\mathfrak{A}, \mathfrak{B}) \supseteq I_1(\mathfrak{A}, \mathfrak{B}) \supseteq \cdots \supseteq I_m(\mathfrak{A}, \mathfrak{B}) \supseteq \cdots$$

von Mengen lokaler Isomorphismen.

$$\begin{aligned} I_0(\mathfrak{A}, \mathfrak{B}) :=& \{p \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B}) : p \text{ endlich}\}. \\ I_{m+1}(\mathfrak{A}, \mathfrak{B}) :=& \{p \in I_m(\mathfrak{A}, \mathfrak{B}) : p \text{ hat die Hin- und Her-Eigenschaft bezüglich } I_m(\mathfrak{A}, \mathfrak{B})\} \end{aligned}$$

Wenn $p \in I_m(\mathfrak{A}, \mathfrak{B})$, dann heisst p *m-fach erweiterbar*.

Beispiele. Wir analysieren die Kette der Mengen $I_m(\mathfrak{A}, \mathfrak{B})$ für lineare Ordnungen. Für solche Strukturen haben wir $I_0(\mathfrak{A}, \mathfrak{B})$ bereits beschrieben.

(1) Sei $\mathfrak{A} = (\mathbb{Z}, <), \mathfrak{B} = (\mathbb{R}, <)$. Betrachte etwa $p = \{(0, \frac{1}{3}), (1, \frac{1}{2})\} \in I_0(\mathfrak{A}, \mathfrak{B})$. Offensichtlich ist $p \notin I_1(\mathfrak{A}, \mathfrak{B})$, da die Her-Eigenschaft nicht erfüllt ist. Für $b \in \mathbb{R}$ mit $\frac{1}{3} < b < \frac{1}{2}$ gibt es *keinen* lokalen Isomorphismus $p \cup \{(a, b)\}$, da es kein $a \in \mathbb{Z}$ gibt mit $0 < a < 1$.

Man sieht nun leicht ein, dass

$$\begin{aligned} I_1(\mathfrak{A}, \mathfrak{B}) \quad = \quad & \{p \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B}) : p \text{ endlich und für alle } a, a' \in \mathrm{Def}(p) \\ & \text{ist } |a - a'| \geq 2\}. \end{aligned}$$

Daraus wiederum folgt, dass $I_2(\mathfrak{A}, \mathfrak{B})$ nur den leeren lokalen Isomorphismus enthält. Wenn nämlich $(a, b) \in p$ dann findet man zu $a + 1$ eben keine Erweiterung in $I_1(\mathfrak{A}, \mathfrak{B})$. Also ist $I_2(\mathfrak{A}, \mathfrak{B}) = \{\varnothing\}$ und daher $I_3(\mathfrak{A}, \mathfrak{B}) = \varnothing$. (Man beachte den Unterschied zwischen $I_2(\mathfrak{A}, \mathfrak{B})$ und $I_3(\mathfrak{A}, \mathfrak{B})$.)

(2) Sei $\mathfrak{A} = (\mathbb{Q}, <)$, $\mathfrak{B} = (\mathbb{R}, <)$. Da sowohl $\mathbb{Q}$ als auch $\mathbb{R}$ dicht geordnet sind, ist jeder endliche lokale Isomorphismus beliebig oft erweiterbar. Also gilt in diesem Fall:

$$I_m(\mathfrak{A}, \mathfrak{B}) = I_0(\mathfrak{A}, \mathfrak{B}) \text{ für alle } m \in \mathbb{N}.$$

Per Induktion über m folgt sofort, dass die Mengen $I_m(\mathfrak{A}, \mathfrak{B})$ abgeschlossen sind unter Restriktionen: Wenn $p \in I_m(\mathfrak{A}, \mathfrak{B})$ und $q \subseteq p$, dann auch $q \in I_m(\mathfrak{A}, \mathfrak{B})$. Daher ist $I_m(\mathfrak{A}, \mathfrak{B}) \neq \varnothing$ genau dann, wenn $\varnothing \in I_m(\mathfrak{A}, \mathfrak{B})$, d.h., wenn der leere lokale Isomorphismus m-fach erweiterbar ist.

Definition 1.16. *(i)* Zwei relationale τ-Strukturen $\mathfrak{A}$, $\mathfrak{B}$ heissen *m-isomorph*, $\mathfrak{A} \cong_m \mathfrak{B}$, wenn $I_m(\mathfrak{A}, \mathfrak{B}) \neq \varnothing$.

(ii) $\mathfrak{A}$ und $\mathfrak{B}$ heissen *endlich isomorph*, $\mathfrak{A} \cong_e \mathfrak{B}$, wenn $I_m(\mathfrak{A}, \mathfrak{B}) \neq \varnothing$ für alle $m \in \mathbb{N}$.

Setze $I_\omega(\mathfrak{A}, \mathfrak{B}) := \bigcap_{m \in \mathbb{N}} I_m(\mathfrak{A}, \mathfrak{B})$. Also ist $\mathfrak{A} \cong_e \mathfrak{B}$ genau dann, wenn $I_\omega(\mathfrak{A}, \mathfrak{B}) \neq \varnothing$. Dies wiederum ist genau dann der Fall wenn $\varnothing \in I_\omega(\mathfrak{A}, \mathfrak{B})$.

Die letzten Beispiele zeigen:

- $(\mathbb{Z}, <) \not\cong_e (\mathbb{R}, <)$, da zwar $(\mathbb{Z}, <) \cong_2 (\mathbb{R}, <)$ aber $(\mathbb{Z}, <) \not\cong_3 (\mathbb{R}, <)$.
- $(\mathbb{Q}, <) \cong_e (\mathbb{R}, <)$.

Satz 1.17. *Für beliebige relationale τ-Strukturen $\mathfrak{A}$, $\mathfrak{B}$ gilt: Wenn $|A| = m$ endlich ist und $\mathfrak{A} \cong_{m+1} \mathfrak{B}$, dann ist $\mathfrak{A} \cong \mathfrak{B}$. Insbesondere sind für endliche Strukturen die Isomorphie und die endliche Isomorphie gleichbedeutend.*

Beweis. Sei $A = \{a_1, \ldots, a_m\}$ und $\mathfrak{A} \cong_{m+1} \mathfrak{B}$. Insbesondere ist dann der leere lokale Isomorphismus $\varnothing \in I_{m+1}(\mathfrak{A}, \mathfrak{B})$ Wir wenden darauf zunächst m Mal die Hin-Eigenschaft an. Zu $a_1 \in A$ gibt es also ein $b_1 \in B$, so dass $(a_1, b_1) \in I_m(\mathfrak{A}, \mathfrak{B})$. Durch Wiederholung des Arguments folgt, dass zu $a_1, a_2, \ldots, a_m$ Elemente $b_1, b_2, \ldots, b_m \in B$, existieren, so dass

$$p := \{(a_1, b_1), (a_2, b_2)\}, \ldots, (a_m, b_m)\} \in I_1(\mathfrak{A}, \mathfrak{B}).$$

Da $\{a_1, \ldots, a_m\} = A$ folgt, dass $p : \mathfrak{A} \hookrightarrow \mathfrak{B}$ eine Einbettung ist.

Zu zeigen bleibt, dass p surjektiv (und also ein Isomorphismus) ist. Angenommen, es gäbe ein $b \in B - \{b_1, \ldots, b_m\}$. Nach der Her-Eigenschaft gibt es zu b ein $a \in A$, so dass $p \cup \{(a, b)\} \in I_0(\mathfrak{A}, \mathfrak{B})$. Dies ist aber unmöglich, da b von allen $b_1, \ldots, b_m$ verschieden ist und $A = \{a_1, \ldots, a_m\}$. Also ist $p : \mathfrak{A} \to \mathfrak{B}$ ein Isomorphismus. □

Übung 1.2. Sei $\tau = \{P\}$, P ein einstelliges Relationssymbol. Der *Charakter* einer τ-Struktur $\mathfrak{A} = (A, P^{\mathfrak{A}})$ ist das Paar (i, j) mit $i = |P^{\mathfrak{A}}|$ wenn $P^{\mathfrak{A}}$ endlich ist, $i = \infty$ sonst, und mit $j = |A - P^{\mathfrak{A}}|$ wenn $A - P^{\mathfrak{A}}$ endlich ist, $j = \infty$ sonst. Zeigen Sie, dass zwei τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ genau dann endlich isomorph sind, wenn sie den gleichen Charakter haben. Wie ist die entsprechende Bedingung für die m-Isomorphie?

Übung 1.3. Seien $\mathfrak{A}$ und $\mathfrak{B}$ zwei lineare Ordnungen, mit $A \cap B = \varnothing$. (Wenn dies nicht erfüllt ist, gehen wir zu einer isomorphen Kopie von $\mathfrak{B}$ über.) Dann bezeichnen wir mit $\mathfrak{A} + \mathfrak{B}$ die lineare Ordnung $(A \cup B, <)$ welche $\mathfrak{A}$ und $\mathfrak{B}$ so erweitert, dass jedes Element von $\mathfrak{B}$ grösser ist als alle Elemente von $\mathfrak{A}$. Man zeige, dass für beliebige lineare Ordnungen und alle $m \in N$ gilt: Wenn $\mathfrak{A} \cong_m \mathfrak{A}'$ und $\mathfrak{B} \cong_m \mathfrak{B}'$, dann auch $\mathfrak{A} + \mathfrak{B} \cong_m \mathfrak{A}' + \mathfrak{B}'$.

Übung 1.4. Zu jeder Äquivalenzstruktur $\mathfrak{A} = (A, \sim)$ definieren wir die Funktion $F_{\mathfrak{A}} : \mathbb{N} \cup \{\infty\} \to \mathbb{N} \cup \{\infty\}$, wobei $F_{\mathfrak{A}}(m)$ die Anzahl der $\sim$-Äquivalenzklassen mit m Elementen angibt. Seien $\mathfrak{A}$, $\mathfrak{B}$ beliebige Äquivalenzstrukturen. Beweisen Sie folgende Aussagen.

(a) Wenn $F_{\mathfrak{A}}(m) = n$ und $\mathfrak{A} \cong_{m(n+1)+1} \mathfrak{B}$, dann auch $F_{\mathfrak{B}}(m) = n$.

(b) Wenn $\mathfrak{A} \cong_{nm} \mathfrak{B}$ und $\mathfrak{A}$ höchstens n Äquivalenzklassen hat, von denen jede höchstens m Elemente enthält, dann gilt dasselbe für $\mathfrak{B}$.

(c) Zeigen Sie, dass die endliche Isomorphie von $\mathfrak{A}$ und $\mathfrak{B}$ nur von $F_{\mathfrak{A}}$ und $F_{\mathfrak{B}}$ abhängt. Formulieren sie eine notwendige und hinreichende Bedingung für $\mathfrak{A} \cong_e \mathfrak{B}$.

1.7 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*

Wir präsentieren nun eine spieltheoretische Deutung der endlichen Isomorphie. Wie im letzten Abschnitt setzen wir voraus, dass $\mathfrak{A}, \mathfrak{B}$ zwei Strukturen mit relationaler Signatur τ sind. Weiter sei m eine beliebige natürliche Zahl.

Das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$. Das Ehrenfeucht-Fraïssé Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ wird von zwei Spielern nach folgenden Regeln gespielt.

Das *Spielfeld* besteht aus den Strukturen $\mathfrak{A}$ und $\mathfrak{B}$. Wir setzten dabei voraus, dass $A \cap B = \varnothing$. Die Spieler sind der *Herausforderer* und die *Duplikatorin*, oft auch bezeichnet als Spieler I und II. Eine Partie besteht aus m Zügen.

Im *i-ten Zug* bestimmt der Herausforderer entweder ein Element $a_i \in A$ oder ein $b_i \in B$. Die Duplikatorin antwortet indem sie ein Element aus der jeweils anderen Struktur auswählt.

Nach m Zügen sind also Elemente $a_1, \dots, a_m$ aus $\mathfrak{A}$ und $b_1, \dots, b_m$ aus $\mathfrak{B}$ ausgezeichnet. Die Duplikatorin hat die Partie gewonnen, wenn die Menge $\{(a_1, b_1), \dots, (a_m, b_m)\}$ ein lokaler Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ ist. Andernfalls hat der Herausforderer gewonnen.

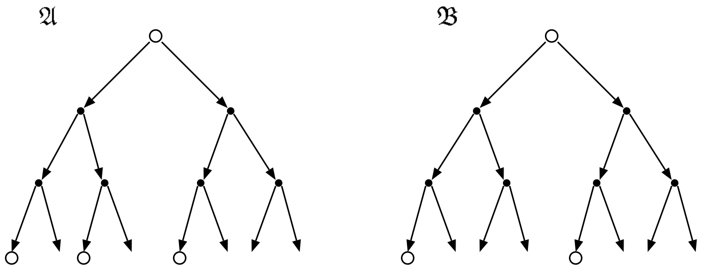
Nach i Zügen in $G_m(\mathfrak{A}, \mathfrak{B})$ ist eine *Position* $(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$ erreicht. Das verbleibende Teil-Spiel, mit $m - i$ Zügen, bezeichnen wir mit $G_{m-i}(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$.

Eine *Gewinn-Strategie* des Herausforderers für ein solches (Teil-)Spiel ist eine Funktion, die ihm in jeder erreichbaren Position mögliche Züge nennt, mit denen er die Partie gewinnt, egal wie seine Gegnerin spielt. Analog sind Gewinnstrategien für die Duplikatorin definiert.

Wir sagen, *der Herausforderer (bzw. die Duplikatorin) gewinnt das Spiel* $G_m(\mathfrak{A}, \mathfrak{B})$, wenn er (bzw. sie) eine Gewinnstrategie dafür hat. Per Induktion über die Anzahl der Züge zeigt man leicht, dass für jedes (Teil-)Spiel genau einer der Spieler eine Gewinnstrategie hat.

Beispiele. (1) Sei $\mathfrak{A} = (\mathbb{Z}, <)$, $\mathfrak{B} = (\mathbb{R}, <)$. Die Duplikatorin gewinnt $G_2(\mathfrak{A}, \mathfrak{B})$, aber der Herausforderer gewinnnt $G_3(\mathfrak{A}, \mathfrak{B})$.

(2) Für $\tau = \{E, P\}$ (wobei P einstelliges und E zweistelliges Relationssymbol) seien die folgenden Strukturen gegeben:



Auch hier gewinnt gewinnt der Herausforderer $G_3(\mathfrak{A}, \mathfrak{B})$, die Duplikatorin aber $G_2(\mathfrak{A}, \mathfrak{B})$.

Das Spiel G($\mathfrak{A}, \mathfrak{B}$). Eine wichtige Variante ist das Ehrenfeucht-Fraïssé Spiel $G(\mathfrak{A}, \mathfrak{B})$ ohne feste Beschränkung der Anzahl der Züge: In jeder Partie bestimmt der Herausforderer zunächst ein $m \in \mathbb{N}$, dann wird das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gespielt.

Der Herausforderer gewinnt also das Spiel $G(\mathfrak{A}, \mathfrak{B})$ genau dann, wenn es ein $m \in \mathbb{N}$ gibt so, dass er das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gewinnt. Anders ausgedrückt: die Duplikatorin gewinnt $G(\mathfrak{A}, \mathfrak{B})$ genau dann, wenn sie für jedes der Spiele $G_m(\mathfrak{A}, \mathfrak{B})$ eine Gewinnstrategie besitzt.

Es besteht ein enger Zusammenhang zwischen der j-fachen Erweiterbarkeit eines lokalen Isomorphismus und Gewinnstrategien der Duplikatorin von einer entsprechenden Position eines Ehrenfeucht-Fraïssé Spiels mit j verbleibenden Zügen. Für den Fall $j = 0$ ist der Zusammenhang offensichtlich: Die Duplikatorin gewinnt $G_0(\mathfrak{A}, a_1, \dots, a_m, \mathfrak{B}, b_1, \dots, b_m)$ genau dann wenn $\{(a_1, b_1), \dots, (a_m, b_m)\} \in I_0(\mathfrak{A}, \mathfrak{B})$.

Satz 1.18. *Für beliebige relationale τ-Strukturen $\mathfrak{A}$, $\mathfrak{B}$ und $m \in \mathbb{N}$ gilt:*

(i) $\mathfrak{A} \cong_m \mathfrak{B}$ genau dann, wenn die Duplikatorin das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gewinnt.

(ii) $\mathfrak{A} \cong_e \mathfrak{B}$ genau dann, wenn die Duplikatorin das Spiel $G(\mathfrak{A}, \mathfrak{B})$ gewinnt.

Wir beweisen folgende allgemeinere Aussage:

Lemma 1.19. *Für alle $m \in \mathbb{N}$, $i \leq m$ und alle $a_1, \dots, a_i \in A, b_1, \dots, b_i \in B$ gilt: Die Duplikatorin gewinnt das Teilspiel $G_{m-i}(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$ genau dann, wenn $\{(a_1, b_1), \dots, (a_i, b_i)\} \in I_{m-i}(\mathfrak{A}, \mathfrak{B})$.*

Beweis. Wir beweisen dies per Induktion über die Anzahl $j := m - i$ der verbleibenden Züge. Für $j = 0$ haben wir dies bereits festgestellt. Sei nun $j > 0$. Die Duplikatorin gewinnt das Spiel $G_j(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$ genau dann, wenn sie zu jedem vom Herausforderer gewählten $a_{i+1} \in A$ ein $b_{i+1} \in B$, und zu jedem $b_{i+1} \in B$ ein $a_{i+1} \in A$ findet, so dass sie das Teilspiel $G_{j-1}(\mathfrak{A}, a_1, \dots, a_i, a_{i+1}, \mathfrak{B}, b_1, \dots, b_i, b_{i+1})$ gewinnt. Nach Induktionsvoraussetzung gewinnt sie ein solches Teilspiel genau dann, wenn $\{(a_1, b_1), \dots, (a_i, b_i), (a_{i+1}, b_{i+1})\} \in I_{j-1}(\mathfrak{A}, \mathfrak{B})$. Also folgt, dass die Duplikatorin das Spiel $G_j(\mathfrak{A}, a_1, \dots, a_i, \mathfrak{B}, b_1, \dots, b_i)$ genau dann gewinnt wenn der lokale Isomorphismus $\{(a_1, b_1), \dots, (a_i, b_i)\}$ die Hin- und Her-Eigenschaft bzgl. $I_{j-1}(\mathfrak{A}, \mathfrak{B})$ hat, d.h. wenn er zu $I_j(\mathfrak{A}, \mathfrak{B})$ gehört. $\square$

Die erste Behauptung von Satz 1.18 ergibt sich nun wenn man in Lemma 1.19 $i = 0$ setzt: Die Duplikatorin gewinnt $G_m(\mathfrak{A}, \mathfrak{B})$ genau dann wenn der leere lokale Isomorphismus zu $I_m(\mathfrak{A}, \mathfrak{B})$ gehört. Dies ist bekanntlich genau dann der Fall wenn $I_m(\mathfrak{A}, \mathfrak{B}) \neq \emptyset$. Die zweite Behauptung von Satz 1.18 ergibt sich unmittelbar aus der ersten.

1.8* Partielle Isomorphie.

Ein Äquivalenzbegriff von Strukturen der zwischen der Isomorphie und der endlichen Isomorphie liegt, ist die *partielle Isomorphie.*

Definition 1.20. Zwei relationale τ-Strukturen $\mathfrak{A}$, $\mathfrak{B}$ sind *partiell isomorph*, $\mathfrak{A} \cong_p \mathfrak{B}$, wenn eine nichtleere Menge $I \subseteq \mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$ existiert so, dass jedes $p \in I$ die Hin- und Her-Eigenschaft bzgl. I selbst besitzt.

Das heisst also, dass zu jedem $p \in I$ und jedem $a \in A$ (bzw. zu jedem $b \in B$) ein $b \in B$ (bzw. ein $a \in A$) existiert mit $p \cup \{(a, b)\} \in I$. Wir sagen in diesem Fall auch: I hat die Hin- und Her-Eigenschaft.

Beispiel. Zwei dichte Ordnungen $\mathfrak{A}$, $\mathfrak{B}$ ohne Endpunkte sind partiell isomorph mit

$$I = I_0(\mathfrak{A}, \mathfrak{B}) = \{p \in \mathrm{Loc}(\mathfrak{A}, \mathfrak{B}) : p \text{ endlich}\}.$$

Insbesondere gilt dies für $\mathfrak{A} = (\mathbb{Q}, <)$ und $\mathfrak{B} = (\mathbb{R}, <)$. Beachte, dass $(\mathbb{Q}, <)$ und $(\mathbb{R}, <)$ nicht isomorph sind, da $\mathbb{Q}$ abzählbar, $\mathbb{R}$ aber überabzählbar ist.

Satz 1.21. *Für beliebige relationale τ-Strukturen $\mathfrak{A}$, $\mathfrak{B}$ gilt:*

(i) $\mathfrak{A} \cong \mathfrak{B} \implies \mathfrak{A} \cong_p \mathfrak{B} \implies \mathfrak{A} \cong_e \mathfrak{B}$.

(ii) $\mathfrak{A} \cong_p \mathfrak{B}$, *$A, B$ abzählbar* $\implies \mathfrak{A} \cong \mathfrak{B}$.

Beweis. Zu *(i):* Ist $\pi : \mathfrak{A} \to \mathfrak{B}$ ein Isomorphismus, so hat $I = \{p : p \subseteq \pi\}$ die Hin- und Her-Eigenschaft. Also sind $\mathfrak{A}$ und $\mathfrak{B}$ partiell isomorph. Weiter können wir zu jedem $I : \mathfrak{A} \cong_p \mathfrak{B}$ die Menge

$$J_0 := \{q \in I_0(\mathfrak{A}, \mathfrak{B}) : \text{ es gibt ein } p \in I \text{ mit } p \supseteq q\}$$

der endlichen Restriktionen aller $p \in I$ bilden.

Offensichtlich ist $J_0 \neq \varnothing$, da $I \neq \varnothing$. Es reicht also zu zeigen, dass $J_0 \subseteq I_m(\mathfrak{A}, \mathfrak{B})$ für alle $m \in \mathbb{N}$. Wir beweisen dies per Induktion nach m.

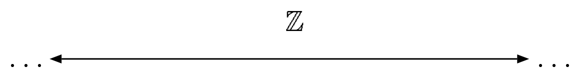
Der Fall $m = 0$ folgt unmittelbar aus der Definition von J_0. Sei nun $m > 0$ und $q \in J_0$. Es gibt also ein $p \in I$ mit $q \subseteq p$. Da p die Hin- und Her-Eigenschaft bzgl. I hat gibt es für alle $a \in A$ (bzw. $b \in B$) ein $b \in B$ (bzw. $a \in A$), so dass $p \cup \{(a, b)\} \in I$, und also $q \cup \{(a, b)\} \in J_0 \subseteq I_{m-1}(\mathfrak{A}, \mathfrak{B})$ (nach Induktionsvoraussetzung). Damit ist gezeigt, dass jedes $q \in J_0$ die Hin- und Her-Eigenschaft bzgl. $I_{m-1}(\mathfrak{A}, \mathfrak{B})$ erfüllt. Damit folgt $J_0 \subseteq I_m(\mathfrak{A}, \mathfrak{B})$.

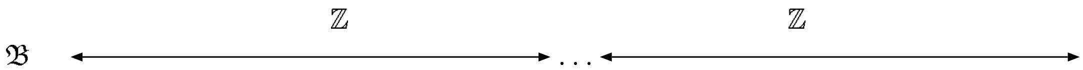
Zu *(ii)*: Der Beweis dieser Aussage ist analog zum Beweis des Satzes von Cantor (Übungsaufgabe). □

Wenn $\mathfrak{A} \cong_p \mathfrak{B}$ und A abzählbar ist, dann folgt nicht unbedingt, dass auch B abzählbar ist (und damit $\mathfrak{A} \cong \mathfrak{B}$), wie das Beispiel $(\mathbb{Q}, <) \cong_p (\mathbb{R}, <)$ zeigt. Als nächtes wollen wir Strukturen $\mathfrak{A}$, $\mathfrak{B}$ angeben, welche endlich isomorph, aber nicht partiell isomorph sind. Sei $\mathfrak{A} = (\mathbb{Z}, <)$ und $\mathfrak{B} = (\mathbb{Z} \times \{0, 1\}, <^{\mathfrak{B}})$ mit

$$(z, i) <^{\mathfrak{B}} (z', j) \text{ gdw. } (i = j \text{ und } z < z') \text{ oder } (i = 0 \text{ und } j = 1).$$

$\mathfrak{A}$





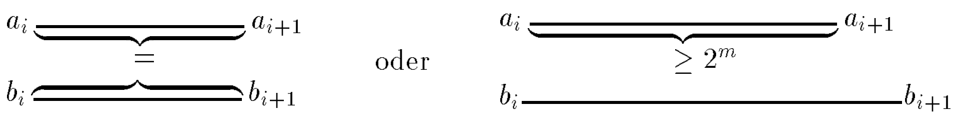
$\mathfrak{B}$ besteht also also zwei 'hintereinander gelegten' Kopien von $\mathfrak{A}$. Für $b, b' \in \mathbb{Z} \times \{0,1\}$, mit $b <^{\mathfrak{B}} b'$, setzen wir

$$b' \dot{-} b := \begin{cases} b' - b & \text{wenn } b, b' \text{ in derselben Kopie von } \mathbb{Z} \text{ sind} \\ \infty & \text{wenn } b \in \mathbb{Z} \times \{0\},\ b' \in \mathbb{Z} \times \{1\}. \end{cases}$$

Für $i, j \in \mathbb{N} \cup \{\infty\}$, $m \in \mathbb{N}$ schreiben wir $i =_m j$ wenn entweder $i = j$ oder $i, j > m$.

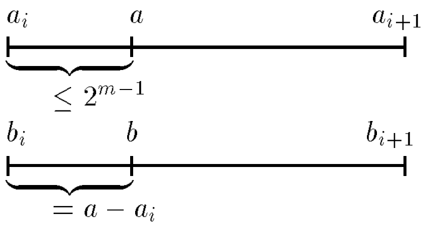
Behauptung. $\mathfrak{A} \cong_e \mathfrak{B}$

Beweis. Sei $p = \{(a_1, b_1), \ldots, (a_r, b_r)\}$ ein lokaler Isomorphismus von $\mathfrak{A}$ und $\mathfrak{B}$ mit $a_1 <^{\mathfrak{A}} a_2 <^{\mathfrak{A}} \cdots <^{\mathfrak{A}} a_r$ und $b_1 <^{\mathfrak{B}} b_2 <^{\mathfrak{B}} \cdots <^{\mathfrak{B}} b_r$, und sei weiter $(a_{i+1} - a_i) =_{2^m} (b_{i+1} \dot{-} b_i)$ für $i = 1, 2, \ldots, r-1$.



Wir zeigen durch Induktion nach m, dass $p \in I_m(\mathfrak{A}, \mathfrak{B})$. Für $m = 0$ ist dies offensichtlich der Fall. Für $m > 0$ ist zu zeigen, dass p die Hin- und Her-Eigenschaft bzgl. $I_{m-1}(\mathfrak{A}, \mathfrak{B})$ besitzt. Wir beschränken uns auf den Beweis der Hin-Eigenschaft. Für ein beliebiges $a \in A$ gilt entweder $a_i < a \leq a_{i+1}$ für ein $i < r$, oder $a \leq a_1$, oder $a_r < a$. Für den Fall, dass $a_i < a \leq a_{i+1}$ unterscheiden wir drei Unterfälle:

(1) Sei $a - a_i \leq 2^{m-1}$. Dann wählen wir b so, dass $b - b_i = a - a_i$.



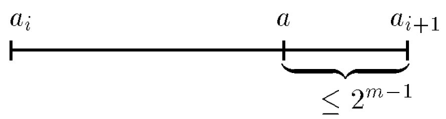
Da $(a_{i+1} - a_i) =_{2^m} (b_{i+1} \dot{-} b_i)$ schliessen wir:

(a) wenn $a_{i+1} - a_i = b_{i+1} - b_i$, dann auch $a_{i+1} - a = b_{i+1} - b$.

(b) wenn $a_{i+1} - a_i > 2^m$ und $b_{i+1} - b_i > 2^m$, dann auch $a_{i+1} - a > 2^{m-1}$ und $b_{i+1} - b > 2^{m-1}$.

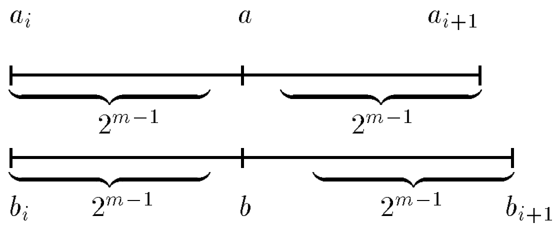
Also gilt $a - a_i = b - b_i$ und $(a_{i+1} - a) =_{2^{m-1}} (b_{i+1} \dot{-} b)$.

(2) Sei $a_{i+1} - a \leq 2^{m-1}$.



Dieser Fall wird völlig analog behandelt.

(3) Es bleibt der Fall, dass $a - a_i > 2^{m-1}$ und $a_{i+1} - a > 2^{m-1}$. Dann ist $a_{i+1} - a_i > 2^m$ und daher auch $b_{i+1} - b_i > 2^m$. Daher existiert ein b mit $b - b_i > 2^{m-1}$ und $b_{i+1} \dot{-} b > 2^{m-1}$.



Die Fälle $a \leq a_1$ oder $a_r < a$ werden in der selben Weise behandelt. Nach Induktionsvoraussetzung folgt, dass $p \cup \{(a, b)\} \in I_{m-1}(\mathfrak{A}, \mathfrak{B})$. Die Argumentation für die Her-Eigenschaft ist weitestgehend analog. Also ist $I_m(\mathfrak{A}, \mathfrak{B}) \neq \varnothing$ für alle $m \in \mathbb{N}$ und somit $\mathfrak{A} \cong_e \mathfrak{B}$. $\square$

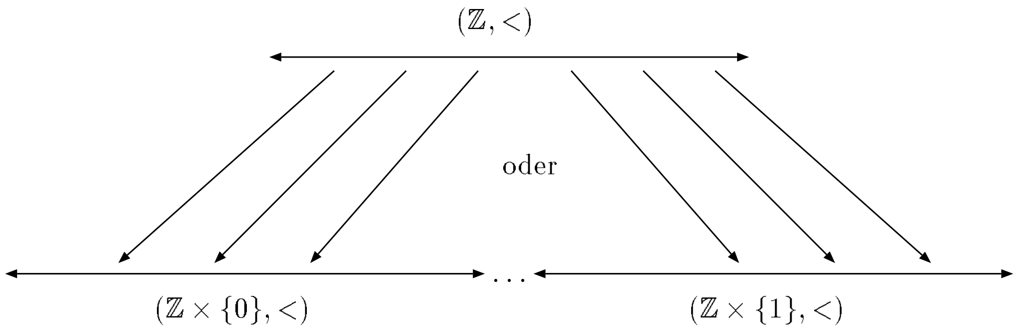
Behauptung. $\mathfrak{A} \not\cong_p \mathfrak{B}$.

Beweis. Offensichtlich ist $\mathfrak{A} \not\cong \mathfrak{B}$. Da $\mathfrak{A}$ und $\mathfrak{B}$ abzählbar sind, würde aus $\mathfrak{A} \cong_p \mathfrak{B}$ aber $\mathfrak{A} \cong \mathfrak{B}$ folgen. $\square$

Über das Endliche hinaus zählen. Für beliebige relationale Strukturen $\mathfrak{A}, \mathfrak{B}$ haben wir aus der Kette $I_0(\mathfrak{A}, \mathfrak{B}) \supseteq I_1(\mathfrak{A}, \mathfrak{B}) \supseteq \cdots$ die Menge

$$I_\omega(\mathfrak{A}, \mathfrak{B}) := \bigcap_{m \in \mathbb{N}} I_m(\mathfrak{A}, \mathfrak{B})$$

definiert. Für die soeben betrachteten Strukturen $\mathfrak{A} = (\mathbb{Z}, <)$ und $\mathfrak{B} = (\mathbb{Z} \times \{0, 1\}, <^{\mathfrak{B}})$ besteht $I_\omega(\mathfrak{A}, \mathfrak{B})$ aus den endlichen lokalen Isomorphismen p für die gilt: $\mathrm{Bild}(p) \subseteq \mathbb{Z} \times \{i\}$ für $i = 0$ oder $i = 1$, und es gibt einen Isomorphismus $\pi : (\mathbb{Z}, <) \to (\mathbb{Z} \times \{i\}, <)$ mit $p \subset \pi$.



So wie $I_{m+1}(\mathfrak{A},\mathfrak{B})$ aus $I_m(\mathfrak{A},\mathfrak{B})$ definiert wurde, können wir auch 'im Unendlichen weiterzählen' und $I_{\omega+1}(\mathfrak{A},\mathfrak{B})$ aus $I_\omega(\mathfrak{A},\mathfrak{B})$ definieren: $p \in I_{\omega+1}(\mathfrak{A},\mathfrak{B})$ wenn für alle $a \in A$ (bzw. $b \in B$) ein $b \in B$ (bzw. $a \in A$) existiert mit $p \cup \{(a,b)\} \in I_\omega(\mathfrak{A},\mathfrak{B})$.

Für das vorliegende Beispiel folgt: $I_{\omega+1}(\mathfrak{A},\mathfrak{B}) = \{\varnothing\}$, $I_{\omega+2}(\mathfrak{A},\mathfrak{B}) = \varnothing$.

Kapitel 2

Syntax und Semantik der Prädikatenlogik

2.1 Syntax der Prädikatenlogik

Terme und Formeln sind *syntaktische Objekte*, d.h. Wörter in einer formalen Sprache. 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 $\mathrm{VAR} = \{v_0, v_1, v_2, \dots\}$ von *Variablen*;
- dem *Gleichheitszeichen* $=$,
- den *aussagenlogischen Junktoren* $\neg, \wedge, \vee, \rightarrow$ und $\leftrightarrow$,
- 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 2.1. Die Menge $T(\tau)$ der *τ-Terme* ist induktiv wie folgt definiert:

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

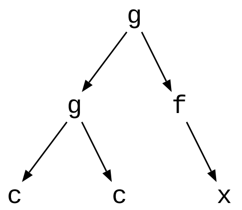
(2) Sind $t_1, \dots, t_n$ τ-Terme und $f \in F^n(\tau)$, so ist auch $ft_1 \cdots t_n$ ein τ-Term.

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

Beispiel. Die Signatur τ enthalte die Funktionssymbole $f \in F^1(\tau)$, $g \in F^2(\tau)$ und $c \in F^0(\tau)$. Sei $x \in \text{VAR}$ 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 $\text{Alph}(\tau)^*$ kann auf höchstens eine Weise als ein Term aufgefasst werden. Um dies nachzuweisen, zeigt man zunächst per Induktion über den Termaufbau, dass kein τ-Term ein echtes Anfangsstück eines andern τ-Terms sein kann. Daraus folgt, dass für jeden Term $ft_1 \cdots t_n$ die unmittelbaren Unterterme $t_1, \dots, t_n$ eindeutig bestimmt sind.

Definition 2.2. Die Menge $\text{FO}(\tau)$ 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 $t_1, \dots, t_n$ Terme aus $T(\tau)$ und ist $P \in \tau$ ein n -stelliges Relationssymbol, dann ist $Pt_1 \cdots t_n$ eine τ-Formel.

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

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

(5) Wenn ψ eine τ-Formel ist und $x \in \text{VAR}$ eine Variable, dann sind $\exists x\psi$ und $\forall x\psi$ τ-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". Die Formel $(\psi \leftrightarrow \varphi)$ heisst die *Bi-Implikation* oder *Äquivalenz* von ψ und φ, gelesen "ψ äquivalent φ" oder "ψ genau dann, wenn φ". Die Formeln $\exists x\psi$ bzw. $\forall x\psi$ lesen wir "es gibt ein x, so dass ψ" bzw. "für alle x, ψ". Obwohl die Leseweise der Formeln natürlich auf ihre Semantik (Bedeutung) anspielen, sind die Formeln bis jetzt als rein syntaktische Objekte, als Wörter in einer formalen Sprache aufzufassen.

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

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

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

Konventionen zur Notation von Formeln. Zur Vesserung der Lesbarkeit bedienen wir uns abkürzender oder vereinfachender Schreibweisen. Zum Beispiel bezeichnen wir in der Regel Variablen anstelle von $v_0, v_1, \dots$, mit andern Symbolen, etwa $x, y, z, x_0, x_1, \dots$. Für Terme, die aus Funktionssymbolen wie $+$, $\cdot$, $\circ$ etc. gebildet werden, verwenden wir in der Regel die Infix-Notation $x + y$ statt $+xy$; ähnliches gilt für Atome wie etwa $t_1 < t_2$ oder gelegentlich auch xEy. Anstelle von $\neg\, t_1 = t_2$ schreiben wir $t_1 \neq t_2$. Wo dies für die Lesbarkeit nützlich ist, werden wir von der klammerfreien Notation von Termen abweichen: So ist etwa $g(fx, g(x, ffy))$ als anschaulichere Beschreibung des Terms $gfxgxffy$ zu verstehen. Zum Beispiel schreiben wir $x + (y + z) = (x + y) + z$ anstelle von $+x + yz = ++xyz$. Andererseits werden wir in Formeln oft Klammern weglassen, welche für das Verständnis überflüssig sind. Wir vereinbaren, dass $\wedge$ und $\vee$ stärker binden als $\rightarrow$ und $\leftrightarrow$. So steht etwa $\psi \wedge \neg\varphi \rightarrow \vartheta$ für $((\psi \wedge \neg\varphi) \rightarrow \vartheta)$ Ausserdem vereinbaren wir Linksklammerung bei iterierten Disjunktionen und Konjunktionen: $\psi \wedge \varphi \wedge \eta$ steht für $((\psi \wedge \varphi) \wedge \eta)$.

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 später folgende 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.

Beweisprinzip der Induktion über den Formelaufbau. Der induktive Aufbau von Termen und Formeln erlaubt das Prinzip der strukturellen Induktion für Definitionen und Beweise.

Induktionsbeweise über den Formelaufbau folgen folgendem Muster. Um nachzuweisen, dass alle Formeln in $\mathrm{FO}(\tau)$ eine Eigenschaft E besitzen, zeigt man:

(1) Alle atomaren Formeln in $\mathrm{FO}(\tau)$ haben die Eigenschaft E.

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

(3) Hat $\psi \in \mathrm{FO}(\tau)$ die Eigenschaft E, dann auch alle Formeln der Form $\exists x\psi$, $\forall x\psi$ für $x \in \mathrm{VAR}$.

Mit diesem Beweisprinzip kann man (wie bei Termen) leicht die *eindeutige Lesbarkeit von Formeln* einsehen: Keine Formel ist ein echtes Anfangsstück einer andern Formel und daher kann man jede Formel auf genau eine Weise gemäss den Regeln (1) – (5) von Definition 2.2 in ihre unmittelbaren Bestandteile zerlegen.

Daraus folgt insbesondere, dass induktive Definitionen über den Formelaufbau eindeutig sind: So können wir etwa für jede Formel $\psi \in \mathrm{FO}(\tau)$ die Menge $\mathrm{UF}(\psi)$ ihrer Unterformeln induktiv wie folgt definieren.

$$\begin{aligned}
\mathrm{UF}(\psi) &:= \{\psi\} && \text{wenn } \psi \text{ atomar,}\\
\mathrm{UF}(\neg\psi) &:= \{\neg\psi\} \cup \mathrm{UF}(\psi), &&\\
\mathrm{UF}((\psi \circ \varphi)) &:= \{(\psi \circ \varphi)\} \cup \mathrm{UF}(\psi) \cup \mathrm{UF}(\varphi) && \text{für } \circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\},\\
\mathrm{UF}(\exists x\psi) &:= \{\exists x\psi\} \cup \mathrm{UF}(\psi), &&\\
\mathrm{UF}(\forall x\psi) &:= \{\forall x\psi\} \cup \mathrm{UF}(\psi). &&
\end{aligned}$$

Übung 2.1. 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 (4) in Definition 2.2 wird dabei ersetzt durch

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

Man zeige andererseits, dass die eindeutige Lesbarkeit nicht mehr gewährleistet ist wenn in Definition 2.2 die Klammern einfach weggelassen werden, d.h. wenn mit ψ und φ auch die Ausdrücke $\psi \wedge \varphi$, $\psi \vee \varphi$, $\psi \rightarrow \varphi$ und $\psi \leftrightarrow \varphi$ als Formeln zugelassen werden.

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

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

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

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

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

Definition 2.3. Sei $t \in T(\tau)$ ein Term und $\psi \in \mathrm{FO}(\tau)$ eine Formel. Mit $\mathrm{Var}(t)$ bzw. $\mathrm{Var}(\psi)$ bezeichnen wir die Menge aller in t bzw. ψ auftretenden Variablen. Die Menge $\mathrm{Frei}(\psi)$ der freien Variablen von ψ ist induktiv wie folgt definiert:

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

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

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

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

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

Mächtigkeit von $\mathbf{T}(\tau)$ und $\mathbf{FO}(\tau)$. Wenn τ abzählbar ist, dann auch das Alphabet $\text{Alph}(\tau)$. Nach Übung 1.1 folgt dann, dass auch $\text{Alph}(\tau)^*$, und damit inbesondere $T(\tau)$ und $\text{FO}(\tau)$ abzählbar sind. Andererseits sind $T(\tau)$ und $\text{FO}(\tau)$ auch bei endlicher Signatur τ (sogar bei $\tau = \emptyset$) unendlich. In der Tat enthält $T(\tau)$ alle Variablen und $\text{FO}(\tau)$ alle Formeln $x = y$ für $x, y \in \text{VAR}$.

2.2 Semantik der Prädikatenlogik

Die Modellbeziehung.

Definition 2.4. Sei τ eine Signatur. Eine τ-*Interpretation* ist ein Paar $\mathfrak{I} = (\mathfrak{A}, \beta)$ wobei $\mathfrak{A}$ eine τ-Struktur und $\beta : X \to A$ eine Belegung von Variablen durch Elemente von A ist. Dabei ist $X = \text{Def}(\beta) \subseteq \text{VAR}$. Eine τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ ordnet

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

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

Interpretation von Termen.

(1) Für $x \in \text{Def}(\beta)$ ist $x^{\mathfrak{I}} := \beta(x)$.

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

Interpretation von Formeln.

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

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

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

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

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

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

(9) $\mathfrak{I}(\psi \leftrightarrow \varphi) := \mathfrak{I}((\psi \to \varphi) \wedge (\varphi \to \psi)) = \begin{cases} 1 & \text{wenn } \mathfrak{I}(\psi) = \mathfrak{I}(\varphi) \\ 0 & \text{sonst.} \end{cases}$

Um $\mathfrak{I}(\exists x\psi)$ und $\mathfrak{I}(\forall x\psi)$ 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 $\beta[x/a] : X \cup \{x\} \to A$ mit $\beta[x/a](y) := \beta(y)$ für $y \neq x$ und $\beta[x/a](x) := a$. Für $\mathfrak{I} = (\mathfrak{A}, \beta)$ setzen wir $\mathfrak{I}[x/a] := (\mathfrak{A}, \beta[x/a])$. Wir definieren nun

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

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

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

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

Lemma 2.5 (Koinzidenzlemma). *Sei* $\psi \in \mathrm{FO}(\sigma \cap \tau)$, $(\mathfrak{A}, \beta)$ *eine* σ*-Interpretation und* $(\mathfrak{A}', \beta')$ *eine* τ*-Interpretation, so dass folgendes gilt:*

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

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

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

Notation. Wie erwähnt, deuten wir mit der Notation $\psi(x_1, \ldots, x_k)$ 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 $\mathrm{Frei}(\psi) = \varnothing$) so schreiben wir $\mathfrak{A} \models \psi$ und nennen $\mathfrak{A}$ ein Modell von ψ.

Beispiel. Sei $\psi := \exists z(Exz \wedge Ezy)$ und $\varphi := \forall x \forall y(Exy \to \psi)$. 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 $(Exy \rightarrow \psi)$ falsch in $\mathfrak{A}$ (2 ist echter Teiler von 4, aber es gibt keine Zahl, welche echt von 2 geteilt wird und ihrerseits 4 echt teilt). Hingegen ist $(\mathbb{Q}, <)$ ein Modell von φ, da $\mathbb{Q}$ dicht geordnet ist.

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

Definition 2.6. Sei Φ eine Menge von τ-Sätzen. Die *Modellklasse von* Φ (kurz: $\mathrm{Mod}(\Phi)$) besteht aus aus allen τ-Strukturen $\mathfrak{A}$ mit $\mathfrak{A} \models \Phi$. Eine Klasse $\mathcal{K}$ von τ-Strukturen ist *axiomatisiert durch* Φ, wenn $\mathcal{K} = \mathrm{Mod}(\Phi)$. Wir nennen Φ dann ein *Axiomensystem* für $\mathcal{K}$.

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

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

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

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

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

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

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

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

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

2.3 Die Folgerungsbeziehung.

Definition 2.7. (Semantische Folgerungsbeziehung) Sei $\Phi \subseteq \mathrm{FO}(\tau)$ eine Formelmenge, $\psi \in \mathrm{FO}(\tau)$ eine Formel. Wir sagen, ψ *folgt aus* Φ (kurz: $\Phi \models \psi$) genau dann, wenn jede zu $\Phi \cup \{\psi\}$ passende Interpretation, welche Modell von Φ ist, auch Modell von ψ ist. Wenn $\Phi = \{\varphi\}$ schreiben wir auch $\varphi \models \psi$ anstelle von $\{\varphi\} \models \psi$.

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

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

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

Definition 2.8. Hat eine Formel ψ (bzw. eine Formelmenge Φ) ein Modell, so heisst ψ (bzw. Φ) *erfüllbar*, andernfalls *unerfüllbar*. Eine Formel ψ heisst *allgemeingültig* oder eine *Tautologie* (kurz: $\models \psi$) wenn jede zu ψ passende Interpretation ein Modell von ψ ist. Dies ist äquivalent zur Aussage, dass ψ aus der leeren Formelmenge folgt. Zwei Formeln ψ und φ heissen *logisch äquivalent* (kurz: $\psi \equiv \varphi$), wenn $\psi \models \varphi$ und $\varphi \models \psi$.

Hier sind ein paar einfache logische Äquivalenzen. Der Nachweis ergibt sich unmittelbar aus der Definition der Modellbeziehung.

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

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

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

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

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

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

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

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

Wir formulieren einige einfache Eigenschaften der Folgerungsbeziehung.

Lemma 2.9. *Seien $\Phi \subseteq \mathrm{FO}(\tau)$ $\quad \psi, \varphi \in \mathrm{FO}(\tau)$ Dann gilt:*

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

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

(iii) $\psi \equiv \varphi$ *genau dann, wenn* $\models \psi \leftrightarrow \varphi$.

(iv) Wenn $\Phi \models \psi$ *dann gilt auch* $\Phi \cup \Phi' \models \psi$ *für jede Formelmenge* Φ'.

(v) ψ *ist erfüllbar genau dann, wenn* $\neg\psi$ *keine Tautologie ist.*

(vi) Φ *ist unerfüllbar genau dann, wenn* $\Phi \models \psi$ *für alle* $\psi \in \mathrm{FO}(\tau)$.

Definition 2.10. Sei ψ eine Formel mit freien Variablen $x_1, \ldots, x_k$. 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 2.11. *(i) Eine Formel ist erfüllbar genau dann, wenn ihr existentieller Abschluss erfüllbar ist.*

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

2.4 Termalgebren

Sei τ eine Signatur und τ_f ihr funktionaler Teil (den wir aus τ durch weglassen der Relationssymbole erhalten). Für jede Variablenmenge $X \subseteq \mathrm{VAR}$ bezeichnen wir mir $T(\tau, X)$ die Menge aller τ-Terme mit Variablen aus X. Offensichtlich ist $T(\tau, X) = T(\tau_f, X)$ für alle X und $T(\tau) = T(\tau_f) = T(\tau_f, \mathrm{VAR})$.

Für jede funktionale Signatur σ können wir die Termmenge $T(\sigma, X)$ selbst als das Universum einer σ-Algebra $\mathfrak{T}(X)$ auffassen, indem wir die Funktionssymbole durch ihre natürliche Operation auf den Termen interpretieren. Dies bedeutet, dass für $f \in F^n(\sigma)$ und $t_1, \dots, t_n \in T(\sigma, X)$

$$f^{\mathfrak{T}(X)}(t_1, \dots, t_n) := ft_1 \cdots t_n.$$

Satz 2.12. *Zu jeder σ-Algebra $\mathfrak{A}$ und jeder Abbildung $\rho : X \to A$ gibt es genau eine Fortsetzung von ρ zu einem Homomorphismus $\overline{\rho} : \mathfrak{T}(X) \to \mathfrak{A}$.*

Beweis. Eine Fortsetzung von ρ zu einem Homomorphismus $\overline{\rho} : \mathfrak{T}(X) \to \mathfrak{A}$ muss folgende Bedingungen erfüllen:

$$\begin{aligned} \overline{\rho}(x) &= \rho(x) \quad \text{für } x \in X. && \text{(Fortsetzung von } \rho) \\ \overline{\rho}(ft_1 \cdots t_n) &= f^{\mathfrak{A}}(\overline{\rho}t_1, \dots, \overline{\rho}t_n) && \text{(Homomorphiebedingung).} \end{aligned}$$

Andererseits ist durch diese Bedingungen eine eindeutige, induktive Definition eines Homomorphismus $\overline{\rho} : \mathfrak{T}(X) \to \mathfrak{A}$ formuliert. □

Beispiel. Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine τ-Interpretation mit $\mathrm{Def}(\beta) = X$ und sei $\sigma = \tau_f$ der funktionale Teil von τ. Die Interpretationsfunktion $t \mapsto t^{\mathfrak{I}}$ auf den Termen ist nichts anderes als die Erweiterung von $\beta : X \to A$ zum eindeutig bestimmten Homomorphismus von $\mathfrak{T}(X)$ nach $(\mathfrak{A} \restriction \sigma)$ (dem funktionalen Redukt von $\mathfrak{A}$).

Sei $\pi : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus von σ-Algebren, $\rho : X \to A$ eine Abbildung und $\overline{\rho} : \mathfrak{T}(X) \to \mathfrak{A}$ der eindeutig bestimmte Homomorphismus, welcher ρ fortsetzt. Dann ist $\pi \circ \overline{\rho} : \mathfrak{T}(X) \to \mathfrak{B}$ ein Homomorphismus. Andererseits können wir auch die Abbildung $\pi \circ \rho : X \to B$ zu einem Homomorphismus $\overline{\pi \circ \rho} : \mathfrak{T}(X) \to \mathfrak{B}$ fortsetzen. Da aber $\pi \circ \overline{\rho}$ und $\overline{\pi \circ \rho}$ auf X übereinstimmen, folgt wegen der Eindeutgkeit der Fortsetzung, dass $\pi \circ \overline{\rho} = \overline{\pi \circ \rho}$. Damit ist gezeigt:

Lemma 2.13. *Für jeden Homomorphismus $\pi : \mathfrak{A} \to \mathfrak{B}$ und jede Abbildung $\rho : X \to A$ gilt: $\pi \circ \overline{\rho} = \overline{\pi \circ \rho}$.*

$$\begin{tikzcd} X \arrow[r, "\rho"] & \mathfrak{A} \arrow[dr, "\pi"] & \\ \mathfrak{T}(X) \arrow[ur, "\overline{\rho}"] \arrow[rr, "\overline{\pi \circ \rho}"'] & & \mathfrak{B} \end{tikzcd}$$

Anwendung. Aus einer Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ und einem Homomorphismus $\pi : \mathfrak{A} \to \mathfrak{B}$ können wir eine neue Interpretation $\mathfrak{I}^\pi := (\mathfrak{B}, \pi \circ \beta)$ definieren. Wie im letzten Beispiel erläutert, sind die Interpretationsfunktionen $t \mapsto t^{\mathfrak{I}}$ bzw. $t \mapsto t^{\mathfrak{I}^\pi}$ gerade die eindeutig bestimmten Erweiterungshomomorphismen von β bzw. von $\pi \circ \beta$. Aus dem Lemma 2.13 folgt daher sofort:

Satz 2.14. *Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine τ-Interpretation, $\pi : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus, und $\mathfrak{I}^\pi$ die Interpretation $(\mathfrak{B}, \pi \circ \beta)$. Dann gilt für jeden Term $t \in T(\tau, X)$: $t^{\mathfrak{I}^\pi} = \pi(t^{\mathfrak{I}})$.*

2.5 Substitution

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

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

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

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

Definition 2.15. Eine Substitution ist eine Funktion $\rho : \mathrm{VAR} \to T(\tau)$. In der Regel wird voraussgesetzt, dass ρ *endlichen Support* hat, d.h. dass ρ alle bis auf endliche viele $x \in \mathrm{VAR}$ fest lässt. Wir bezeichnen eine Substitution, welche die Variablen $x_1, \ldots, x_k$ auf die Terme $t_1, \ldots, t_k$ abbildet und alle andern Variablen fest lässt, auch in der Form $x_1/t_1, \ldots, x_k/t_k$.

Operation auf Termen. Eine Substitution kann auf eindeutige Weise zu einem Homorphismus $\overline{\rho} : T(\tau) \to T(\tau)$ fortgesetzt werden. Wir bezeichnen das Resultat der Anwendung von $\overline{\rho}$ auf t mit $t[\rho]$. Offensichtlich ist $ft_1 \cdots t_n[\rho] = ft_1[\rho] \cdots t_n[\rho]$.

Operation auf Formeln. Zur Definition der Operation einer Substititution auf einer Formel führen wir folgenden Begriff ein. Eine Formel der Form $\exists x\psi$ und eine Substitution ρ sind *konfliktfrei* wenn keine Variable $y \in \text{Frei}(\exists x\psi)$ existiert, so dass x im Term $\rho(y)$ vorkommt. Mit ρ_x bezeichnen wir die Substitution, die x fest lässt und auf allen Variablen $y \neq x$ mit ρ übereinstimmt. Wir definieren induktiv die Transformation einer Formel $\psi \in \text{FO}(\tau)$ durch ρ in eine neue Formel welche wir mit $(\psi)[\rho]$ bezeichnen.

(1) Die Operation von ρ auf den Termen überträgt sich unmittelbar zur Operation auf Atomen:

$$\begin{aligned}(t_1 = t_2)[\rho] &:= t_1[\rho] = t_2[\rho]\\ (Pt_1 \cdots t_n)[\rho] &:= Pt_1[\rho] \cdots t_n[\rho].\end{aligned}$$

(2) Die Operation von ρ kommutiert mit den aussagenlogischen Junktoren, d.h. $(\neg\psi)[\rho] := \neg(\psi)[\rho]$ und $(\psi \circ \varphi)[\rho] := (\psi)[\rho] \circ (\varphi)[\rho]$ für $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

(3) Wenn $\exists x\psi$ und ρ konfliktfrei sind, dann ist $(\exists x\psi)[\rho] := \exists x(\psi)[\rho_x]$ (gebundene Variabeln werden nicht substituiert). Andernfalls sei z die erste Variable in VAR, die in ψ nicht vorkommt und für die $\exists z\psi[x/z]$ und ρ konfliktfrei sind; wir setzen dann $(\exists x\psi)[\rho] := \exists z(\psi)[\rho_x, x/z]$. Formeln der Form $\forall x\psi$ werden analog behandelt.

Beispiel. Sei $\psi := Rx_0x_2 \wedge \exists x_0(Rx_0x_1 \wedge Rx_0x_2)$ und sei ρ die Substitution $(x_0/x_4, x_1/c, x_2/gx_0x_0)$. Dann gilt

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

Sei τ eine Signatur und τ_f ihr funktionaler Teil. Jede τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ mit $\text{Def}(\beta) = X$ induziert einen Homomorphismus von $\mathfrak{T}(X)$ nach $(\mathfrak{A} \restriction \tau_f)$, welcher t auf $t^{\mathfrak{I}}$ abbildet. Sei nun $\rho = (x_1/t_1, \ldots, x_k/t_k)$ eine Substitution und sei $Y \subseteq \text{VAR}$ so, dass $\text{Var}(\rho(y)) \subseteq X$ für alle $y \in Y$ (d.h. Y enthält nur Variablen, deren Bild unter ρ im Definitionsbereich der Abbildung $\mathfrak{I} : t \mapsto t^{\mathfrak{I}}$ liegt). Wir können $\mathfrak{I}$ und ρ auf zwei verschiedene Arten zu einer Interpretationsfunktion auf $T(\tau, Y)$ zusammensetzen.

Einerseits ist $\mathfrak{I} \circ \rho = (\mathfrak{A}, \beta[x_1/t_1^{\mathfrak{I}}, \ldots, x_k/t_k^{\mathfrak{I}}])$ eine Interpretation über der Struktur $\mathfrak{A}$, welche Variablen $y \in Y$ durch $\rho(y)^{\mathfrak{I}}$ bewertet. Der induzierte Homomorphismus $\overline{\mathfrak{I} \circ \rho}$ ist die Interpretationsfunktion welche $t \in T(\tau, Y)$ auf $t^{\mathfrak{I} \circ \rho}$ abbildet.

Andererseits können wir direkt $\mathfrak{I}$ mit der durch ρ induzierten Operation $\overline{\rho}$ auf den Termen zusammensetzen und erhalten die Interpretationsfunktion

$$\begin{aligned}\mathfrak{I} \circ \overline{\rho} : \mathfrak{T}(Y) &\to (\mathfrak{A} \restriction \tau_f)\\ t &\mapsto t[\rho]^{\mathfrak{I}}.\end{aligned}$$

Da beide so erhaltetenen Interpretationsfunktionen die zu $\mathfrak{I} \circ \rho$ gehörende Belegung $\beta[x_1/t_1^{\mathfrak{I}}, \ldots, x_k/t_k^{\mathfrak{I}}])$ zu einem Homomorphismus von $\mathfrak{T}(Y)$ nach $(\mathfrak{A} \restriction \tau_f)$ erweitern, müssen sich nach Lemma 2.13 gleich sein. Also ist

$$t[\rho]^{\mathfrak{I}} = t[x_1/t_1, \ldots, x_k/t_k]^{\mathfrak{I}} = t^{\mathfrak{I}[x_1/t_1^{\mathfrak{I}}, \ldots, x_k/t_k^{\mathfrak{I}}]} = t^{\mathfrak{I} \circ \rho}.$$

$$\begin{tikzcd} Y \arrow[r, "\rho"] & \mathfrak{T}(X) \arrow[dr, "\mathfrak{I}"] & \\ \mathfrak{T}(Y) \arrow[ur, "\overline{\rho}"'] \arrow[rr, "\overline{\mathfrak{I}\circ\rho}"'] & & (\mathfrak{A} \restriction \tau_f) \end{tikzcd}$$

Eine analoge Aussage gilt auch für Formeln.

Lemma 2.16 (Substitutionslemma). *Für jede Formel $\psi \in \mathrm{FO}(\tau)$, jede Substitution $\rho : \mathrm{VAR} \to T(\tau)$ und jede zu $\psi[\rho]$ passende Interpretation $\mathfrak{I}$ gilt:*

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

Beweis. Der Beweis erfolgt per Induktion über den Formelaufbau. Aus der soeben bewiesenen Tatsache $t[\rho]^{\mathfrak{I}} = t^{\mathfrak{I}\circ\rho}$ für Terme folgt die Behauptung für Atomformeln ψ unmittelbar. Da der Substitutionsoperator mit den aussagenlogischen Junktoren kommutiert ist der Induktionsschritt für Formeln der Form $\neg\psi$ und $\psi \circ \varphi$ trivial. Betrachte nun eine Formel der Gestalt $\exists x\psi$. Für eine geignete Variable z ist $(\exists x\psi)[\rho] := \exists z(\psi)[\rho_x, x/z]$. Also gilt $\mathfrak{I} \models (\exists x\psi)[\rho]$ genau dann, wenn ein Element a existiert so dass $\mathfrak{I}[x_k/a] \models (\psi)[\rho, x/x_k]$ Nach der Induktionsvoraussetzung für ψ ist dies äquivalent zu der Aussage, dass $(\mathfrak{I}[z/a] \circ (\rho_x, x/z)) \models \psi$. Nun ist aber offensichtlich $\mathfrak{I}[z/a] \circ (\rho_x, x/z) = (\mathfrak{I} \circ \rho)[x/a]$. Also gilt $\mathfrak{I} \models (\exists x\psi)[\rho]$ genau dann, wenn ein Element a existiert so dass $(\mathfrak{I} \circ \rho)[x/a] \models \psi$, d.h. genau dann, wenn $(\mathfrak{I} \circ \rho) \models \exists x\psi$. Die Argumentation für Formeln der Form $\forall x\psi$ ist völlig analog. $\square$

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

2.6 Normalformen

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

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 Erfüllbarkeitsäquivalenz.

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

Lemma 2.17 (Ersetzungslemma). *Für beliebige Formeln $\psi, \psi', \varphi, \varphi'$ gilt:*

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

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

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

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

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

Reduzierte Formeln. Aus der Definition der Modellbeziehung ergibt sich sofort, dass für beliebige Formeln ψ, φ folgende Äquivalenzen gelten.

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

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

(3) $\psi \leftrightarrow \varphi \equiv (\neg\psi \wedge \neg\varphi) \vee (\psi \wedge \varphi) \equiv \neg(\psi \vee \varphi) \vee \neg(\neg\psi \vee \neg\varphi)$

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

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

Lemma 2.18. *Zu jeder Formel $\psi \in \mathrm{FO}(\tau)$ kann man effektiv eine logisch äquivalente reduzierte Formel konstruieren.*

Wir können daher im folgenden für alle semantischen Aussagen die Betrachtung auf reduzierte Formeln beschränken. Der Vorteil der Verwendung reduzierter Formeln liegt darin, dass sie aus weniger Symbole aufgebaut sind, und daher konzisere Definitionen und kürzere Induktionsbeweise erlauben.[1] Ein Nachteil reduzierter Formeln ist, dass sie länger und schlechter lesbar werden (siehe etwa die reduzierte Form von $(\psi \leftrightarrow \varphi)$).

Termreduzierte Formeln. Eine zweite Normalform, welche insbesondere für die Elimination von Funktionen nützlich ist (siehe Kapitel 4.5) betrifft die Komplexität der darin auftreteneden Terme. Eine Formel heisst *termreduziert* , wenn sie nur Atome der Form $R\bar{x}$, $f\bar{x} = y$ und $x = y$ enthält (also insbesondere keine Terme der Tiefe ≥ 2).

Lemma 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 $R \cdots t \cdots$, oder $t = t'$, oder als Subterm eines komplizierteren Terms). Führe eine neue Variable x_t ein und ersetze jedes Atom α, das t an einer verbotenen Stelle enthält, durch $\exists x_t(x_t = t \wedge \alpha[t/x_t])$ wobei $\alpha[t/x_t]$ die Formel sein soll, die man durch Ersetzten von t durch x_t gewinnt. Offensichtlich ist die modifierte Formel logisch äquivalent zu ψ. Dieser Eliminationsschritt wird solange ausgeführt, bis ψ termreduziert ist. □

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

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

Lemma 2.20.

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

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

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

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

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

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

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

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

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

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

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

Definition 2.21. Eine Formel ist in *Pränex-Normalform* (PNF), wenn sie bereinigt ist und die Form $Q_1 x_1 \cdots Q_r x_r \varphi$ hat, wobei φ quantorenfrei ist und $Q_i \in \{\exists, \forall\}$. Das Anfangsstück $Q_1 x_1 \cdots Q_r x_r$ nennt man das *Präfix* der Formel.

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 die Junktoren $\rightarrow$ und $\leftrightarrow$ nicht enthält.

(1) Quantorenfreie Formeln sind bereits in PNF.

(2) Sei $\psi = \neg\varphi$. Nach Induktionsvoraussetzung kann φ in eine logisch äquivalente Formel $\varphi' = Q_1 x_1 \cdots Q_r x_r \vartheta'$ 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.

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

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

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 $\psi \equiv \psi'$.

(4) 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.

□

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 2.2. 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) $\exists y Rxy \leftrightarrow \forall x Rxx$

Definition 2.23. Zwei Formeln ψ und φ heissen *erfüllbarkeitsäquivalent*, wenn entweder beide erfüllbar oder beide unerfüllbar sind.

Satz 2.24 (Satz über die Skolem-Normalform). *Zu jeder Formel $\psi \in \mathrm{FO}(\sigma)$ lässt sich eine Formel $\varphi \in \mathrm{FO}(\tau)$ mit $\sigma \subseteq \tau$ konstruieren, so dass gilt:*

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

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

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

(iv) Wenn ψ erfüllbar ist, dann auch φ.

Die letzten beiden Punkte implizieren insbesondere, dass ψ und φ erfüllbarkeitsäquivalent sind.

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

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

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

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

Offensichtlich liefert die Iteration dieses Eliminationsschrittes schliesslich eine Formel der gewünschten syntaktischen Gestalt. Zu zeigen bleibt, dass $\psi' \models \psi$ und dass die Erfüllbarkeit von ψ auch die Erfüllbarkeit von ψ' impliziert.

Zur ersten Behauptung nehmen wir an, dass

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

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

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

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

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

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

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

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

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

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

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

also nach dem Substitutionslemma auch

$$(\mathfrak{B}, \beta)[x_1/a_1, \ldots, x_k/a_k] \models \eta[x_{k+1}/fx_1 \cdots x_k].$$

Damit ist gezeigt, dass $(\mathfrak{B}, \beta) \models \forall x_1 \cdots \forall x_k \eta[x_{k+1}/fx_1 \cdots x_k]$ und daher ψ' erfüllbar ist. □

Übung 2.3. (Relationale Skolem-Normalform) Zeigen Sie, dass zu jeder Formel $\psi \in \mathrm{FO}(\sigma)$ eine erfüllbarkeitsäquivalente, *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.

Kapitel 3

Aussagenlogik

3.1 Syntax und Semantik der Aussagenlogik

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

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

Syntax. Die *Aussagenlogik* (AL) kann als das Fragment der Prädikatenlogik aufgefasst werden, in dem nur Aussagenvariablen (d.h. 0-stellige Relationssymbole) aber keine Funktionen, keine Relationssymbole mit positiver Stelligkeit und keine Gleichheit vorkommen. Daher gibt es in der Aussagenlogik auch keine Variablen, Terme und Quantoren.

Definition 3.1. Wir fixieren eine abzählbare Menge $\tau = \{X_0, X_1, X_2, \dots\}$ von *Aussagenvariablen*. 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 $\psi \in \mathrm{AL}$, dann auch $\neg\psi \in \mathrm{AL}$.

(4) Wenn $\psi, \varphi \in \mathrm{AL}$, dann sind auch $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$, $(\psi \rightarrow \varphi)$ und $(\psi \leftrightarrow \varphi)$ Formeln aus AL.

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

Semantik. Eine *(aussagenlogische) Interpretation* ist eine Abbildung $\mathfrak{I} : \sigma \rightarrow \{0, 1\}$ für $\sigma \subseteq \tau$. Diese definiert für jede Formel $\psi \in \mathrm{AL}$ mit $\tau(\psi) \subseteq \sigma$ einen Wahrheitswert $\mathfrak{I}(\psi) \in \{0, 1\}$, durch die folgenden Festlegungen:

(1) $\mathfrak{I}(0) = 0,\ \mathfrak{I}(1) = 1.$

(2) $\mathfrak{I}(\neg\psi) := 1 - \mathfrak{I}(\psi).$

(3) $\mathfrak{I}(\psi \wedge \varphi) := \min(\mathfrak{I}(\psi), \mathfrak{I}(\varphi))$

(4) $\mathfrak{I}(\psi \vee \varphi) := \max(\mathfrak{I}(\psi), \mathfrak{I}(\varphi)).$

(5) $\mathfrak{I}(\psi \rightarrow \varphi) := \mathfrak{I}(\neg\psi \vee \varphi).$

(6) $\mathfrak{I}(\psi \leftrightarrow \varphi) := \mathfrak{I}((\psi \rightarrow \varphi) \wedge (\varphi \rightarrow \psi)).$

Diese Definition entspricht völlig der Semantik der Prädikatenlogik, angewandt auf den Spezialfall einer nur aus 0-stelligen Relationssymbolen bestehenden Signatur.

Notation: In diesem Kapitel stehen kleine griechische Buchstaben $\psi, \varphi, \vartheta, \dots$ immer für aussagenlogische Formeln, grosse griechische Buchstaben Φ, Γ für Mengen aussagenlogischer Formeln. Wir verwenden die Schreibweise $\psi(X_1, \dots, X_n)$ um anzudeuten, dass $\tau(\psi) \subseteq \{X_1, \dots, X_n\}$. Sei $\mathfrak{I}(X_1) = \varepsilon_1, \dots, \mathfrak{I}(X_n) = \varepsilon_n$. Dann schreiben wir auch $\psi[\varepsilon_1, \dots, \varepsilon_n]$ oder $\psi[\bar{\varepsilon}]$ für $\mathfrak{I}(\psi)$.

Für Formelmengen $\Phi \in$ AL ist $\mathfrak{I}(\Phi) := \min_{\varphi \in \Phi} \mathfrak{I}(\varphi)$. Die Begriffe *Modell, Folgerung, Tautologie* und *Erfüllbarkeit* ergeben sich als Spezialfälle der entsprechenden Begriffe der Prädikatenlogik:

- Ein Modell von ψ ist eine Interpretation $\mathfrak{I} : \tau(\psi) \rightarrow \{0,1\}$ mit $\mathfrak{I}(\psi) = 1$.
- $\Phi \models \psi$ bedeutet, dass jede Interpretation $\mathfrak{I} : \tau(\Phi \cup \{\psi\}) \rightarrow \{0,1\}$, welche Modell von Φ ist, auch ein Modell von ψ ist.
- ψ ist eine (aussagenlogische) Tautologie, wenn $\mathfrak{I}(\psi) = 1$ für alle $\mathfrak{I} : \tau(\psi) \rightarrow \{0,1\}$.
- ψ ist erfüllbar, wenn es ein $\mathfrak{I} : \tau(\psi) \rightarrow \{0,1\}$ gibt, mit $\mathfrak{I}(\psi) = 1$.

Übung 3.1. Beweisen Sie das *aussagenlogische Interpolationstheorem*: Sei $\psi \rightarrow \varphi$ eine aussagenlogische Tautologie. Dann existiert eine aussagenlogische Formel ϑ mit $\tau(\vartheta) \subseteq \tau(\psi) \cap \tau(\varphi)$, so dass $\psi \rightarrow \vartheta$ und $\vartheta \rightarrow \varphi$ Tautologien sind. Hinweis: Führen Sie einen Induktionsbeweis über die Anzahl der Aussagenvariablen, die in ψ, aber nicht in φ vorkommen.

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

Satz 3.3. *Zu jeder Formel* $\psi \in$ AL *gibt es äquivalente Formeln* ψ_D *in* DNF *und* ψ_K *in* KNF.

Beweis. Sei $\mathfrak{I} : \tau(\psi) \to \{0,1\}$ eine Interpretation. Für jedes $X \in \tau(\psi)$ definieren wir

$$X^{\mathfrak{I}} = \begin{cases} X & \text{falls } \mathfrak{I}(X) = 1 \\ \neg X & \text{falls } \mathfrak{I}(X) = 0 \end{cases} \qquad \varphi^{\mathfrak{I}} = \bigwedge_{X \in \tau(\psi)} X^{\mathfrak{I}}.$$

Da $\mathfrak{I}(X^{\mathfrak{I}}) = 1$ für alle $X \in \tau(\psi)$ folgt $\mathfrak{I}(\varphi^{\mathfrak{I}}) = 1$. Für alle von $\mathfrak{I}$ verschiedenen Interpretationen $\mathfrak{I}' : \tau(\psi) \to \{0,1\}$ gibt es ein X mit $\mathfrak{I}'(X) \neq \mathfrak{I}(X)$, also $\mathfrak{I}'(X^{\mathfrak{I}}) = 0$ und somit $\mathfrak{I}'(\varphi^{\mathfrak{I}}) = 0$. Damit ist gezeigt, dass für alle Interpretationen $\mathfrak{I}, \mathfrak{I}' : \tau(\psi) \to \{0,1\}$ gilt:

$$\mathfrak{I}'(\varphi^{\mathfrak{I}}) = 1 \iff \mathfrak{I}' = \mathfrak{I}. \tag{*}$$

Sei nun $M(\psi)$ die Menge aller (aussagenlogischen) Modelle von ψ und

$$\psi_D := \bigvee_{\mathfrak{I} \in M(\psi)} \varphi^{\mathfrak{I}} = \bigvee_{\mathfrak{I} \in M(\psi)} \bigwedge_{X \in \tau(\psi)} X^{\mathfrak{I}}.$$

Offensichtlich ist ψ_D in disjunktiver Normalform. Sei $\mathfrak{I}' : \tau(\psi) \to \{0,1\}$ eine beliebige Interpretation. Es gilt

$$\begin{aligned} \mathfrak{I}'(\psi_D) = 1 &\iff \mathfrak{I}'(\varphi^{\mathfrak{I}}) = 1 \quad \text{für ein } \mathfrak{I} \in M(\psi) \\ &\iff \mathfrak{I}' \in M(\psi) \quad (\text{wegen } (*)). \end{aligned}$$

Also ist $\psi_D \equiv \psi$.

Die 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. □

Bemerkung. Es gibt 2^n Interpretationen für Formeln mit n Aussagenvariablen. Die im Beweis konstruierten Formeln ψ_D bzw. ψ_K können also exponentiell länger werden als ψ. Sie sind im Allgemeinen nicht die kürzesten zu ψ äquivalenten Formeln in DNF bzw. KNF. Als Beispiel betrachte man $\psi = X_1 \wedge (X_2 \vee \neg X_2) \wedge \cdots \wedge (X_n \vee \neg X_n)$ in KNF. Die Formel ψ_D besteht aus einer Disjunktion über 2^{n-1} Teilformeln $\varphi^{\mathfrak{I}}$; offensichtlich ist aber ψ auch äquivalent zu einer sehr kurzen Formeln in DNF, nämlich zu X_1.

Übung 3.2. Eine aussagenlogische Formel ist in 3-KNF, wenn sie folgende Gestalt hat:

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

Zeigen Sie, dass es man zu jeder aussagenlogischen Formel eine erfüllbarkeitsäquivalente Formel in 3-KNF konstruieren kann. Hinweis: Man fasse überzählige Literale mit Hilfe neuer Aussagenvariablen zusammen.

3.2 Aussagenlogik und Boolesche Funktionen

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

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

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

Jede Formel $\psi(X_1, \dots, X_n) \in \mathrm{AL}$ definiert eine Boolesche Funktion $h_\psi \in B^n$, durch die Vorschrift $h_\psi(\varepsilon_1, \dots, \varepsilon_n) := \psi[\varepsilon_1, \dots, \varepsilon_n]$. Der folgende Satz zeigt, dass sich umgekehrt jede Boolesche Funktion durch eine aussagenlogische Formel darstellen lässt.

Satz 3.4. *Zu jeder Funktion $f \in B^n$ gibt es eine Formel $\psi(X_1, \dots, X_n)$ mit $f = h_\psi$.*

Beweis. Die Funktionen in B^0 werden durch die Formeln 0 und 1 dargestellt, die vier Funktionen in B^1 durch die Formeln $(X_1 \wedge \neg X_1), (X_1 \vee \neg X_1)$, X_1 und $\neg X_1$. Für den Induktionsschluss, sei $f \in B^{n+1}$. Wir erhalten zwei Funktionen $g_0, g_1 \in B^n$ durch $g_0(\overline{\varepsilon}) := f(\overline{\varepsilon}, 0)$ und $g_1(\overline{\varepsilon}) := f(\overline{\varepsilon}, 1)$, wobei $\overline{\varepsilon} \in \{0,1\}^n$. Nach Induktionsvoraussetzung gibt es Formeln $\psi_0(X_1, \dots, X_n)$ und $\psi_1(X_1, \dots, X_n)$ mit $h_{\psi_0} = g_0$ und $h_{\psi_1} = g_1$. Setze nun

$$\psi := (\psi_0 \wedge \neg X_{n+1}) \vee (\psi_1 \wedge X_{n+1}).$$

Diese Formel definiert f, denn es gilt

$$\psi[\overline{\varepsilon}, \varepsilon_{n+1}] = \begin{cases} \psi_0[\overline{\varepsilon}] & \text{wenn } \varepsilon_{n+1} = 0 \\ \psi_1[\overline{\varepsilon}] & \text{wenn } \varepsilon_{n+1} = 1 \end{cases} = \begin{cases} g_0(\overline{\varepsilon}) & \text{wenn } \varepsilon_{n+1} = 0 \\ g_1(\overline{\varepsilon}) & \text{wenn } \varepsilon_{n+1} = 1 \end{cases} = f(\overline{\varepsilon}, \varepsilon_{n+1})$$

□

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

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

Die im Beweis von Satz 3.4 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 3.5. Eine Menge $\Omega \subseteq B$ von Booleschen Funktionen heisst *funktional vollständig*, wenn sich daraus jede Boolesche Funktion $f : B^n \to B$ im Sinne von Satz 3.4 definieren lässt (für $n \geq 1$).

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

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

Es gibt aber noch weitere funktional vollständige Mengen:

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

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

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

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

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

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

Übung 3.3. Die Funktion $sel \in B^3$ sei definiert durch $sel(u, v, w) = v$, wenn $u = 0$ und $sel(u, v, w) = w$, wenn $u = 1$. Zeigen Sie, dass $\{sel, 0, 1\}$ funktional vollständig ist.

Übung 3.4. 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 3.5. Eine Boolesche Funktion $f \in B^n$ ist *linear*, wenn sie durch eine lineares Polynom $f(X_1, \dots, X_n) = a_0 + a_1X_1 + \dots + a_nX_n$ über dem Körper $\mathbb{F}_2$ beschrieben werden kann. Zeigen Sie, dass die meisten Booleschen Funktion nicht linear sind.

Übung 3.6. Die zu $f \in B^n$ *duale Funktion* ist definiert durch $f^\delta(x_1, \dots, x_n) := \neg f(\neg x_1, \dots, \neg x_n)$.

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

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

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

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.

3.3 Der Kompaktheitssatz der Aussagenlogik

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

Satz 3.6 (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* $\Phi_0 \models \psi$.

Beweis. Zu *(i):* Es ist klar, dass mit Φ auch jede endliche Teilmenge von Φ erfüllbar ist. Für die Umkehrung nehmen wir an, dass jedes endliche $\Phi_0 \subseteq \Phi$ erfüllbar ist und definieren induktiv ein Modell $\mathfrak{I}$ von Φ: Seien $\mathfrak{I}(X_0), \dots, \mathfrak{I}(X_{n-1})$ bereits festgelegt, und zwar so, dass folgende Bedingung erfüllt ist:

(B_n) Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ besitzt ein Modell $\mathfrak{I}'$ mit $\mathfrak{I}' \upharpoonright \{X_0, \dots, X_{n-1}\} = \mathfrak{I} \upharpoonright \{X_0, \dots, X_{n-1}\}$.

Wir zeigen, dass $\mathfrak{I}(X_n)$ so definiert werden kann, dass auch die Bedingung (B_{n+1}) erfüllt ist. Dazu setzen wir:

$$\mathfrak{I}(X_n) := 1, \text{ wenn jede endliche Teilmenge } \Phi_0 \subseteq \Phi \text{ ein Modell } \mathfrak{I}' \text{ besitzt mit } \mathfrak{I}' \upharpoonright \{X_0, \dots, X_{n-1}\} = \mathfrak{I} \upharpoonright \{X_0, \dots, X_{n-1}\} \text{ und } \mathfrak{I}'(X_n) = 1.$$
$$\mathfrak{I}(X_n) := 0, \text{ sonst.}$$

Wenn $\mathfrak{I}(X_n) = 1$, dann ist die Bedingung (B_{n+1}) offensichtlich erfüllt. Wenn $\mathfrak{I}(X_n) = 0$ dann gibt es eine endliche Teilmenge $\Phi_1 \subseteq \Phi$, so dass für jedes Modell $\mathfrak{I}'$ von Φ_1 gilt:

$$\mathfrak{I}' \upharpoonright \{X_0, \dots, X_{n-1}\} = \mathfrak{I} \upharpoonright \{X_0, \dots, X_{n-1}\} \implies \mathfrak{I}'(X_n) = 0.$$

Sei Φ_0 eine beliebige endliche Teilmenge von Φ. Dann ist auch $\Phi_0 \cup \Phi_1$ endlich und besitzt also gemäss (B_n) ein Modell $\mathfrak{I}'$ mit $\mathfrak{I}' \upharpoonright \{X_0, \dots, X_{n-1}\} = \mathfrak{I} \upharpoonright \{X_0, \dots, X_{n-1}\}$. Da $\mathfrak{I}'$ ein Modell von Φ_1 ist, gilt also $\mathfrak{I}'(X_n) = 0$. Also besitzt Φ_0 in der Tat ein Modell, das mit $\mathfrak{I}$ auf $X_0, \dots, X_n$ übereinstimmt, d.h., die Bedingung (B_{n+1}) ist erfüllt.

Sei $\mathfrak{I}$ die induktiv auf diese Weise konstruierte Interpretation. Es bleibt zu zeigen, dass $\mathfrak{I}$ tatsächlich ein Modell von Φ ist. Dies sehen wir wie folgt: Für jedes $\varphi \in \Phi$ gibt es ein n mit $\tau(\varphi) \subseteq \{X_0, \dots, X_n\}$. Da $\{\varphi\} \subseteq \Phi$ endlich ist, gibt es ein Modell $\mathfrak{I}'$ für $\{\varphi\}$, so dass $\mathfrak{I}' \upharpoonright \{X_0, \dots, X_n\} = \mathfrak{I} \upharpoonright \{X_0, \dots, X_n\}$. Da also $\mathfrak{I}'(\varphi) = 1$ und $\mathfrak{I}' \upharpoonright \tau(\varphi) = \mathfrak{I} \upharpoonright \tau(\varphi)$ gilt $\mathfrak{I}(\varphi) = 1$.

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

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

Lemma 3.7 (König). *Sei T ein endlich verzweigter Baum mit Wurzel w, in dem es beliebig lange endliche Wege gibt. Dann gibt es auch einen unendlichen Weg in T, der bei der Wurzel w beginnt.*

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

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

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

(1) $|W \cap S_n| = 1$ für alle n;

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

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

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

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

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

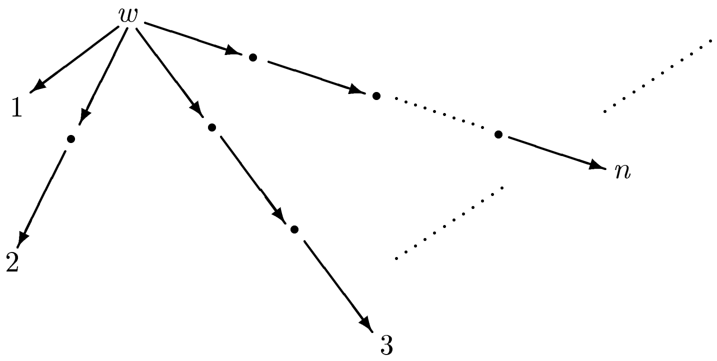
Offensichtlich ist $\mathfrak{I}(\Phi_0) = 1$. Mit dem Kompaktheitssatz folgt, dass es ein Modell $\mathfrak{I}$ für Φ gibt. Setze $W := \{v \in V : \mathfrak{I}(X_v) = 1\}$. Es folgt, dass W einen unendlichen Weg von w aus definiert:

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

(2) Sei $v \in W$ und $(u, v) \in E$. Da $\mathfrak{I}(X_v) = 1$ und $\mathfrak{I}(X_v \to X_n) = 1$ gilt auch $\mathfrak{I}(X_n) = 1$, also $u \in W$.

□

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



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

Übung 3.7. Ein ungerichteter Graph $G = (V, E)$ heisst *k-färbbar*, wenn es eine Funktion $f : V \to \{1, \ldots, k\}$ gibt, so dass $f(p) \neq f(q)$ für alle Kanten $(p, q) \in E$. Zeigen Sie, dass ein ungerichteter Graph G *k-färbbar* ist, wenn jeder endliche Untergraph von G *k-färbbar* ist. Hinweis: Konstruieren Sie zu jedem endlichen Untergraphen von G eine aussagenlogische Formel, die genau dann erfüllbar ist, wenn der Untergraph k-färbbar ist. Führen Sie dazu zu jedem Knoten $g \in V$ und jeder Farbe i, $1 \leq i \leq k$, eine Aussagenvariable $X_{g,i}$ ein, die besagt, dass der Knoten g die Farbe i hat.

Übung 3.8. (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, welche X nicht enthält, so dass $\Phi \models X \leftrightarrow \varphi$. (In Modellen von Φ ist also der Wahrheitswert von X durch eine Formel, die nicht von X abhängt, explizit festgelegt). Demgegenüber heisst X *implizit definierbar* in Φ, wenn für alle Modelle $\mathfrak{I}, \mathfrak{I}'$ von Φ gilt: Wenn $\mathfrak{I}(Z) = \mathfrak{I}'(Z)$ für alle Ausssagenvariablen $Z \neq X$, dann auch $\mathfrak{I}(X) = \mathfrak{I}'(X)$. (In Modellen von Φ ist also der Wahrheitswert von X durch die Wahrheitswerte der andern Variablen implizit festgelegt).

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

Hinweis: Die Formelmenge Φ' entstehe dadurch, dass man X in allen Formeln von Φ durch eine neue Aussagenvariable $X' \notin \tau(\Phi)$ ersetzt. Die implizite Definierbarkeit von X in Φ besagt dann, dass $\Phi \cup \Phi' \models X \leftrightarrow X'$. Benutzen Sie den Kompaktheitssatz um Φ durch eine endliche Formelmenge zu ersetzen und verwenden Sie das aussagenlogische Interpolationstheorem (Übung 3.1) um eine explizite Definition von X in Φ zu konstruieren.

***Der Kompaktheitssatz für überabzählbare Formelmengen.** Es gibt interessante Anwendungen der Aussagenlogik die von überabzählbar vielen Aussagenvariablen ausgehen. Der Beweis des Kompktheitssatzes muss dann aber anders geführt werden. Er basiert auf dem Lemma von Zorn.

Lemma 3.8 (Zorn). *Sei $(A, <)$ eine nicht-leere partielle Ordnung in der jede Kette nach oben beschränkt ist. Dann besitzt $(A, <)$ ein maximales Element.*

Wie skizzieren den Beweis des Kompaktheitssatz für überabzählbare Formelmengen. Sei Φ eine Menge aussagenlogischer Formeln, so dass jede endliche Teilmenge von Φ erfüllbar ist. Sei

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

A ist partiell geordnet durch die Inklusionsbeziehung und nicht leer (da $\Phi \in A$). Sei $K \subseteq A$ eine Kette, d.h. $\Theta \subseteq \Psi$ oder $\Psi \subseteq \Theta$ für alle $\Psi, \Theta \in K$. Offensichtlich ist $\Gamma := \bigcup K$, die Vereinigung aller Elemente von 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. Unter den endlich vielen Mengen $\Psi(\gamma)$ gibt es 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 $\Phi_{\max}$. Für jede Formel ψ ist entweder $\psi \in \Psi_{\max}$ oder $\neg\psi \in \Psi_{\max}$. Andernfalls betrachten wir die Erweiterungen $\Psi_{\max} \cup \{\psi\}$ und $\Psi_{\max} \cup \{\neg\psi\}$. Aufgrund der Maximalität von $\Psi_{\max}$ gehört keine dieser Mengen zu A. Also gibt es endliche Teilmengen $\Psi_0, \Psi_1 \subseteq \Psi_{\max}$ 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 $\Psi_{\max}$, im Widerspruch zu $\Psi_{\max} \in A$.

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

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

Per Induktion über den Formelaufbau zeigt man leicht, dass $\mathfrak{I}(\psi) = 1$ genau dann, wenn $\psi \in \Psi_{\max}$. Also ist $\mathfrak{I}$ ein Modell von $\Psi_{\max}$ und damit auch von Φ.

Damit ist der Kompaktheitssatz für überabzählbare Formelmengen bewiesen.

3.4 Der aussagenlogische Sequenzenkalkül

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

Definition 3.9. Eine *Sequenz* ist ein Ausdruck der Form $\Gamma \Rightarrow \Delta$ für endliche Formelmengen $\Gamma, \Delta \subseteq \mathrm{AL}$. Wir nennen Γ das *Antezedens* und Δ das *Sukzedens* der Sequenz $\Gamma \Rightarrow \Delta$.

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

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

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

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

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

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

Definition 3.10. Die *Axiome* von SK sind alle Sequenzen der Form $\Gamma, \psi \Rightarrow \Delta, \psi$. Die *Schlussregeln* von SK sind:

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

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

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

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

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

Definition 3.11. Die Menge der *ableitbaren Sequenzen* von SK ist die induktiv durch die Axiome und Schlussregeln definierte Sequenzenmenge, d.h. die kleinste Menge, welche alle Axiome umfasst und mit jeder Instanz der oberen Zeile einer Schlussregel auch die entsprechende Instanz der unteren Zeile enthält.

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

(1) Jedes Blatt ist mit einem Axiom beschriftet.

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

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

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

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

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

Übung 3.9. Beweisen Sie dieses Lemma.

Eine unmittelbare Konsequenz ist der Korrektheitssatz für SK.

Satz 3.13 (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 3.14. Sei $\Phi \subseteq$ AL eine Formelmenge. Eine aussagenlogische Formel ψ ist *ableitbar* aus der Hypothesenmenge Φ, (kurz: $\Phi \vdash \psi$), wenn eine endliche Teilmenge Γ von Φ existiert, so dass die Sequenz $\Gamma \Rightarrow \psi$ im Sequenzenkalkül ableitbar ist. Insbesondere ist ψ aus der leeren Hypothesenmenge ableitbar (kurz: $\vdash \psi$) wenn die Sequenz $\varnothing \Rightarrow \psi$ in SK abgeleitet werden kann.

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

Wir erläutern diesen Algorithmus zunächst an zwei Beispielen.

Beispiele. (1) Betrachte die Formel $\psi := (X \to Y) \to (\neg Y \to \neg X)$. Wir suchen also einen Beweis in SK für die Sequenz $\varnothing \Rightarrow \psi$. Wir beobachten zunächst, dass ψ die Form $(\varphi \to \vartheta)$ hat. Die einzige Regel, die zu einer Sequenz der Form $\varnothing \Rightarrow (\varphi \to \vartheta)$ 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:

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

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:

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

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

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

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

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

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

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

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

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

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

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

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

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

Definition 3.15. Ein *Ableitungsbaum* T für eine Sequenz S ist ein Baum, dessen Wurzel mit S beschriftet ist, so dass jeder innere Knoten von T mit der unteren Zeile einer Schlussregel und die Kinder dieses Knotens mit den in der oberen Zeile derselben Regel auftretenden Sequenzen beschriftet sind.

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

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

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

Beweissuche im aussagenlogischen Sequenzenkalkül

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

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

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

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

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

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

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

Satz 3.16. *Der angegebene Suchalgorithmus terminiert auf jeder gegebenen Sequenz* $\Gamma \Rightarrow \Delta$ *in endlich vielen Schritten. Er findet einen Beweis genau dann wenn* $\Gamma \Rightarrow \Delta$ *gültig ist; andernfalls findet er eine falsifizierende Interpretation für* $\Gamma \Rightarrow \Delta$.

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

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

Andernfalls enthält der konstruierte Ableitungsbaum ein negatives Blatt, mit einer Beschriftung $\Gamma' \Rightarrow \Delta'$, so dass Γ' und Δ' disjunkte Mengen von Aussagenvariablen sind. Indem man die Aussagenvariablen in Γ' mit wahr, diejenigen in Δ' mit falsch, und alle übrigen beliebig belegt, gewinnt man eine Interpretation welche $\Gamma' \Rightarrow \Delta'$ falsifiziert. Aus Lemma 3.12 folgt dass diese Interpretation auch die Ausgangssequenz $\Gamma \Rightarrow \Delta$ falsifiziert. □

Der Sequenzenkalkül liefert also sogar ein *Entscheidungsverfahren* für die gültigen aussagenlogischen Sequenzen und damit auch für die aussagenlogischen Tautologien. Insbesondere folgt aus Satz 3.16, dass der aussagenlogische Sequenzenkalkül vollständig ist.

Korollar 3.17 (Vollständigkeit des Sequenzenkalküls). *Jede gültige aussagenlogische Sequenz is im Sequenzenkalkül ableitbar.*

Übung 3.10. Konstruieren Sie Beweise oder falsifizierende Interpretationen für die folgenden Sequenzen:

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

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

Übung 3.11. Konstruieren Sie Beweise in SK für die folgenden aussagenlogischen Tautologien:

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

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

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

Übung 3.12. 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 3.13. 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.

3.5 Aussagenlogische Resolution

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

Definition 3.18. Eine *Klausel* ist eine endliche Menge von Literalen. Mit $\Box$ bezeichnet man die leere Klausel. Einer Formel $\psi = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m_i} Y_{ij}$ in KNF wird eine endliche *Klauselmenge* $K(\psi)$ wie folgt zugeordnet: Jeder Disjunktion $\bigvee_{j=1}^{m_i} Y_{ij}$ ordnet man die Klausel $C_i = \{Y_{ij} : j = 1, \dots, m_i\}$ zu und setzt $K(\psi) := \{C_1, \dots, C_n\}$.

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 $\mathfrak{I}(Y) = 1$. Beachte :

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

Definition 3.19. Seien C, C_1, C_2 Klauseln. C ist *Resolvente* von C_1 und C_2 genau dann, wenn es ein Literal Y gibt mit $Y \in C_1, \overline{Y} \in C_2$ und $C = (C_1 - \{Y\}) \cup (C_2 - \{\overline{Y}\})$. Dies wird folgendermassen notiert:

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

Beispiele.

$$\begin{tikzcd}
\{X_1, X_3, \neg X_4\} \arrow[dr, dash] & & \{X_2, \neg X_4\} \arrow[dl, dash] \\
& \{X_1, \neg X_2, X_3\} &
\end{tikzcd}
\qquad
\begin{tikzcd}
\{X_1\} \arrow[dr, dash] & & \{\neg X_1\} \arrow[dl, dash] \\
& \square &
\end{tikzcd}$$

Lemma 3.20 (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 $\mathfrak{I}(K \cup \{C\}) = 1$, dann offensichtlich erst recht $\mathfrak{I}(K) = 1$. Sei umgekehrt $\mathfrak{I}(K) = 1$ und $C = (C_1 - \{Y\}) \cup (C_2 - \{\overline{Y}\})$.

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

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

Also ist $\mathfrak{I}(K \cup \{C\}) = 1$. $\square$

Definition 3.21. Für jede Klauselmenge K sei

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

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

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

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

Satz 3.22 (Resolutionssatz). *Eine Klauselmenge K ist unerfüllbar genau dann, wenn $\square \in Res^*(K)$.*

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

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

Sei $n = 0$. Es gibt nur zwei Klauselmengen ohne Aussagenvariablen, nämlich $\varnothing$ 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^+, K_0^- in denen X_n nicht vorkommt: $K_0^+ := \{C - \{\neg X_n\} : X_n \notin C, C \in K_0\}$ (d.h. wir streichen aus K_0 alle Klauseln, in denen X_n vorkommt und streichen $\neg X_n$ aus allen verbleibenden Klauseln). Indem wir die Rollen von X_n und $\neg X_n$ vertauschen, erhalten wir $K_0^- := \{C - \{X_n\} : \neg X_n \notin C, C \in K_0\}$.

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

Aus der Induktionsvoraussetzung folgt, dass $\square \in Res^*(K_0^+)$ und $\square \in Res^*(K_0^-)$. 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 $\neg X_{n+1}$ entstanden sein. Wenn nicht, dann sind $C_1, \ldots, C_m$ auch in $Res^*(K_0)$, also $\square \in Res^*(K_0)$. Wenn ja, erhalten wir durch Wiedereinfügen von $\neg X_{n+1}$ eine Folge von Klauseln $C_1', \ldots, C_m'$ welche beweist, dass $\{\neg X_{n+1}\} \in Res^*(K_0)$.

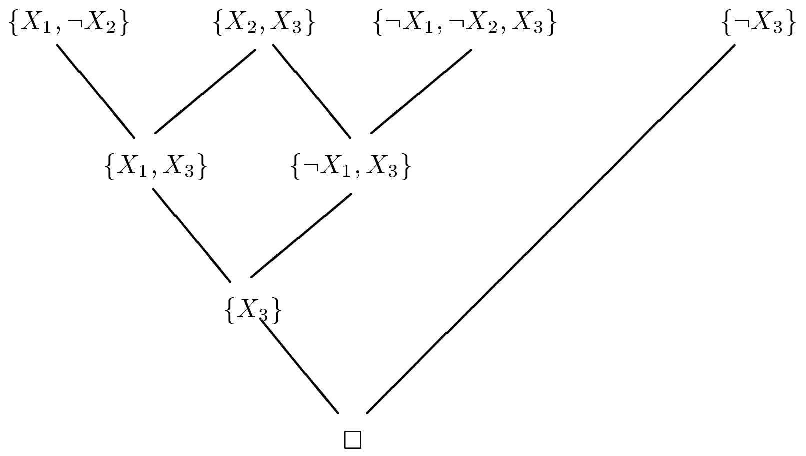
$$\begin{tikzcd}[column sep=small] C_j & & C_k & & & C_j \cup \{\neg X_{n+1}\} & & \{C_k\} \\ & C_i \arrow[from=1-1, no head] \arrow[from=1-3, no head] & & \Longrightarrow & & & C_i \cup \{\neg X_{n+1}\} \arrow[from=1-6, no head] \arrow[from=1-8, no head] & \end{tikzcd}$$

Analog folgt aus $\square \in Res^*(K_0^-)$, dass entweder $\square \in Res^*(K_0)$ oder $\{X_{n+1}\} \in Res^*(K_0)$. Mit

$$\begin{tikzcd}[column sep=small] \{\neg X_{n+1}\} & & \{X_{n+1}\} \\ & \square \arrow[from=1-1, no head] \arrow[from=1-3, no head] & \end{tikzcd}$$

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

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



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

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

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

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

Erfüllbarkeitstest mit Resolution

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

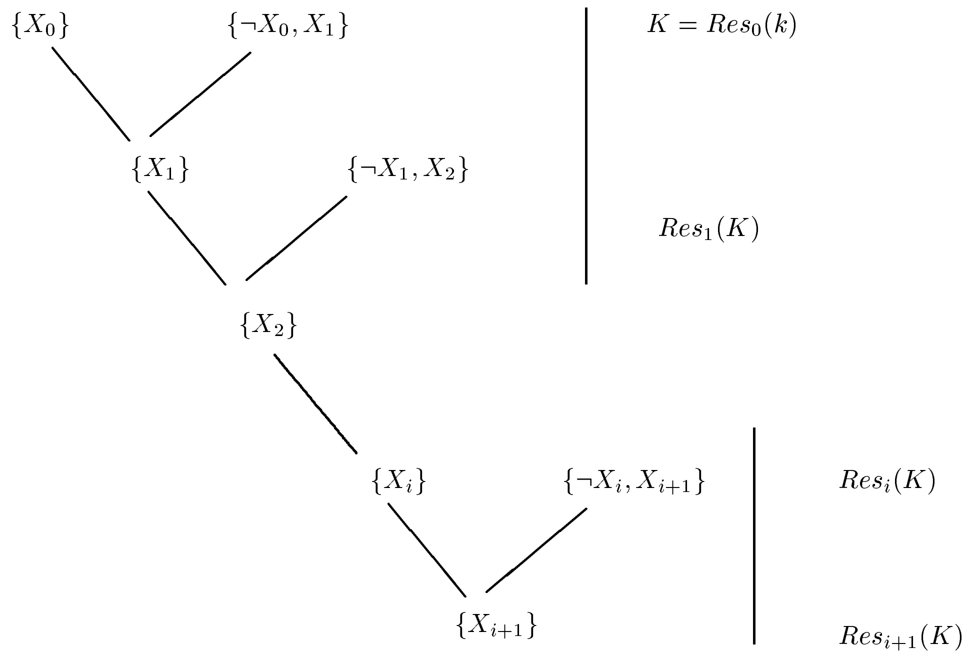
Dieser Algorithmus hat (im worst case) exponentielle Komplexität. Es ist auch nicht zu erwarten, dass es einen effizienten (in polynomialer Zeit laufenden) Algorithmus für dieses Problem gibt, denn das Erfüllbarkeitsproblem für KNF-Formeln ist NP-vollständig.

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

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

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

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



3.6 Erfüllbarkeitstests für Horn-Formeln

Die Resolutionsmethode liefert ein Entscheidungsverfahren für die (Un-)Erfüllbarkeit endlicher Klauselmengen (und damit von aussagnelogischen Formeln in KNF), welches allerdings nicht immer effizient ist. Es gibt aber Teilklassen für die das Erfüllbarkeitsproblem effizient gelöst werden kann.

Definition 3.23. 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. (Vergleiche Horn-Formeln der Prädikatenlogik).

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

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

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

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

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

Erfüllbarkeitstest für Horn-Formeln

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

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

Satz 3.24. *Der angegebene Erfüllbarkeitstest für Horn-Formeln ist korrekt. Wenn ψ erfüllbar ist, dann ist $\mathfrak{I}_M$ ein Modell von ψ. Für Formeln mit n Aussagenvariabeln hält der Erfüllbarkeitstest nach höchstens $n+1$ Iterationen der while-Schleife.*

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

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

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

(2) Für alle Unterformeln $X_1 \wedge \ldots \wedge X_k \to 0$ gilt: $\{X_1, \ldots, X_k\} \not\subseteq M$ (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. □

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

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

Definition 3.25. 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 3.26 (Vollständigkeit der Einheitsresolution für Horn-Formeln). *Eine aussagenlogische Horn-Formel ψ ist unerfüllbar genau dann, wenn $\Box$ durch Einheitsresolution aus $K(\psi)$ ableitbar ist.*

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

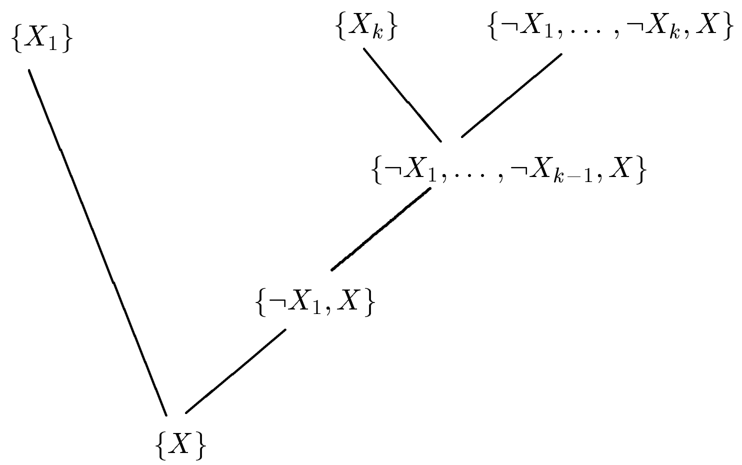
Für die Umkehrung betrachten wir den Erfüllbarkeitstest für Horn-Formeln. Setze:

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

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

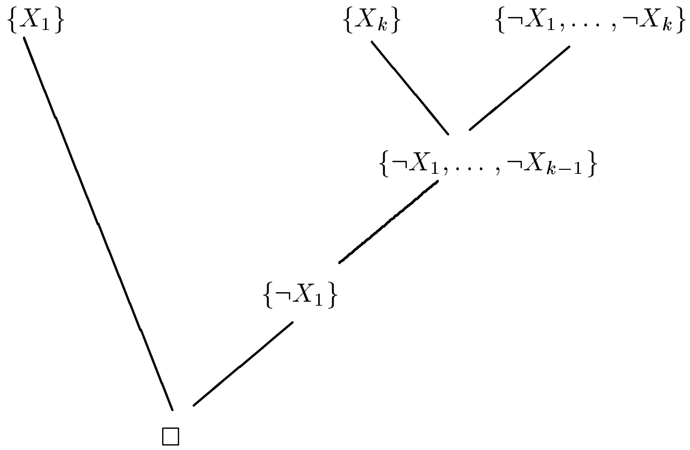
Die Korrektheit des Erfüllbarkeitstests (Satz 3.24) ergibt: ψ ist unerfüllbar genau dann, wenn $X_1, \dots, X_k \in M^*$ existieren, so dass $\{\neg X_1, \dots, \neg X_k\} \in K(\psi)$. Wir zeigen: Wenn $X \in M^*$, dann ist $\{X\}$ per Einheitsresolution aus $K(\psi)$ ableitbar.

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



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

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



Ableitung von $\square$ per Einheitsresolution.

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

Kapitel 4

Definierbarkeit und elementare Äquivalenz

4.1 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 4.1. Sei $\mathrm{Str}(\tau)$ die Klasse aller τ-Strukturen. Eine Strukturklasse $\mathcal{K} \subseteq \mathrm{Str}(\tau)$ ist FO-*axiomatisierbar* (oder einfach: axiomatisierbar), wenn eine Satzmenge $\Phi \subseteq \mathrm{FO}(\tau)$ existiert, so dass $\mathcal{K} = \mathrm{Mod}(\Phi)$. Wenn das Axiomensystem Φ für $\mathcal{K}$ endlich ist, dann können wir die Konjunktion $\psi = \bigwedge\{\varphi : \varphi \in \Phi\}$ bilden und damit $\mathcal{K}$ durch einen einzigen Satz axiomatisieren. Wir sagen in diesem Fall, $\mathcal{K}$ ist *elementar* oder *endlich axiomatisierbar*.

Wir beginnen in diesem Kapitel mit der Untersuchung der Ausdrucksstärke der Prädikatenlogik. Ein wichtiger Aspekt ist dabei die Frage: Welche Strukturklassen sind FO-axiomatisierbar, welche sind sogar endlich axiomatisierbar.

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 2.2 dafür angegeben haben, besteht aus unendlich vielen Formeln. (Wir werden später sehen, dass kein endliches Axiomensystem für diese Klasse existiert.)

Hier sind noch einige weitere Beispiele für axiomatisierbare Strukturklassen.

Beispiele. (1) Die Klasse aller Körper ist axiomatisiert durch $\psi_{\text{Körper}} \in \mathrm{FO}(\tau_{ar})$, die Konjunktion aller Körperaxiome. Für jede Primzahl p ist auch die Klasse der Körper mit Charakteristik p endlich axiomatisierbar, durch $\psi_{\text{Körper}} \wedge \chi_p$ wobei χ_p der Satz $\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$ ist. Für Körper der Charakteristik 0 können wir zumindest ein unendliches Axiomensystem angeben, nämlich

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

(2) Auch die Klasse ACF der algebraisch abgeschlossenen Körper ist FO-axiomatisierbar. Der Satz

$$\psi_n := \forall u_0 \cdots \forall u_n (u_n \neq 0 \rightarrow \exists x (u_0 + u_1 x + \cdots u_n x^n = 0))$$

besagt, dass jedes Polynom n-ten Grades mit Koeffizienten aus dem Körper auch eine Nullstelle im Körper hat. (Hier ist x^n als abkürzende Schreibweise für den Term $\underbrace{x \cdot x \ldots x}_{n \text{ mal}}$ aufzufassen.)

Also ist $\Phi_{\text{ACF}} = \{\psi_{\text{Körper}}\} \cup \{\psi_n : n \geq 1\}$ ein Axiomensystem für algebraisch abgeschlossene Körper.

Übung 4.1. Ein (abstrakter) Stack über einem endlichen Alphabet Γ ist formalisiert durch eine Algebra $\mathfrak{S} = (\Gamma^*, pop, top, (push_a)_{a \in \Gamma})$ mit einstelligen Funktionen

$$\begin{aligned} pop(wa) &:= w, & pop(\lambda) = \lambda \\ top(wa) &:= a, & top(\lambda) = \lambda \\ push_a(w) &:= wa \end{aligned}$$

für alle $w \in \Gamma^*$, $a \in \Gamma$.

Offensichtlich ist jedoch nicht jede Algebra der Signatur $\tau_{\text{stack}} = \{pop, top, (push_a)_{a \in \Gamma})\}$ ein Stack. Geben Sie ein endliches Axiomensystem für die Klasse aller Stacks an.

Übung 4.2. Sei $\mathfrak{A}$ eine endliche Struktur mit endlicher Signatur. Zeigen Sie, dass $\{\mathfrak{B} : \mathfrak{B} \cong \mathfrak{A}\}$ endlich axiomatisierbar ist.

Der Nachweis, dass eine Strukturklasse (endlich) axiomatisierbar ist, wird in der Regel durch explizite Angabe eines Axiomensystems geführt. Um nachzuweisen, dass eine Strukturklasse gar kein oder mindestens kein endliches Axiomensystem zulässt, sind andere Methoden erforderlich, welche in diesem und den folgenden Kapiteln entwickelt werden sollen.

Zunächst aber diskutieren wir noch einen andern 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 4.2. Eine Relation $R \subseteq A^r$ auf dem Universum einer τ-Struktur $\mathfrak{A}$ ist *(elementar) definierbar* in $\mathfrak{A}$ wenn $R = \psi^{\mathfrak{A}}$ für eine Formel $\psi \in \text{FO}(\tau)$. Eine Funktion $f : A^r \rightarrow A$ heisst elementar definierbar, wenn ihr Graph R_f elementar definierbar ist.

Insbesondere ist also eine Konstante a elementar definierbar, wenn eine Formel $\varphi(x) \in \text{FO}(\tau)$ existiert, so dass $\mathfrak{A} \models \varphi(a)$ und $\mathfrak{A} \models \neg\varphi(b)$ für alle $b \neq a$. Wir sagen, a ist *termdefinierbar* in $\mathfrak{A}$, wenn ein Grundterm $t \in T(\tau)$ existiert, so dass $t^{\mathfrak{A}} = a$. Jede termdefinierbare Konstante ist insbesondere elementar definierbar durch eine Formel der Form $x = t$.

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

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

(2) In $(\mathbb{Z}, <)$ ist die Nachfolgerfunktion $z \mapsto z{+}1$ elementar definierbar durch die Formel $\varphi(x, y) := x < y \wedge \forall z(x < z \wedge y \neq z \rightarrow y < z)$.

(3) In $(\mathbb{N}, +, 0, 1)$ ist jedes n termdefinierbar, durch den Term $\boldsymbol{n} = \underbrace{1 + \cdots + 1}_{n \text{ mal}}$ (für $n \geq 1$).

(4) Im Körper $(\mathbb{Q}, +, \cdot, 0, 1)$ der rationalen Zahlen sind die termdefinierbaren Konstanten genau die natürlichen Zahlen $n \in \mathbb{N}$. Alle andern Elemente sind elementar definierbar durch Formeln der Form $\boldsymbol{p} \cdot x = \boldsymbol{q}$ oder , $\boldsymbol{p} \cdot x + \boldsymbol{q} = 0$, aber nicht termdefinierbar.

(5) Im Körper der reellen Zahlen können schon aus Mächtigkeitsgründen nicht alle Elemente elementar definierbar sein: es gibt überabzählbar viele reelle Zahlen, aber nur abzählbar viele Formeln $\varphi(x) \in \mathrm{FO}(\tau_{ar})$.

Das Hinzunehmen definierbarer Relationen bringt keinen Gewinn an Ausdrucksstärke.

Lemma 4.3. *Sei $\mathfrak{A}$ eine σ-Struktur und $\mathfrak{B}$ eine Expansion von $\mathfrak{A}$ durch beliebig viele, in $\mathfrak{A}$ elementar definierbare Relationen und Funktionen. Dann ist jede in $\mathfrak{B}$ elementar definierbare Relation oder Funktion bereits in $\mathfrak{A}$ elementar definierbar.*

Beweis. Sei τ die Signatur von $\mathfrak{B}$. In jeder Formel $\psi(\bar{x}) \in \mathrm{FO}(\tau)$ kommen nur endlich viele Relations- und Funktionssymbole $R_1, \ldots, R_s, f_1, \ldots, f_t$ aus $\tau - \sigma$ vor. Zu jedem dieser R_i bzw. f_j gibt es eine σ-Formel $\vartheta_i(\bar{y})$ bzw. $\chi_j(\bar{y}, z)$, welche in $\mathfrak{A}$ die entsprechende Relation bzw. Funktion von $\mathfrak{B}$ definiert.

Weiter können wir nach Lemma 2.19 annehmen, dass ψ termreduziert ist, d.h., dass Funktionssymbole aus $\tau - \sigma$ nur in Atomen der Form $f_j\bar{y} = z$ auftreten. Indem wir in $\psi(\bar{x})$ die Relations- und Funktionssymbole aus $\tau - \sigma$ durch die definierenden Formeln ersetzen (d.h. jedes Atom $R_i\bar{u}$ durch $\vartheta_i(\bar{u})$ und jedes Atom $f_j\bar{u} = v$ durch $\chi_j(\bar{u}, v)$), erhalten wir eine Formel $\varphi(\bar{x}) \in \mathrm{FO}(\sigma)$ so, dass $\mathfrak{B} \models \forall x(\psi \leftrightarrow \varphi)$. Da φ eine σ-Formel ist, folgt insbesondere, dass $\psi^{\mathfrak{B}} = \varphi^{\mathfrak{A}}$. □

Relativierte Quantoren. Sei $f : \mathbb{R} \rightarrow \mathbb{R}$ eine Funktion auf den reellen Zahlen. Ist die Menge $\{a \in \mathbb{R} : f \text{ stetig am Punkt } a\}$ in der Struktur $(\mathbb{R}, +, \cdot, 0, 1, <, f)$ elementar definierbar?

Wir betrachten dazu die Stetigkeitsdefinition aus der Analysis: Sei $U_\varepsilon(x)$ die ε-Umgebung von x. Die Funktion f ist stetig in x, wenn für alle $\varepsilon > 0$ ein $\delta > 0$ existiert so, dass für alle $y \in U_\delta(x)$ gilt: $f(y) \in U_\varepsilon(f(x))$.

Die Existenz- und Allaussagen für δ, ε und y sind hier *relativiert*: es werden nur Elemente betrachtet, die gewisse Eigenschaften erfüllen. Man beachte, dass relativierte Aussagen der Form "es gibt ein x mit α, so dass $\cdots$" bzw. "für alle x mit α gilt $\cdots$" durch $\exists x(\alpha \wedge \cdots)$ bzw. $\forall x(\alpha \rightarrow \cdots)$ formalisiert werden können Wir benutzen gelegentlich die Schreibweise $(\exists x \,.\, \alpha)\psi$ als Umschreibung für $\exists x(\alpha \wedge \psi)$ und $(\forall x \,.\, \alpha)\psi$ für $\forall x(\alpha \rightarrow \psi)$.

Um Stetigkeit zu formalisieren gehen wir nun wie folgt vor. (Wir verwenden die Relation $\leq$, was aufgrund ihrer elementaren Definierbarkeit unproblematisch ist.) Zunächst ist leicht einzusehen, dass die Relation $\{(a, b, \varepsilon) \in \mathbb{R}^3 : \varepsilon \geq 0 \text{ und } b \in U_\varepsilon(a)\}$ durch die Formel

$$\varphi(x, y, z) := 0 \leq z \wedge (\exists u \,.\, 0 \leq u \leq z)(x + u = y \vee y + u = x)$$

definiert wird. Die Stetigkeit von f im Punkt x ist nun ausgedrückt durch die Formel

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

4.2 Das Isomorphielemma

Lemma 4.4 (Isomorphielemma). *Sei $\pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$ ein Isomorphismus von τ-Strukturen. Dann gilt für alle $\psi(x_1, \dots, x_n) \in \mathrm{FO}(\tau)$ und alle $a_1, \dots, a_n \in A$*

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

Beweis. Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine Interpretation mit $\beta(x_1) = a_1, \dots, \beta(x_n) = a_n$, und sei $\mathfrak{I}^\pi$ die Interpretation $(\mathfrak{B}, \pi \circ \beta)$. Wir haben bereits in Satz 2.14 gezeigt, dass für jeden Term $t \in T(\tau)$ gilt

$$t^{\mathfrak{I}^\pi} = \pi(t^{\mathfrak{I}}) \tag{*}$$

sogar wenn nur vorausgesetzt ist, dass $\pi : \mathfrak{A} \to \mathfrak{B}$ ein Homomorphismus ist.

Es ist zu zeigen, dass $\mathfrak{I} \models \psi$ genau dann, wenn $\mathfrak{I}^\pi \models \psi$. Wir führen den Beweis per Induktion über den Formelaufbau; nach Lemma 2.18 können wir dabei annehmen, dass ψ reduziert ist.

(1) Für Formeln der Form $t_1 = t_2$ gilt

$$\begin{aligned} \mathfrak{I} \models t_1 = t_2 &\iff t_1^{\mathfrak{I}} = t_2^{\mathfrak{I}} \\ &\iff \pi t_1^{\mathfrak{I}} = \pi t_2^{\mathfrak{I}} \quad \text{(da } \pi \text{ injektiv ist)} \\ &\iff t_1^{\mathfrak{I}^\pi} = t_2^{\mathfrak{I}^\pi} \quad \text{(nach (*))} \\ &\iff \mathfrak{I}^\pi \models t_1 = t_2 \end{aligned}$$

(2) Für Atome $Pt_1 \cdots t_n$ gilt

$$\begin{aligned} \mathfrak{I} \models Pt_1 \cdots t_n &\iff (t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}}) \in P^{\mathfrak{A}} \\ &\iff (\pi t_1^{\mathfrak{I}}, \dots, \pi t_n^{\mathfrak{I}}) \in P^{\mathfrak{B}} \quad \text{(da } \pi \text{ ein starker Homomorphismus ist)} \\ &\iff (t_1^{\mathfrak{I}^\pi}, \dots, t_n^{\mathfrak{I}^\pi}) \in P^{\mathfrak{B}} \quad \text{(nach (*))} \\ &\iff \mathfrak{I}^\pi \models Pt_1 \cdots t_n \end{aligned}$$

(3) Für Formeln der Form $\neg\psi$ oder $\psi \vee \varphi$ ist der Induktionsschluss trivial.

(4) Für Formeln $\exists x \psi$ gilt

$$\begin{aligned} \mathfrak{I} \models \exists x \psi &\iff \mathfrak{I}[x/a] \models \psi \ \text{ für ein } a \in A \\ &\iff \mathfrak{I}[x/a]^\pi \models \psi \ \text{ für ein } a \in A \text{ (nach Induktionsvoraussetzung)} \\ &\iff \mathfrak{I}^\pi[x/\pi a] \models \psi \ \text{ für ein } a \in A \text{ (da } \mathfrak{I}[x/a]^\pi = \mathfrak{I}^\pi[x/\pi a]) \\ &\iff \mathfrak{I}^\pi[x/b] \models \psi \ \text{ für ein } b \in B \text{ (da } \pi \text{ bijektiv ist)} \\ &\iff \mathfrak{I}^\pi \models \exists x \psi. \end{aligned}$$

□

Insbesondere lassen sich isomorphe τ-Strukturen durch Sätze der Prädikatenlogik nicht unterscheiden. Sind $\mathfrak{A}$ und $\mathfrak{B}$ isomorphe τ-Strukturen, so gilt für alle τ-Sätze ψ:

$$\mathfrak{A} \models \psi \iff \mathfrak{B} \models \psi.$$

Also sind axiomatisierbare Modellklassen immer isomorphie-abgeschlossen. Dies bedeutet, dass für jede Klasse $\mathcal{K} = \text{Mod}(\psi)$ und alle Strukturen $\mathfrak{A}, \mathfrak{B}$ gilt

$$\mathfrak{A} \in \mathcal{K},\ \mathfrak{A} \cong \mathfrak{B} \implies \mathfrak{B} \in \mathcal{K}.$$

In manchen Fällen liefert das Isomorphielemma ein einfaches Kriterium, um nachzuweisen, dass eine Relation in einer Struktur *nicht* elementar definierbar ist

Lemma 4.5. *Sei π ein Automorphismus einer τ-Struktur $\mathfrak{A}$ und sei $\psi \in \text{FO}(\tau)$. Dann ist π auch ein Automorphismus der expandierten Struktur $(\mathfrak{A}, \psi^{\mathfrak{A}})$.*

Beweis. Da π ein Automorphisus ist, gilt für alle Tupel $\bar{a}$ aus A: $\mathfrak{A} \models \psi(\bar{a}) \iff \mathfrak{A} \models \psi(\pi\bar{a})$. Also ist $\pi(\psi^{\mathfrak{A}}) = \psi^{\mathfrak{A}}$. □

Beispiel. In $(\mathbb{R}, +, 0)$ ist $<$ nicht elementar definierbar. Die Abbildung $\pi : x \mapsto -x$ ist ein Automorphismus von $(\mathbb{R}, +, 0)$, nicht aber von $(\mathbb{R}, +, 0, <)$, denn aus $a < b$ folgt eben gerade *nicht* $-a < -b$.

Übung 4.3. Sei $\tau = \varnothing$ und A unendlich. Beschreiben Sie alle in A elementar definierbaren Relationen $R \subseteq A^n$.

Übung 4.4. Zeigen Sie, dass in $(\mathbb{N}, \cdot, 1)$ die Addition nicht elementar definierbar ist.

4.3 Erhaltungseigenschaften für bestimmte Formelklassen

Universelle und existentielle Formeln. Wir haben gesehen, dass jede FO-axiomatisierbare Klasse $\mathcal{K}$ von Strukturen abgeschlossen ist unter Isomorphie: Wenn $\mathfrak{A} \in \mathcal{K}$ und $\mathfrak{A} \cong \mathfrak{B}$, dann auch $\mathfrak{B} \in \mathcal{K}$. Nun gibt es auch andere interessante Abschlusseigenschaften, die von gewissen Strukturklassen erfüllt werden. So ist etwa die Klasse $\text{Mod}(\Phi_{\text{Gruppe}})$ aller Gruppen $(G, \circ, e, {}^{-1})$ abgeschlossen unter Substrukturen: Jede Substruktur einer so formalisierten Gruppe ist wieder eine Gruppe. Analoges gilt für die Klasse aller Vektorräume $(V, +, 0, (f_k)_{k \in K})$ über einem festen Körper K. Allgemein sagen wir, dass eine Strukturklasse $\mathcal{K}$ abgeschlossen ist unter Substrukturen, wenn $\mathcal{K}$ mit jeder Struktur auch alle ihre Substrukturen enthält.

Offensichtlich haben nicht alle FO-axiomatisierbaren Modellklassen diese Eigenschaft. Ein triviales Gegenbeispiel ist etwa die Klasse $\text{Mod}(\exists x Px)$. Es gibt aber ein einfaches syntaktisches Kriterium, welches impliziert, dass $\text{Mod}(\Phi)$ abgeschlossen ist unter Substrukturen.

Definition 4.6. Die Menge der *universellen Formeln* ist induktiv wie folgt definiert:

(1) Jede quantorenfreie Formel ist universell.

(2) Wenn ψ und φ universell sind, dann auch $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $\forall x \psi$ (für alle $x \in \text{VAR}$).

Aus dem Beweis des Satzes über die Pränex-Normalform ergibt sich leicht, dass jede universelle Formel logisch äquivalent ist zu einer Formel der Gestalt $\forall y_1 \cdots \forall y_r \varphi$ mit quantorenfreiem φ.

Lemma 4.7 (Substrukturlemma). *Seien $\mathfrak{A} \subseteq \mathfrak{B}$ τ-Strukturen und $\psi(x_1, \ldots, x_n)$ eine universelle Formel. Dann gilt für alle $a_1, \ldots, a_n \in A$*

$$\mathfrak{B} \models \psi(a_1, \ldots, a_n) \implies \mathfrak{A} \models \psi(a_1, \ldots, a_n).$$

Beweis. Wir stellen zunächst fest, dass die Behauptung für quantorenfreie Formeln offensichtlich richtig ist. Weiter können wir annehmen, dass $\psi(\bar{x}) = \forall y_1 \cdots \forall y_r \varphi(\bar{x}, \bar{y})$ mit quantorenfreiem $\varphi(\bar{x}, \bar{y})$. Wenn $\mathfrak{B} \models \psi(\bar{a})$, dann gilt für alle $\bar{b} \in B^r$, insbesondere also für alle $\bar{b} \in A^r$, dass $\mathfrak{B} \models \varphi(\bar{a}, \bar{b})$. Da φ quantorenfrei ist, folgt $\mathfrak{A} \models \varphi(\bar{a}, \bar{b})$ für alle $\bar{b} \in A^r$, also $\mathfrak{A} \models \psi(\bar{a})$. □

Korollar 4.8. *Für jede Menge Φ von universellen Sätzen ist* $\mathrm{Mod}(\Phi)$ *abgeschlossen unter Substrukturen.*

Beispiel. Die Klasse aller Gruppen, formalisiert in der Form $(G, \circ, e)$ (also ohne explizit gegebene Inversenfunktion) ist nicht durch universelle Sätze axiomatisierbar, denn $(\mathbb{N}, +, 0)$ ist eine Substruktur der Gruppe $(\mathbb{Z}, +, 0)$, aber selbst keine Gruppe.

Die *existentiellen Formeln* sind dual zu den universellen Formeln definiert, indem in Definition 4.6 der Allquantor durch den Existenzquantor ersetzt wird.

Lemma 4.9. *(i) Die Negation einer existentiellen Formel ist logisch äquivalent zu einer universellen Formel (und umgekehrt).*

(ii) Jede existentielle Formel ist logisch äquivalent zu einer Formel der Gestalt $\exists x_1 \ldots \exists x_r \varphi$ mit quantorenfreiem φ.

(iii) Jede durch eine Menge existentieller Formeln axiomatisierte Modellklasse $\mathcal{K}$ ist abgeschlossen unter Erweiterungen: Wenn $\mathfrak{A} \in \mathcal{K}$ und $\mathfrak{A} \subseteq \mathfrak{B}$, dann ist auch $\mathfrak{B} \in \mathcal{K}$.

Positive Formeln. Eine Formel ist *positiv*, wenn sie nur die Junktoren $\wedge$ und $\vee$ enthält.

Satz 4.10. *Sei $\pi : \mathfrak{A} \to \mathfrak{B}$ ein surjektiver Homomorphismus und $\psi(x_1, \ldots, x_n)$ eine positive Formel. Dann gilt für alle $a_1, \ldots, a_n \in A$*

$$\mathfrak{A} \models \psi(a_1, \ldots, a_n) \implies \mathfrak{B} \models \psi(\pi a_1, \ldots, \pi a_n).$$

Beweis. Wir gehen analog zum Beweis des Isomorphielemmas vor. Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine Interpretation mit $\beta(x_1) = a_1, \ldots, \beta(x_n) = a_n$ und sei $\mathfrak{I}^\pi$ die Interpretation $(\mathfrak{B}, \pi \circ \beta)$. Es ist zu zeigen, dass

$$\mathfrak{I} \models \psi \implies \mathfrak{I}^\pi \models \psi$$

für jedes positives ψ. Wir benutzen wieder den in Satz 2.14 bewiesenen Sachverhalt, dass

$$t^{\mathfrak{I}^\pi} = \pi(t^{\mathfrak{I}}) \qquad (*)$$

für jeden Term $t \in T(\tau)$ und führen den Beweis per Induktion über den Formelaufbau (wobei wir im Gegensatz zum Beweis des Isomorphielemmas nicht mehr annehmen können, dass ψ reduziert ist).

(1) Für Formeln der Form $t_1 = t_2$ gilt

$$\begin{aligned}
\mathfrak{I} \models t_1 = t_2 &\implies t_1^{\mathfrak{I}} = t_2^{\mathfrak{I}} \\
&\implies \pi t_1^{\mathfrak{I}} = \pi t_2^{\mathfrak{I}} \\
&\implies t_1^{\mathfrak{I}^\pi} = t_2^{\mathfrak{I}^\pi} \quad \text{(nach (*))} \\
&\implies \mathfrak{I}^\pi \models t_1 = t_2
\end{aligned}$$

(2) Für Atome $Pt_1 \cdots t_n$ gilt

$$\begin{aligned}
\mathfrak{I} \models Pt_1 \cdots t_n &\implies (t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}}) \in P^{\mathfrak{A}} \\
&\implies (\pi t_1^{\mathfrak{I}}, \dots, \pi t_n^{\mathfrak{I}}) \in P^{\mathfrak{B}} \quad \text{(da } \pi \text{ ein Homomorphismus ist)} \\
&\implies (t_1^{\mathfrak{I}^\pi}, \dots, t_n^{\mathfrak{I}^\pi}) \in P^{\mathfrak{B}} \quad \text{(nach (*))} \\
&\implies \mathfrak{I}^\pi \models Pt_1 \cdots t_n
\end{aligned}$$

(3) Für Formeln der Form $\psi \wedge \varphi$ oder $\psi \vee \varphi$ ergibt sich der Induktionsschluss unmittelbar aus der Monotonie von $\wedge$ und $\vee$.

(4) Für Formeln $\exists x \psi$ gilt

$$\begin{aligned}
\mathfrak{I} \models \exists x \psi &\implies \mathfrak{I}[x/a] \models \psi \quad \text{für ein } a \in A \\
&\implies \mathfrak{I}[x/a]^\pi \models \psi \quad \text{für ein } a \in A \text{ (nach Induktionsvoraussetzung)} \\
&\implies \mathfrak{I}^\pi[x/\pi a] \models \psi \quad \text{für ein } a \in A \text{ (da } \mathfrak{I}[x/a]^\pi = \mathfrak{I}^\pi[x/\pi a]) \\
&\implies \mathfrak{I}^\pi \models \exists x \psi.
\end{aligned}$$

(5) Für Formeln $\forall x \psi$ gilt

$$\begin{aligned}
\mathfrak{I} \models \forall x \psi &\implies \mathfrak{I}[x/a] \models \psi \quad \text{für alle } a \in A \\
&\implies \mathfrak{I}[x/a]^\pi \models \psi \quad \text{für alle } a \in A \text{ (nach Induktionsvoraussetzung)} \\
&\implies \mathfrak{I}^\pi[x/\pi a] \models \psi \quad \text{für alle } a \in A \text{ (da } \mathfrak{I}[x/a]^\pi = \mathfrak{I}^\pi[x/\pi a]) \\
&\implies \mathfrak{I}^\pi[x/b] \models \psi \quad \text{für alle } b \in B \text{ (da } \pi \text{ surjektiv ist)} \\
&\implies \mathfrak{I}^\pi \models \forall x \psi.
\end{aligned}$$

□

Korollar 4.11. *Sei* Φ *eine Menge positiver Sätze. Dann ist* $\mathrm{Mod}(\Phi)$ *abgeschlossen unter homomorphen Bildern, d.h. für jedes Modell* $\mathfrak{A} \in \mathrm{Mod}(\Phi)$ *und jeden Homomorphismus* $\pi : \mathfrak{A} \to \mathfrak{B}$ *ist auch* $\pi(\mathfrak{A}) \in \mathrm{Mod}(\Phi)$. *(Das homomorphe Bild* $\pi(\mathfrak{A})$ *ist die von* $\pi(A)$ *induzierte Substruktur von* $\mathfrak{B}$*).*

Beispiel. Sei $\mathfrak{B}$ eine relationale Struktur, welche aus $\mathfrak{A}$ durch 'Vergrössern' gewisser Relationen gewonnen wurde, d.h. es gilt $B = A$ (beide Strukturen haben dasselbe Universum), und $R^{\mathfrak{B}} \supseteq R^{\mathfrak{A}}$ für alle Relationssymbole $R \in \tau$. Dann vermittelt die Identität auf A einen surjektiver Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$. Satz 4.10 impliziert, dass beim Übergang von $\mathfrak{A}$ nach $\mathfrak{B}$ auch alle durch positive Formeln defininierten Relationen vergrössert werden, d.h. $\psi^{\mathfrak{B}} \supseteq \psi^{\mathfrak{A}}$ für jede positive Formel ψ.

Horn-Formeln. Eine sehr wichtige Formelklasse, insbesondere für die Logik-Programmierung, ist die Klasse der Horn-Formeln.

Definition 4.12. Die Menge der *Horn-Formeln* ist induktiv wie folgt definiert:

(1) Jede Disjunktion $\neg\vartheta_1 \vee \cdots \vee \neg\vartheta_n$ oder $\neg\vartheta_1 \vee \cdots \vee \neg\vartheta_n \vee \chi$ von negierten Atomen und höchstens einem nicht-negierten Atom ist eine Horn-Formel.

(2) Wenn ψ und φ Hornformeln sind, dann auch $\psi \wedge \varphi$, $\exists x\psi$ und $\forall x\psi$.

Bemerkung. Die Formeln aus (1) werden oft äquivalent als Implikationen $\vartheta_1 \wedge \cdots \wedge \vartheta_n \to 0$ bzw. $\vartheta_1 \wedge \cdots \wedge \vartheta_n \to \chi$ geschrieben.

Definition 4.13. Das *direkte Produkt* zweier τ-Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ ist die τ-Struktur $\mathfrak{A}\times\mathfrak{B}$ mit Universum $A \times B$, dessen Relationen und Funktionen komponentenweise definiert sind, d.h. für jedes n-stellige Relationssymbol $R \in \tau$ ist

$$R^{\mathfrak{A}\times\mathfrak{B}} := \{(a_1, b_1), \ldots, (a_n, b_n) \in (A \times B)^n : (a_1, \ldots, a_n) \in R^{\mathfrak{A}}, (b_1, \ldots, b_n) \in R^{\mathfrak{B}}\}$$

und für jedes n-stellige Funktionssymbol $f \in \tau$ ist

$$f^{\mathfrak{A}\times\mathfrak{B}}((a_1, b_1), \ldots, (a_n, b_n)) := (f^{\mathfrak{A}}(a_1, \ldots, a_n), f^{\mathfrak{B}}(b_1, \ldots, b_n)).$$

Satz 4.14. *Sei $\psi(x1, \ldots, x_n)$ eine Horn-Formel. Wenn $\mathfrak{A} \models \psi(a_1, \ldots, a_n)$ und $\mathfrak{B} \models \psi(b_1, \ldots, b_n)$, dann auch $\mathfrak{A} \times \mathfrak{B} \models \psi((a_1, b_1), \ldots, (a_n, b_n))$.*

Beweis. Für $\bar{a} = (a_1, \ldots, a_n)$ und $\bar{b} = (b_1, \ldots, b_n)$ sei $\bar{a} \times \bar{b} := ((a_1, b_1), \ldots, (a_n, b_n))$. Für atomare $\vartheta(\bar{x})$ ergibt sich sofort aus der Definition des direkten Produkts, dass

$$\mathfrak{A} \times \mathfrak{B} \models \vartheta(\bar{a} \times \bar{b}) \iff \mathfrak{A} \models \vartheta(\bar{a}) \text{ und } \mathfrak{B} \models \vartheta(\bar{b}). \tag{*}$$

Der Beweis wird nun per Induktion über den Formelaufbau geführt.

(1) Sei $\psi = \neg\vartheta_1 \vee \cdots \vee \neg\vartheta_n$. Wenn $\mathfrak{A} \models \psi(\bar{a})$, dann existiert ein $i \leq n$ mit $\mathfrak{A} \models \neg\vartheta_i(\bar{a})$ Nach (*) folgt $\mathfrak{A} \times \mathfrak{B} \models \neg\vartheta(\bar{a} \times \bar{b})$ und daher $\mathfrak{A} \times \mathfrak{B} \models \psi(\bar{a} \times \bar{b})$.

(2) Sei $\psi = \neg\vartheta_1 \vee \cdots \vee \neg\vartheta_n \vee \chi$ und es gelte $\mathfrak{A} \models \psi(\bar{a})$,$\mathfrak{B} \models \psi(\bar{b})$. Wenn $\mathfrak{A} \models \chi(\bar{a})$ und $\mathfrak{B} \models \chi(\bar{b})$ dann folgt nach (*) $\mathfrak{A}\times\mathfrak{B} \models \chi(\bar{a}\times\bar{b})$ und daher $\mathfrak{A}\times\mathfrak{B} \models \psi(\bar{a}\times\bar{b})$. Andernfalls gilt $\mathfrak{A} \models \neg\vartheta_i(\bar{a})$ oder $\mathfrak{B} \models \neg\vartheta_i(\bar{b})$ für ein $i \leq n$. Wie in (1) folgt $\mathfrak{A} \times \mathfrak{B} \models \psi(\bar{a} \times \bar{b})$.

(3) Für Formeln $\psi \wedge \varphi$, $\exists x\psi$ und $\forall x\psi$ ist der Induktionsschluss offensichtlich. □

Korollar 4.15. *Sei Φ eine Menge von Horn-Sätzen. Dann ist* $\mathrm{Mod}(\Phi)$ *abgeschlossen unter direkten Produkten, d.h., wenn $\mathfrak{A}, \mathfrak{B} \in \mathrm{Mod}(\Phi)$, dann ist auch $\mathfrak{A} \times \mathfrak{B} \in \mathrm{Mod}(\Phi)$.*

Beispiele. (1) Das Axiomensystem Φ_{Gruppe} besteht nur aus Hornsätzen. Damit folgt sofort, dass das direkte Produkt zweier Gruppen wieder eine Gruppe ist.

(2) Die Klasse der linearen Ordnungen ist axiomatisiert durch die Sätze

$$\begin{array}{ll}
\forall x \neg\, x < x & \text{(Hornsatz)} \\
\forall x \forall y \forall z (x < y \wedge y < z \to x < z) & \text{(Hornsatz)} \\
\forall x \forall y (x < y \vee x = y \vee y < x) & (\textit{kein}\ \text{Hornsatz})
\end{array}$$

Es gibt auch kein anderes Axiomensystem für diese Klasse, welches nur aus Hornsätzen besteht, denn die linaren Ordnungen sind nicht abgeschlossen unter direkten Produkten. Zum Beispiel ist $(\mathbb{R}, <) \times (\mathbb{R}, <)$ keine lineare Ordnung.

Bemerkung. Man kann auch direkte Produkte von beliebigen Familien $\{\mathfrak{A}_i : i \in I\}$ von τ-Strukturen bilden (I eine Indexmenge). Das Universum von $\mathfrak{A} = \prod_{i \in I} \mathfrak{A}_i$ ist

$$A := \{g : I \to \bigcup_{i \in I} A_i : \text{ für alle } i \in I \text{ ist } g(i) \in A_i\}.$$

Für jedes n-stellige Relationssymbol $R \in \tau$ ist

$$R^{\mathfrak{A}} := \{(g_1, \dots, g_n) \in A^n : (g_1(i), \dots, g_n(i)) \in R^{\mathfrak{A}_i} \text{ für alle } i \in I\}$$

und für jedes n-stellige Funktionssymbole $f \in \tau$ und jedes $i \in I$ ist

$$f^{\mathfrak{A}}(g_1, \dots, g_n)(i) = f_i^{\mathfrak{A}}(g_1(i), \dots, g_n(i)).$$

Satz 4.14 und Korollar 4.15 gelten auch für solche allgemeinen direkten Produkte (mit im wesentlichen unverändertem Beweis).

Übung 4.5. Sei $\mathfrak{A}_0 \subseteq \mathfrak{A}_1 \subseteq \cdots \subseteq \mathfrak{A}_n \subseteq \cdots$ eine Kette von τ-Strukturen. Wir können dann auf offensichtliche Weise eine τ-Struktur $\bigcup_{n \in \mathbb{N}} \mathfrak{A}_n$ bilden. Zeigen Sie, dass alle Sätze der Form $\psi := \forall x_1 \cdots \forall x_r \exists y_1 \cdots \exists y_s \varphi$ (mit φ quantorenfrei) abgeschlossen sind unter Vereinigung von Ketten, d.h. wenn $\mathfrak{A}_n \models \psi$ für alle n, dann auch $\bigcup_n \mathfrak{A}_n \models \psi$.

4.4 Theorien und elementar äquivalente Strukturen

Definition 4.16. Eine *Theorie* ist eine erfüllbare Menge $T \subseteq \mathrm{FO}(\tau)$ von Sätzen, die unter $\models$ abgeschlossen ist, d.h. es gilt für alle τ-Sätze ψ:

$$T \models \psi \;\Rightarrow\; \psi \in T.$$

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

Sei $\mathfrak{A}$ eine τ-Struktur. Die *Theorie von* $\mathfrak{A}$ ist $\mathrm{Th}(\mathfrak{A}) := \{\psi : \mathfrak{A} \models \psi\}$. Offensichtlich ist $\mathrm{Th}(\mathfrak{A})$ vollständig. Die Theorie einer τ-Modellklasse $\mathcal{K}$ ist

$$\mathrm{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A} \in \mathcal{K}} \mathrm{Th}(\mathfrak{A}).$$

Wenn Φ ein Axiomensystem für $\mathcal{K}$ ist, dann ist $\mathrm{Th}(\mathcal{K}) = \{\psi : \Phi \models \psi\}$. Natürlich ist nicht jede Theorie vollständig. Zum Beispiel enthält die Theorie der Gruppen weder den Satz $\forall x \forall y (x \circ y = y \circ x)$ noch seine Negation, da es sowohl kommutative wie nicht-kommutative Gruppen gibt. Jede Theorie T lässt sich aber zu einer vollständigen Theorie erweitern; für jedes Modell $\mathfrak{A} \models T$ ist $\mathrm{Th}(\mathfrak{A})$ eine vollständige Erweiterung von T.

Definition 4.17. Zwei τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ sind *elementar äquivalent* (kurz: $\mathfrak{A} \equiv \mathfrak{B}$), wenn $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$, d.h., wenn für alle τ-Sätze ψ gilt:

$$\mathfrak{A} \models \psi \iff \mathfrak{B} \models \psi.$$

Lemma 4.18. *Eine Theorie ist vollständig genau dann, wenn alle ihre Modelle elementar äquivalent sind.*

Beweis. Sei T eine vollständige Theorie. Für jedes Modell $\mathfrak{A} \models T$ gilt $T \subseteq \mathrm{Th}(\mathfrak{A})$ und wegen der Vollständigkeit von T daher sogar $T = \mathrm{Th}(\mathfrak{A})$. Also haben alle Modelle von T dieselbe Theorie.

Wenn andererseits T nicht vollständig ist, dann gibt es einen Satz ψ, so dass sowohl $T \cup \{\psi\}$ und $T \cup \{\neg\psi\}$ erfüllbar sind. T besitzt daher zwei nicht elementar äquivalente Modelle. □

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

Definition 4.19. Der *Quantorenrang* $\mathrm{qr}(\psi)$ einer Formel ψ ist definiert durch:

(1) $\mathrm{qr}(\psi) = 0$ für quantorenfreie ψ

(2) $\mathrm{qr}(\neg\psi) = \mathrm{qr}(\psi)$

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

(4) $\mathrm{qr}(\exists x\psi) = \mathrm{qr}(\forall x\psi) = \mathrm{qr}(\psi) + 1$

Der Quantorenrang ist also die maximale Schachtelungstiefe von Quantoren in der gegebenen Formel.

Beispiel. Der Quantorenrang von $\forall x(\exists yPxy \rightarrow \forall zPxz)$ ist 2. Eine äquivalente Formel in PNF ist $\forall x\forall y\forall z(Pxy \rightarrow Pxz)$. Man beachte, dass die Transformation in PNF in der Regel den Quantorenrang erhöht.

Definition 4.20. Sei $\Phi \subseteq \mathrm{FO}(\tau)$. Der *Boolesche Abschluss* $\langle\Phi\rangle$ von Φ ist die Menge aller Formeln, die aus den Formeln in Φ mit den aussagenlogischen Junktoren $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ gebildet werden können. Formeln in $\langle\Phi\rangle$ heissen *Boolesche Kombinationen* von Formeln aus Φ.

- Wenn $\mathfrak{A} \models \psi(\bar{a})$ gdw. $\mathfrak{B} \models \psi(\bar{b})$, für alle $\psi(\bar{x}) \in \Phi$, dann gilt dies auch für alle $\psi(\bar{x}) \in \langle\Phi\rangle$.
- Jede Formel mit Quantorenrang $\leq m + 1$ ist logisch äquivalent zu einer Boole'schen Kombination von Formeln mit Quantorenrang $\leq m$ und Formeln der Form $\exists x\psi$ mit $\mathrm{qr}(\psi) = m$.

Definition 4.21. Zwei τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ sind *m-äquivalent*, (kurz $\mathfrak{A} \equiv_m \mathfrak{B}$), wenn für alle τ-Sätze ψ mit $\mathrm{qr}(\psi) \leq m$ gilt: $\mathfrak{A} \models \psi$ gdw. $\mathfrak{B} \models \psi$.

Wir erweitern die Begriffe der elementaren Äquivalenz und der m-Äquivalenz auf Strukturen mit Parametern, d.h. in denen zusätzlich gewisse Elemente ausgezeichnet sind. Seien $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen, und $\bar{a} = a_1, \ldots, a_r$, $\bar{b} = b_1, \ldots, b_r$ Tupel von Elementen aus A bzw. B. Dann ist $(\mathfrak{A}, \bar{a}) \equiv (\mathfrak{B}, \bar{b})$, wenn für alle τ-Formeln $\psi(x_1, \ldots, x_r)$ gilt: $\mathfrak{A} \models \psi(\bar{a})$ gdw. $\mathfrak{B} \models \psi(\bar{b})$. Analog definiert man $(\mathfrak{A}, \bar{a}) \equiv_m (\mathfrak{B}, \bar{b})$.

4.5 Der Satz von Ehrenfeucht und Fraïssé

Wir beschränken uns zunächst wieder auf relationale Strukturen.

Satz 4.22 (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) $\mathfrak{A} \cong_e \mathfrak{B}$

(iii) 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) $\mathfrak{A} \cong_m \mathfrak{B}$

(iii) Die Duplikatorin gewinnt $G_m(\mathfrak{A}, \mathfrak{B})$.

Für beide Fälle wurde die Äquivalenz von *(ii)* und *(iii)* bereits im ersten Kapitel bewiesen (Satz 1.18). Wir führen nun zunächst den Beweis, dass eine Gewinnstrategie der Duplikatorin für das Spiel $G(\mathfrak{A}, \mathfrak{B})$ (bzw. für $G_m(\mathfrak{A}, \mathfrak{B})$) die elementare Äquivalenz (bzw. m-Äquivalenz) von $\mathfrak{A}$ und $\mathfrak{B}$ impliziert. Wir beweisen dazu die folgende, etwas stärkere Aussage.

Satz 4.23. *Seien $\mathfrak{A}, \mathfrak{B}$ τ-Strukturen, $\bar{a} = a_1, \dots, a_r \in A$, $\bar{b} = b_1, \dots, b_r \in B$. Wenn es eine Formel $\psi(\bar{x})$ mit $\mathrm{qr}(\psi) = m$ gibt, so dass $\mathfrak{A} \models \psi(\bar{a})$ und $\mathfrak{B} \models \neg\psi(\bar{b})$, dann hat der Herausforderer eine Gewinnstrategie für $G_m(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$.*

Beweis. Sei $m = 0$. Quantorenfreie Formeln sind Boolesche Kombinationen von atomaren Formeln. Wenn $\mathfrak{A}, \bar{a}$ und $\mathfrak{B}, \bar{b}$ durch eine quantorenfreie Formel unterschieden werden, dann also bereits durch ein Atom. Daraus folgt, dass $\{(a_1, b_1), \dots, (a_r, b_r)\}$ kein partieller Isomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ ist, also gewinnt der Herausforderer $G_0(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$.

Sei nun $\mathrm{qr}(\psi) = m > 0$, $\mathfrak{A} \models \psi(\bar{a})$ und $\mathfrak{B} \models \neg\psi(\bar{b})$. Wie bemerkt ist $\psi(\bar{x})$ eine Boolesche Kombination von Formeln der Form $\exists y \varphi(\bar{x}, y)$ mit $\mathrm{qr}(\varphi) \leq m - 1$. Es muss also mindestens eine Formel dieser Gestalt geben, welche $\mathfrak{A}, \bar{a}$ und $\mathfrak{B}, \bar{b}$ unterscheidet. Also entweder

(1) $\mathfrak{A} \models \exists y \varphi(\bar{a}, y)$ und $\mathfrak{B} \models \forall y \neg\varphi(\bar{b}, y)$, oder

(2) $\mathfrak{A} \models \forall y \neg\varphi(\bar{a}, y)$ und $\mathfrak{B} \models \exists y \varphi(\bar{b}, y)$.

Im Fall (1) wählt der Herausforderer im ersten Zug ein $c \in A$ mit $\mathfrak{A} \models \varphi(\bar{a}, c)$. Für jedes beliebige $d \in B$, welches die Duplikatorin wählen kann gilt $\mathfrak{B} \models \neg\varphi(\bar{b}, d)$. Nach Induktionsvoraussetzung gewinnt der Herausforderer das Restspiel $G_{m-1}(\mathfrak{A}, \bar{a}, c, \mathfrak{B}, \bar{b}, d)$. Im Fall (2) gewinnt der Herausforderer, indem er ein $d \in B$ mit $\mathfrak{B} \models \varphi(\bar{b}, d)$ wählt. Die Duplikatorin wählt ein beliebiges $c \in A$. Also ist nach diesem Zug eine Position $(\mathfrak{A}, \bar{a}, c, \mathfrak{B}, \bar{b}, d)$ erreicht, mit $\mathfrak{A} \models \neg\varphi(\bar{a}, c)$ und $\mathfrak{B} \models \varphi(\bar{b}, d)$. Da $\mathrm{qr}(\neg\varphi) = \mathrm{qr}(\varphi) \leq m - 1$ gewinnt der Herausforderer nach Induktionsvoraussetzung das verbleibende Teilspiel $G_{m-1}(\mathfrak{A}, \bar{a}, c, \mathfrak{B}, \bar{b}, d)$. □

Daraus erhalten erhalten wir (indem wir $r = 0$ setzen und also Sätze betrachten) die Implikationen *(iii)* $\Rightarrow$ *(i)* und damit auch *(ii)* $\Rightarrow$ *(i)* des Satzes von Ehrenfeucht und Fraïssé.

(1) $\mathfrak{A} \cong_e \mathfrak{B} \iff$ Die Duplikatorin gewinnt $G(\mathfrak{A}, \mathfrak{B}) \implies \mathfrak{A} \equiv \mathfrak{B}$

(2) $\mathfrak{A} \cong_m \mathfrak{B} \iff$ Die Duplikatorin gewinnt $G_m(\mathfrak{A}, \mathfrak{B}) \implies \mathfrak{A} \equiv_m \mathfrak{B}$.

Beispiel. Die Strukturen $\mathfrak{A} = (\mathbb{Z}, <)$, $\mathfrak{B} = (\mathbb{R}, <)$ lassen sich durch einen Satz ψ vom Quantorenrang 3 trennen, welcher ausdrückt, dass $<$ nicht dicht ist:

$$\psi := \exists x \exists y (x < y \wedge \forall z (\neg x < z \wedge z < y)).$$

Nach dem Satz von Ehrenfeucht-Fraïssé gilt $\mathfrak{A} \not\cong_3 \mathfrak{B}$, d.h. der Herausforderer gewinnt $G_3(\mathfrak{A}, \mathfrak{B})$. (In der Tat haben wir dies bereits in Kapitel 1 festgestellt.) 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.

Anwendung. Dies liefert eine wichtige Methode, um zu zeigen, dass eine Modellklasse $\mathcal{K}$ *nicht* elementar definierbar ist. Wenn es gelingt, Strukturen $\mathfrak{A} \in \mathcal{K}$ und $\mathfrak{B} \notin \mathcal{K}$ zu finden, so dass die Duplikatorin das Spiel $G(\mathfrak{A}, \mathfrak{B})$ gewinnt (d.h. $\mathfrak{A} \cong_e \mathfrak{B}$), dann folgt, dass kein FO-Satz $\mathfrak{A}$ und $\mathfrak{B}$ unterscheiden kann, und damit auch kein FO-Satz $\mathcal{K}$ axiomatisiert.

Eine stärkere Variante der Ehrenfeucht-Fraïssé-Methode besteht darin, Folgen $(\mathfrak{A}_m)_{m \in \mathbb{N}}$, $(\mathfrak{B}_m)_{m \in \mathbb{N}}$ von τ-Strukturen zu konstruieren, so dass für alle m, $\mathfrak{A}_m \in \mathcal{K}$, $\mathfrak{B}_m \notin \mathcal{K}$ und $\mathfrak{A} \cong_m \mathfrak{B}$. Die Annahme, dass $\mathcal{K}$ elementar ist, also $\mathcal{K} = \mathrm{Mod}(\psi)$ für ein $\psi \in \mathrm{FO}(\tau)$, führt nun sofort auf einen Widerspruch: Sei $m = \mathrm{qr}(\psi)$. Da $\mathfrak{A}_m \cong_m \mathfrak{B}_m$, gilt auch $\mathfrak{A}_m \equiv_m \mathfrak{B}_m$. 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 $\mathfrak{B}_m \notin \mathcal{K}$.

Beispiele. (1) Sei $\tau = \varnothing$ und $\mathcal{K}_\infty$ die Klasse aller unendlichen τ-Strukturen, d.h. aller unendlichen Mengen. Wir haben gesehen, dass $\mathcal{K}$ durch eine unendliche Satzmenge Φ_∞ axiomatisiert wird. Mit der Ehrenfeucht-Fraïssé-Methode können wir nun zeigen, dass $\mathcal{K}_\infty$ *nicht* endlich axiomatisierbar ist.

Für alle $m \in \mathbb{N}$, setze $\mathfrak{A}_m = \mathbb{N}$ und $\mathfrak{B}_m = \{1, \ldots, m\}$. Offensichtlich gewinnt die Duplikatorin das Spiel $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$, also trennt kein Satz $\psi \in \mathrm{FO}(\varnothing)$ die endlichen von den unendlichen Mengen.

(2) Eine *Wohlordnung* ist eine lineare Ordnung ohne unendliche absteigende Ketten (siehe Kapitel 1.3). Wir zeigen, dass die Klasse der Wohlordnungen nicht endlich axiomatisierbar ist. Sei $\mathfrak{A} = (\mathbb{N}, <)$ und $\mathfrak{B} = (\mathbb{N}, <) + (\mathbb{Z}, <)$, d.h. $(\mathbb{N}, <)$ und 'dahinter' eine Kopie von $(\mathbb{Z}, <)$. Formaler: $\mathfrak{B}$ ist eine lineare Ordnung $(C \cup D, <)$ mit $C \cap D = \varnothing$, für die von C bzw. D induzierten Substrukturen gilt $(C, <) \cong (\mathbb{N}, <)$ und $(D, <) \cong (\mathbb{Z}, <)$ und es gilt $c < d$ für alle $c \in C, d \in D$.

Offensichtlich ist $\mathfrak{A}$ eine Wohlordnung und $\mathfrak{B}$ keine Wohlordnung. Es bleibt zu zeigen, dass $\mathfrak{A} \cong_e \mathfrak{B}$. Dies folgt mit denselben Argumenten, mit denen wir am Ende von Kapitel 1 die endliche Isomorphie von $(\mathbb{Z}, <)$ und $(\mathbb{Z}, <) + (\mathbb{Z}, <)$ bewiesen haben. Zum Beispiel ist jede endliche Restriktion des (eindeutig bestimmten) Isomorphismus von $(A, <)$ auf $(C, <)$ m-fach erweiterbar, für jedes endliche m.

***Elementare Äquivalenz impliziert endliche Isomorphie.** Es bleibt noch die Implikation *(i)* $\Rightarrow$ *(ii)* des Satzes von Ehrenfeucht und Fraïssé zu zeigen:

(1) $\mathfrak{A} \equiv \mathfrak{B} \implies \mathfrak{A} \cong_e \mathfrak{B}$

(2) $\mathfrak{A} \equiv_m \mathfrak{B} \implies \mathfrak{A} \cong_m \mathfrak{B}$.

Aus der zweiten Implikation (für alle $m \in \mathbb{N}$) folgt die erste unmittelbar. Wir erinnern an die Voraussetzung, dass τ endlich und relational ist.

Für $m, r \in \mathbb{N}$, (wobei m und r nicht beide 0 sein sollen), sei

$$\boldsymbol{C}(m,r) := \{(\mathfrak{A}, a_1, \ldots, a_r) : \mathfrak{A} \in \mathrm{Str}(\tau), a_1, \ldots, a_r \in A\}/_{\cong_m}$$

die Menge der $\cong_m$-Äquivalenzklassen von τ-Strukturen mit r ausgezeichneten Parametern. Wir werden zeigen, dass jede Äquivalenzklasse $\mathcal{C} \in \boldsymbol{C}(m,r)$ durch eine Formel $\psi_{\mathcal{C}}(x_1, \ldots, x_r)$ beschrieben wird, so dass gilt

(1) Der Quantorenrang von $\psi_{\mathcal{C}}$ ist m,

(2) $(\mathfrak{A}, \bar{a}) \in \mathcal{C} \iff \mathfrak{A} \models \psi_{\mathcal{C}}(\bar{a})$.

Aus dem Spezialfall $r = 0$ können wir die gewünschte Behauptung sofort ableiten: Wenn $\mathfrak{A} \equiv_m \mathfrak{B}$, dann gilt insbesondere

$$\mathfrak{A} \models \psi_{\mathcal{C}} \iff \mathfrak{B} \models \psi_{\mathcal{C}}$$

für alle $\mathcal{C} \in \boldsymbol{C}(m,0)$ (da $\mathrm{qr}(\psi_{\mathcal{C}}) = m$). Also liegen $\mathfrak{A}$ und $\mathfrak{B}$ in derselben $\cong_m$-Äquivalenzklasse.

Wir überlegen uns nun, per Induktion nach m, dass die Mengen $\boldsymbol{C}(m,r)$ alle endlich sind und konstruieren die Formeln $\psi_{\mathcal{C}}(\bar{x})$.

Sei $m = 0$ und $\Phi(r)$ die Menge aller τ-Atome mit (höchstens) den Variablen $x_1, \ldots, x_r$. Da die Signatur endlich und relational, ist $\Phi(0)$ leer und $\Phi(r)$ endlich für alle r.

Für ein $\mathfrak{A}, \mathfrak{B} \in \mathrm{Str}(\tau)$, $\bar{a} \in A^r$, $\bar{b} \in B^r$ ist $(\mathfrak{A}, \bar{a}) \cong_0 (\mathfrak{B}, \bar{b})$ genau, dann wenn für alle τ-Atome $\varphi(x_1, \ldots, x_r)$ gilt

$$\mathfrak{A} \models \varphi(\bar{a}) \iff \mathfrak{B} \models \varphi(\bar{b}).$$

Also ist $|\boldsymbol{C}(0,r)| \leq 2^{|\Phi(r)|}$. Sei nun $\mathcal{C}$ eine Äquivalenzklasse in $\boldsymbol{C}(0,r)$ und $(\mathfrak{A}, \bar{a})$ ein Repräsentant von $\mathcal{C}$. Mit $\overline{\Phi}(r)$ bezeichnen wir die Menge $\Phi(r) \cup \{\neg\varphi : \varphi \in \Phi(r)\}$ aller Atome und negierten Atome in $x_1, \ldots, x_r$. Dann ist $\mathcal{C}$ charakterisiert durch die quantorenfreie Formel

$$\psi_{\mathcal{C}} := \bigwedge \Big\{ \varphi(\bar{x}) : \varphi \in \overline{\Phi}(r), \mathfrak{A} \models \varphi(\bar{a}) \Big\}.$$

(Für endliche Formelmengen Γ bezeichnet $\bigwedge \Gamma$ die Konjunktion über alle Formeln aus Γ.) In der Tat gilt offensichtlich

$$(\mathfrak{B}, \bar{b}) \in \mathcal{C} \iff (\mathfrak{A}, \bar{a}) \cong_0 (\mathfrak{B}, \bar{b}) \iff \mathfrak{B} \models \psi_{\mathcal{C}}(\bar{b}).$$

Wir kommen zum Induktionsschritt. Nach Definition der m-Isomorphie ist $(\mathfrak{A}, a_1, \ldots, a_r)$ $\cong_{m+1}$ $(\mathfrak{B}, b_1, \ldots, b_r)$ genau dann, wenn für alle $a_{r+1} \in A$ ein $b_{r+1} \in B$, und für alle $b_{r+1} \in B$ ein $a_{r+1} \in A$ existiert, so dass $(\mathfrak{A}, \bar{a}, a_{r+1}) \cong_m (\mathfrak{B}, \bar{b}, b_{r+1})$. Mit andern Worten: $(\mathfrak{A}, \bar{a}) \cong_{m+1} (\mathfrak{B}, \bar{b})$ genau dann, wenn $(\mathfrak{A}, \bar{a})$ und $(\mathfrak{B}, \bar{b})$ zu denselben Äquivalenzklassen $\mathcal{C} \in \boldsymbol{C}(m, r+1)$ erweiterbar sind. Sei

$$\mathrm{Erw}(\mathfrak{A}, \bar{a}) := \Big\{ \mathcal{C} \in \boldsymbol{C}(m, r+1) : \text{ es gibt ein } a_{r+1}, \text{ so dass } (\mathfrak{A}, \bar{a}, a_{r+1}) \in \mathcal{C} \Big\}.$$

Wir haben also gezeigt, dass

$$(\mathfrak{A}, \bar{a}) \cong_{m+1} (\mathfrak{B}, \bar{b}) \iff \mathrm{Erw}(\mathfrak{A}, \bar{a}) = \mathrm{Erw}(\mathfrak{B}, \bar{b}).$$

Da jede Menge $\mathrm{Erw}(\mathfrak{A}, \bar{a}) \subseteq \boldsymbol{C}(m, r+1)$, ist $|\boldsymbol{C}(m+1, r)| \leq 2^{|\boldsymbol{C}(m,r+1)|}$ und daher endlich. Um eine Äquivalenzklasse $\mathcal{C} \in \boldsymbol{C}(m+1, r)$ zu charakterisieren, genügt es also, die Menge ihrer Erweiterungen in $\boldsymbol{C}(m, r+1)$ zu beschreiben. Sei $(\mathfrak{A}, \bar{a})$ ein Repräsentant von $\mathcal{C}$. Setze

$$\begin{aligned}\psi_{\mathcal{C}}(\bar{x}) := \bigwedge\Big\{\exists x_{r+1}\psi_{\mathcal{D}}(\bar{x}, x_{r+1}) : \mathcal{D} \in \mathrm{Erw}(\mathfrak{A}, \bar{a})\Big\}\wedge \\ \bigwedge\Big\{\neg\exists x_{r+1}\psi_{\mathcal{D}}(\bar{x}, x_{r+1}) : \mathcal{D} \in \boldsymbol{C}(m, r+1) - \mathrm{Erw}(\mathfrak{A}, \bar{a})\Big\}.\end{aligned}$$

Offensichtlich hat ψ_C Quantorenrang $m+1$ und es gilt

$$(\mathfrak{B}, \bar{b}) \in C \iff \mathrm{Erw}(\mathfrak{A}, \bar{a}) = \mathrm{Erw}(\mathfrak{B}, \bar{b}) \iff \mathfrak{B} \models \psi_{\mathcal{C}}(\bar{b}).$$

Damit ist der Satz von Ehrenfeucht-Fraïssé bewiesen.

Elimination von Funktionen. Die Beschränkung auf relationale Strukturen ist nicht essentiell, denn man kann jeder τ-Struktur $\mathfrak{A}$ eine relationale Struktur $\mathfrak{A}_{\mathrm{rel}}$ so zuordnen, dass gilt:

$$\mathfrak{A} \equiv \mathfrak{B} \iff \mathfrak{A}_{\mathrm{rel}} \equiv \mathfrak{B}_{\mathrm{rel}}.$$

Die zugehörige relationale Signatur τ_{rel} enthält die Relationssymbole von τ, und zusätzlich für jedes n-stellige Funktionssymbol f von τ ein neues $(n+1)$-stelliges Relationssymbol R_f, welches in $\mathfrak{A}_{\mathrm{rel}}$ durch den Graph von $f^{\mathfrak{A}}$ interpretiert wird.

Lemma 4.24. *Zu jeder Formel $\psi(\bar{x}) \in \mathrm{FO}(\tau)$ kann man eine Formel $\psi_{rel}(\bar{x}) \in \mathrm{FO}(\tau_{rel})$ konstruieren, und umgekehrt auch zu jedem $\psi_{rel} \in \mathrm{FO}(\tau_{rel})$ ein Formel $\psi \in \mathrm{FO}(\tau)$ so dass für alle τ-Strukturen $\mathfrak{A}$ und alle $\bar{a}$ gilt:*

$$\mathfrak{A} \models \psi(\bar{a}) \iff \mathfrak{A}_{rel} \models \psi_{rel}(\bar{a}).$$

Beweis. Zunächst transformiere man $\psi \in \mathrm{FO}(\tau)$ in eine äquivalente termreduzierte Formel, gemäss Lemma 2.19. Aus einem termreduzierten $\psi(\bar{x})$ erhält man die gewünschte Formel $\psi_{\mathrm{rel}}(\bar{x})$, indem man alle Atome der Form $f\bar{y} = z$ durch $R_f\bar{y}z$ ersetzt.

Umgekehrt erhält man aus ψ_{rel} durch Ersetzen von Atomen $R_f\bar{y}z$ durch $f\bar{y} = z$ eine τ-Formel mit den gewünschten Eigenschaften. □

Korollar 4.25. *Für alle τ-Strukturen $\mathfrak{A}, \mathfrak{B}$ gilt:*

$$\mathfrak{A} \equiv \mathfrak{B} \iff \mathfrak{A}_{rel} \equiv \mathfrak{B}_{rel}.$$

Kapitel 5

Vollständigkeit und Kompaktheit

5.1 Der Sequenzenkalkül

Wir erweitern den in Kapitel 3.4 beschriebenen aussagenlogischen Sequenzenkalkül auf die Prädikatenlogik.

Durch Einführen neuer Konstantensymbole können wir uns auf die Betrachtung von Sätzen beschränken und so die etwas lästigen Komplikationen vermeiden, die sich aus Konflikten zwischen freien und gebundenen Variablen ergeben können. Sei σ eine beliebige Signatur und seien $c_1, c_2, \dots$ abzählbar viele, paarweise verschiedene und nicht in σ enthaltene Konstantensymbole. Wenn wir jede Formel $\psi(x_1, \dots, x_n)$ mit den freien Variablen $x_1, \dots, x_n$ durch den Satz $\psi(c_1, \dots, c_n)$ ersetzten, dann können wir alle Fragen über Gültigkeit, Erfüllbarkeit und die Folgerungsbeziehung auf Sätze reduzieren.

Im Folgenden bezeichnet σ eine beliebige abzählbare Signatur und $\tau = \sigma \cup C$ für eine abzählbar unendliche Menge C von Konstanten, welche nicht in σ enthalten sind. Wenn von $\psi \in \mathrm{FO}(\tau)$ oder $\Gamma \subseteq \mathrm{FO}(\tau)$ die Rede ist, sind immer Sätze bzw. Satzmengen gemeint, es sei denn, wir deuten durch die Notation $\psi(x)$ explizit an, dass x in ψ frei vorkommt.

Definition 5.1. Eine *Sequenz* ist ein Ausdruck $\Gamma \Rightarrow \Delta$, wobei Γ, Δ endliche Mengen von Sätzen in $\mathrm{FO}(\tau)$ sind. Eine Sequenz $\Gamma \Rightarrow \Delta$ ist *korrekt*, wenn jedes Modell von Γ auch ein Modell mindestens einer Formel aus Δ ist. Die *Axiome* des Sequenzenkalküls sind alle Sequenzen der Form $\Gamma, \psi \Rightarrow \Delta, \psi$. Die *Schlussregeln* sind dieselben wie beim aussagenlogischen Sequenzenkalkül, erweitert um die Gleichheitsregel, die Substitutionsregeln und die Einführungsregeln für die Quantoren $\exists$ und $\forall$.

Die Gleichheitsregel ist

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

Die Substitutionsregeln erlauben das Austauschen von Termen. Die Schreibweise $t \doteq t'$ deutet an, dass entweder $t = t'$ oder $t' = t$ benutzt werden kann.

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

Hier stehen t, t' für beliebige konstante Terme aus $T(\tau)$; $\psi(x)$ ist eine beliebige Formel aus $\mathrm{FO}(\tau)$, in der keine andere Variable als x frei vorkommt, und $\psi(t)$ ist die Formel, die man daraus durch Substitution von t für x erhält.

Die Korrektheit der Gleichheitsregel ist trivial. Es ist auch leicht einzusehen, dass die Substitutionsregeln korrekt sind. Wir erläutern dies für $(\Rightarrow S)$: Sei $\Gamma \Rightarrow \Delta, \psi(t)$ eine gültige Sequenz, und $\mathfrak{A}$ ein Modell von $\Gamma, t \doteq t'$. Zu zeigen ist, dass $\mathfrak{A}$ dann entweder Modell einer Formel aus Δ oder Modell von $\psi(t')$ ist. Nehmen wir also an, dass in $\mathfrak{A}$ alle Formeln aus Δ falsch sind. Aber dann folgt $\mathfrak{A} \models \psi(t)$, denn $\Gamma \Rightarrow \Delta, \psi(t)$ ist gültig und $\mathfrak{A} \models \Gamma$. Da aber auch $\mathfrak{A} \models t = t'$, folgt $\mathfrak{A} \models \psi(t')$.

Die Einführungsregeln für $\exists$ und $\forall$ haben folgende Form:

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

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

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

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

Beispiele. (1) Hier ist ein Beweis für die gültige Sequenz $\exists x \forall y Rxy \Rightarrow \forall y \exists x Rxy$, welcher die Anwendung der Quantorenregeln illustriert:

$Rcd \Rightarrow Rcd$	Axiom
$Rcd \Rightarrow \exists x Rxd$	$(\Rightarrow \exists)$
$\forall y Rcy \Rightarrow \exists x Rxd$	$(\forall \Rightarrow)$
$\forall y Rcy \Rightarrow \forall y \exists x Rxy$	$(\Rightarrow \forall)$
$\exists x \forall y Rxy \Rightarrow \forall y \exists x Rxy$	$(\exists \Rightarrow)$

(2) Um die Sequenz $Rfc, \forall x(fx = x) \Rightarrow Rffc$ abzuleiten, beginnt man mit dem Axiom $Rfc \Rightarrow Rfc$. Wenn wir $\psi(x) := Rfx$ wählen, dann ist dies die Sequenz $Rfc \Rightarrow \psi(c)$. Mit der Regel $(\Rightarrow S)$ können wir daraus die Sequenz $Rfc, fc = c \Rightarrow \psi(fc)$, also $Rfc, fc = c \Rightarrow Rffc$ ableiten. Durch Anwendung der Regel $(\forall \Rightarrow)$ erhalten wir daraus eine Ableitung von $Rfc, \forall x(fx = x) \Rightarrow Rffc$.

Übung 5.1. Beweisen Sie die Korrektheit der Quantorenregeln. Zeigen Sie, dass in den Regeln $(\exists \Rightarrow)$ und $(\Rightarrow \forall)$ die Bedingung, dass c nicht in Γ, ψ und Δ vorkommt, nicht weggelassen werden kann.

Die weiteren wesentlichen Begriffe können unmittelbar vom aussagenlogischen Sequenzenkalkül übernommen werden:

Die Menge der *ableitbaren Sequenzen* ist die kleinste Menge, welche alle Axiome umfasst und mit jeder Instanz der oberen Zeile einer Schlussregel auch die entsprechende Instanz der unteren Zeile enthält. Ein *Beweis* ist ein beschrifteter Baum, so dass alle Blätter mit Axiomen, alle inneren Knoten mit der Konklusion einer Schlussregel und deren Kinder mit den Prämissen derselben Regel beschriftet sind. Tabelle 5.1 fasst alle Regeln des Sequenzenkalküls nochmals zusammen.

Tabelle 5.1: Die Regeln des Sequenzenkalküls

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

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

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

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

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

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

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

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

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

wenn c in Γ, Δ und $\psi(x)$ nicht vorkommt

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

Satz 5.2 (Korrektheitssatz für den Sequenzenkalkül). *Jede im Sequenzenkalkül ableitbare Sequenz ist gültig.*

5.2 Ableitbarkeit in Theorien

Aus dem Sequenzenkalkül erhält man auch einen Ableitungsbegriff für einen einzelnen Satz oder eine Sequenz aus einer Menge von Hypthesen, z.B. aus den Axiomen einer mathematischen Theorie.

Definition 5.3. Sei $\Phi \subseteq \mathrm{FO}(\sigma)$ eine Menge von Sätzen. Ein Satz ψ ist *ableitbar* aus dem Axiomensystem Φ, (kurz $\Phi \vdash \psi$), wenn eine endliche Teilmenge Γ von Φ existiert, so dass die Sequenz $\Gamma \Rightarrow \psi$ im Sequenzenkalkül ableitbar ist. Eine Sequenz $\Gamma \Rightarrow \Delta$ ist ableitbar aus Φ, wenn es eine ableitbare Sequenz $\Gamma, \Gamma' \Rightarrow \Delta$ gibt mit $\Gamma' \subseteq \Phi$.

Die Ableitbarkeit von Sequenzen und die Ableitbarkeit von einzelnen Sätzen sind im Wesentlichen austauschbare Begriffe, denn die Sequenz $\Gamma \Rightarrow \Delta$ ist ableitbar aus Φ genau dann, wenn $\Phi \vdash \bigwedge \Gamma \rightarrow \bigvee \Delta$.

Es gibt auch Satzmengen Φ aus denen *jeder* Satz (der entsprechenden Signatur) ableitbar ist. Eine solche Menge nennen wir *inkonsistent*. Aufgrund der Korrektheit des Sequenzenkalküls sind inkonsistente Mengen unerfüllbar.

Beispiel. Jede Menge, welche einen Satz und gleichzeitig auch dessen Negation enthält, ist inkonsistent. In der Tat können wir jede Sequenz der Form $\psi, \neg\psi \Rightarrow \varphi$ mit der Regel $(\neg \Rightarrow)$ aus dem Axiom $\psi \Rightarrow \psi, \varphi$ ableiten.

Wenn nicht jeder Satz aus Φ ableitbar ist, dann nennen wir Φ *konsistent*. Offensichtlich ist Φ konsistent genau dann, wenn jede endliche Teilmenge von Φ konsistent ist. Man beachte, dass Konsistenz und Ableitbarkeit $(\vdash)$ *syntaktische* Begriffe sind, da sie sich auf Formelmengen und Sätze als sprachliche Objekte und nicht auf ihre Bedeutung beziehen. Die zugehörigen semantischen Begriffe sind die Erfüllbarkeit und die Folgerungsbeziehung $(\models)$.

Der Korrektheitssatz für den Sequenzenkalkül impliziert: Wenn $\Phi \vdash \psi$, dann auch $\Phi \models \psi$. Im nächsten Abschnitt werden wir den Vollständigkeitssatz beweisen, welcher besagt, dass auch die Umkehrung gilt.

5.3 Der Vollständigkeitssatz

Satz 5.4 (Vollständigkeitssatz für den Sequenzenkalkül). *Für jede Satzmenge* $\Phi \subseteq \mathrm{FO}(\sigma)$ *und jeden Satz* $\psi \in \mathrm{FO}(\sigma)$ *gilt:*

(i) $\Phi \models \psi \iff \Phi \vdash \psi$

(ii) Φ *erfüllbar* $\iff$ Φ *konsistent.*

Wir werden den Vollständigkeitssatz beweisen, indem wir für jede beliebige, nicht aus Φ ableitbare Sequenz $\Gamma \Rightarrow \Delta$ ein Modell $\mathfrak{A}$ von $\Phi \cup \Gamma \cup \neg\Delta$ konstruieren. Dabei ist $\neg\Delta := \{\neg\psi : \psi \in \Delta\}$.

Daraus erhalten wir sofort die beiden Aussagen des Vollständigkeitssatzes:

(i) Wir wissen bereits, dass $\Phi \vdash \psi \;\Rightarrow\; \Phi \models \psi$. Wenn $\Phi \nvdash \psi$, dann ist insbesondere die Sequenz $\varnothing \Rightarrow \psi$ nicht aus Φ ableitbar. Die Existenz eines Modells $\mathfrak{A} \models \Phi \cup \{\neg\psi\}$ bedeutet aber, dass $\Phi \not\models \psi$.

(ii) Wir wissen bereits, dass jede erfüllbare Menge konsistent ist. Sei umgekehrt Φ konsistent. Dann gibt es ein ψ, so dass $\Phi \not\vdash \psi$ und daher (nach *(i)*) auch $\Phi \not\models \psi$. Also ist $\Phi \cup \{\neg\psi\}$ und daher insbesondere Φ erfüllbar.

Wenn wir $\Phi = \varnothing$ setzen, zeigt dies insbesondere, dass jede gültige Sequenz im Sequenzenkalkül ableitbar ist.

Es bleibt also die Aufgabe, für jede nicht aus Φ ableitbare Sequenz $\Gamma \Rightarrow \Delta$ ein Modell von $\Phi \cup \Gamma \cup \neg\Delta$ zu konstruieren

5.3.1 Herbrandstrukturen und kanonische Modelle

Als Vorbereitung für die Modellkonstruktion behandeln wir Mengen von atomaren Sätzen. Wir definieren den Begriff einer Herbrandstruktur und konstruieren daraus, durch Übergang zu einer geeigneten Quotientenstruktur, für jede unter Substitution abgeschlossenen Menge von atomaren Aussagen das sogenannte *kanonische Modell*.

Definition 5.5. Eine *Herbrandstruktur* zu einer Signatur τ ist eine τ-Struktur $\mathfrak{H}$, deren Universum die Menge aller konstanten τ-Terme ist und deren Funktionssymbole durch ihre natürliche Operation auf den Termen interpretiert werden: Für n-stelliges $f \in \tau$ ist $f^{\mathfrak{H}}(t_1, \dots, t_n) := ft_1 \cdots t_n$. Die Interpretation der Relationssymbole aus τ ist beliebig.

Eine Herbrandstruktur $\mathfrak{H}$ ist eine Struktur, deren algebraisches Redukt gerade die Termalgebra über der leeren Variablenmenge ist. Beachte, dass in $\mathfrak{H}$ jeder konstante Term durch sich selbst interpretiert ist: $t^{\mathfrak{H}} = t$.

Sei Σ eine Menge von atomaren τ-Sätzen. Mit $\mathfrak{H}(\Sigma)$ bezeichnen wir die Herbrandstruktur mit folgender Interpretation der Relationssymbole: Für n-stelliges $R \in \tau$ ist

$$R^{\mathfrak{H}(\Sigma)} = \{(t_1, \dots, t_n) : Rt_1 \cdots t_n \in \Sigma\}.$$

Im Allgemeinen ist $\mathfrak{H}(\Sigma)$ *kein* Modell von Σ: Seien t und t' zwei (syntaktisch) verschiedene Terme, so dass aber Σ die Formel $t = t'$ enthält. Dann ist $\mathfrak{H}(\Sigma)$ Modell von $t \neq t'$ und daher kein Modell von Σ. Es ist also offensichtlich notwendig, Gleichheiten herauszufaktorisieren.

Definition 5.6. Eine Menge Σ von atomaren Sätzen in $\mathrm{FO}(\tau)$ ist *abgeschlossen unter Substitution*, wenn für jede atomare Formel $\psi(x)$ und alle konstanten Terme $t, t' \in T(\tau)$ gilt:

(i) Σ enthält die Gleichung $t = t$.

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

Beispiel. Sei $\mathfrak{A}$ eine τ-Struktur und Σ die Menge aller atomaren Sätze φ, so dass $\mathfrak{A} \models \varphi$. Dann ist Σ abgeschlossen unter Substitution.

Für beliebige konstante Terme $t, t' \in T(\tau)$ setzen wir nun: $t \sim t'$ genau dann, wenn Σ die Formel $t = t'$ enthält.

Lemma 5.7. *Sei Σ abgeschlossen unter Substitution. Dann ist $\sim$ eine Kongruenzrelation auf $\mathfrak{H}(\Sigma)$.*

Beweis. Wir zeigen zuerst, dass $\sim$ eine Äquivalenzrelation ist. Nach Bedingung *(i)* von Definition 5.6 ist $\sim$ reflexiv. Sei nun $t \sim t'$ und also $t = t' \in \Sigma$. Wenn $\psi(x)$ die Formel $x = t$ ist, dann ist $\psi(t)$ die Gleichung $t = t$ und also in Σ. Nach Bedingung *(ii)* von Definition 5.6 enthält Σ dann auch $\psi(t')$; dies ist aber gerade die Gleichung $t' = t$. Also folgt $t' \sim t$. Schliesslich nehmen wir an, dass $t \sim t'$ und $t' \sim t''$. Sei $\psi(x)$ die Formel $t = x$. Also enthält Σ $\psi(t')$ und daher auch $\psi(t'')$; dies ist aber die Gleichung $t = t''$. Also $t \sim t''$.

Es bleibt zu zeigen, dass $\sim$ mit den Funktionen und Relationen von $\mathfrak{H}(\Sigma)$ kompatibel ist. Sei f ein n-stelliges Funktionssymbol und seien $s_1 \sim t_1, \dots, s_n \sim t_n$. Wir müssen zeigen, dass $fs_1 \cdots s_n \sim ft_1 \cdots t_n$. Zu diesem Zweck sei $\psi_i(x)$ die Gleichung $fs_1 \cdots s_n = ft_1 \cdots t_{i-1}xs_{i+1} \cdots s_n$ für $i = 1, \dots, n$. 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 $s_1 \sim t_1, \dots, s_n \sim t_n$ folgt

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

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

Wir können also die Faktorstruktur $\mathfrak{A}(\Sigma) := \mathfrak{H}(\Sigma)/_\sim$ bilden. Wir bezeichnen mit $[t]$ die Äquivalenzklasse von t bezüglich $\sim$; das Universum von $\mathfrak{A}(\Sigma)$ ist also die Menge $\{[t] : t$ konstanter Term in $T(\tau)\}$ der Äquivalenzklassen aller konstanten Terme. Offensichtlich wird in $\mathfrak{A}(\Sigma)$ jeder konstante Term t durch seine Äquivalenzklasse interpretiert: $t^{\mathfrak{A}(\Sigma)} = [t]$. Unmittelbar aus der Definition folgt:

Lemma 5.8. *Für jeden atomaren Satz ψ aus $\mathrm{FO}(\tau)$ gilt: $\mathfrak{A}(\Sigma) \models \psi \iff \psi \in \Sigma$.*

$\mathfrak{A}(\Sigma)$ heisst das *kanonische Modell* von Σ. Leider lässt sich Lemma 5.8 nicht direkt auf Mengen von nicht-atomaren Sätzen übertragen. Betrachte etwa die Menge $\Sigma := \{t = t : t \text{ ein konstanter Term}\} \cup \{\exists x Rx\}$. Diese Menge ist trivialerweise abgeschlossen unter Substitution, enthält aber keine Aussage der Form Rt. Daher ist $R^{\mathfrak{A}(\Sigma)} = \varnothing$ und also $\mathfrak{A}(\Sigma) \not\models \exists x Rx$. Analoges gilt für die Menge $\{t = t : t \text{ ein konstanter Term}\} \cup \{Rx \vee Ry\}$. Man sieht aus diesen Beispielen, dass Σ neben der Abgeschlossenheit unter Substitution noch weitere Abschlusseigenschaften besitzen muss, damit $\mathfrak{A}(\Sigma) \models \Sigma$ gilt.

5.3.2 Hintikka-Mengen und Modell-Existenz-Satz

Sei $\Gamma \Rightarrow \Delta$ eine nicht aus Φ ableitbare Sequenz. Wir werden eine unendliche Folge von nicht aus Φ ableitbaren Sequenzen $\Gamma_n \Rightarrow \Delta_n$ konstruieren und damit eine Satzmenge gewinnen, welche $\Phi \cup \Gamma \cup \neg\Delta$ umfasst und welche hinreichende Abschlusseigenschaften besitzt, um zu garantieren, dass die dadurch definierte kanonische Struktur ein Modell von $\Phi \cup \Gamma \cup \neg\Delta$ ist.

Um den Beweis zu vereinfachen, beschränken wir uns auf reduzierte Sätze (d.h. solche, die aus den Atomen mittels $\vee, \neg$ und $\exists$ aufgebaut sind).

Obwohl wir im Sequenzenkalkül auch Schlussregeln für $\wedge, \rightarrow$ und $\forall$ angegeben haben, bedeutet die Reduktion auf reduzierte Sätze keine Einschränkung der Allgemeinheit: Sei etwa $\Gamma_0 \Rightarrow \Delta_0$ eine nicht-ableitbare Sequenz bestehend aus beliebigen Sätzen und sei $\Gamma_1 \Rightarrow \Delta_1$ die Sequenz, die wir erhalten, indem wir jeden Satz durch eine äquivalente reduzierte Variante ersetzen.

Zunächst überlegt man, dass auch $\Gamma_1 \Rightarrow \Delta_1$ nicht ableitbar ist. Wir zeigen exemplarisch, dass die Ableitung einer Sequenz der Form $\Gamma, (\psi \wedge \varphi) \Rightarrow \Delta$ aus $\Gamma, \psi \Rightarrow \Delta$ und $\Gamma, \varphi \Rightarrow \Delta$ mittels der Regel $(\wedge \Rightarrow)$ simuliert werden kann durch eine Ableitung der äquivalenten Sequenz $\Gamma, \neg(\neg\psi \vee \neg\varphi) \Rightarrow \Delta$ mit den Regeln $(\Rightarrow \neg), (\neg \Rightarrow)$ und $(\Rightarrow \vee)$.

$$\cfrac{\cfrac{\cfrac{\Gamma, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\psi} \qquad \cfrac{\Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}}{\Gamma \Rightarrow \Delta, (\neg\psi \vee \neg\varphi)}}{\Gamma \neg(\neg\psi \vee \neg\varphi) \Rightarrow \Delta}$$

Die Argumentation für Sequenzen mit Sätzen der Form $\psi \rightarrow \varphi$ und $\forall x \psi(x)$ ist analog.

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

Sei $\Phi \subseteq \mathrm{FO}(\sigma)$ und sei $\tau = \sigma \cup C$ für eine abzählbar unendliche Menge von neuen Konstantensymbolen. Wir fixieren zunächst eine Aufzählung $(\varphi_0, t_0), (\varphi_1, t_1), \dots$, in der jedes Paar (φ, t), bestehend aus einem Satz $\varphi \in \mathrm{FO}(\tau)$ und einem konstanten Term $t \in T(\tau)$ unendlich oft vorkommt, und eine Aufzählung $\psi_0(x_0), \psi_1(x_1), \dots$ aller atomaren $\mathrm{FO}(\tau)$-Formeln mit genau einer freien Variablen.

Wir definieren induktiv aufsteigende Folgen $\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots$ und $\Delta_0 \subseteq \Delta_1 \subseteq \cdots$ wie folgt: Sei $\Gamma_0 := \Gamma$ und $\Delta_0 := \Delta$. Wir nehmen nun an, Γ_n und Δ_n seien bereits konstruiert und $\Gamma_n \Rightarrow \Delta_n$ sei nicht aus Φ ableitbar.

(a) Sei φ_n eine Formel aus Φ oder eine Gleichung $t = t$. Dann setze $\Gamma_{n+1} := \Gamma_n, \varphi_n$ und $\Delta_{n+1} := \Delta_n$.

Die Sequenz $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ ist nicht aus Φ ableitbar, denn sonst wäre auch $\Gamma_n \Rightarrow \Delta_n$ aus Φ ableitbar.

(b) Sei φ_n von der Gestalt $t = t'$. Wenn $\varphi_n \in \Gamma_n$ und ein $m \in \mathbb{N}$ existiert, so dass $\psi_m(t') \in \Gamma_n$, aber $\psi_m(t) \notin \Gamma_n$, dann wähle das kleinste solche m und setze $\Gamma_{n+1} := \Gamma_n, \psi_m(t)$ und $\Delta_{n+1} := \Delta_n$.

Die Sequenz $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ ist nicht aus Φ ableitbar, denn sonst würde mit Regel $(S \Rightarrow)$ folgen, dass auch $\Gamma_n, t = t', \psi_m(t') \Rightarrow \Delta_n$ ableitbar ist. Da $t = t'$ und $\psi_m(t')$ bereits in Γ_n enthalten sind, wäre also $\Gamma_n \Rightarrow \Delta_n$ ableitbar, im Widerspruch zur Induktionsannahme.

(c) Sei $\varphi_n := \neg\psi$. Wenn $\varphi_n \in \Gamma_n$, dann setze $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} := \Delta_n, \psi$. Wenn $\varphi_n \in \Delta_n$, dann setze $\Gamma_{n+1} := \Gamma_n, \psi$ und $\Delta_{n+1} := \Delta_n$.

Mit den Regeln $(\neg \Rightarrow)$ und $(\Rightarrow \neg)$ folgt, dass $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ nicht aus Φ ableitbar ist.

(d) Sei $\varphi_n = \psi \vee \vartheta$. Wenn $\varphi_n \in \Gamma_n$, dann setzen wir $\Delta_{n+1} := \Delta_n$ und können aufgrund der Regel $(\vee \Rightarrow)$ entweder $\Gamma_{n+1} := \Gamma_n, \psi$ oder $\Gamma_{n+1} := \Gamma_n, \vartheta$ so wählen, dass $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$

nicht ableitbar ist. Wenn $\varphi_n \in \Delta_n$, dann setzen wir $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} = \Delta_n, \psi, \vartheta$ und verwenden die Regel ($\Rightarrow \vee$).

(e) Sei φ_n von der Gestalt $\exists x \psi(x)$. Wenn $\varphi_n \in \Gamma_n$, dann wähle ein $c \in C$, welches in Γ_n und Δ_n nicht vorkommt. Setze $\Gamma_{n+1} := \Gamma_n, \psi(c)$ und $\Delta_{n+1} := \Delta_n$. Die Sequenz $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ ist nicht ableitbar; andernfalls würde (da c in Φ, Γ_n und Δ_n nicht vorkommt) mit der Regel ($\exists \Rightarrow$) folgen, dass auch $\Gamma_n, \exists x \psi(x) \Rightarrow \Delta_n$ und also $\Gamma_n \Rightarrow \Delta_n$ aus Φ ableitbar wäre.

Wenn $\varphi_n \in \Delta_n$, dann setze $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} = \Delta_n, \psi(t_n)$. Mit Regel ($\Rightarrow \exists$) folgt, dass $\Gamma_{n+1} \Rightarrow \Delta_{n+1}$ nicht ableitbar ist.

In allen andern Fällen sei $\Gamma_{n+1} := \Gamma_n$ und $\Delta_{n+1} := \Delta_n$. Man beachte, dass aufgrund von Schritt (a) der Konstruktion Φ in $\bigcup_{n\in\mathbb{N}} \Gamma_n$ enthalten ist.

Lemma 5.9. *Die Mengen $\Gamma^* := \bigcup_{n\in\mathbb{N}} \Gamma_n$ und $\Delta^* := \bigcup_{n\in\mathbb{N}} \Delta_n$ besitzen folgende Eigenschaften:*

(1) Γ^* und Δ^* sind disjunkt.

(2) Die atomaren Sätze in Γ^* sind abgeschlossen unter Substitution (gemäss Defintion 5.6).

(3) Wenn $\neg\psi \in \Gamma^*$, dann ist $\psi \in \Delta^*$. Wenn $\neg\psi \in \Delta^*$, dann ist $\psi \in \Gamma^*$.

(4) Wenn $\psi \vee \vartheta \in \Gamma^*$, dann gehört ψ oder ϑ zu Γ^*. Wenn $\psi \vee \vartheta \in \Delta^*$ dann gehören ψ und ϑ zu Δ^*.

(5) Wenn $\exists x \psi(x) \in \Gamma^*$, dann gibt es einen konstanten Term t, so dass $\psi(t) \in \Gamma^*$. Wenn $\exists x \psi(x) \in \Delta^*$, dann ist $\psi(t) \in \Delta^*$ für alle konstanten Terme t.

Beweis. Die Eigenschaften ergeben sich unmittelbar aus der Konstruktion der Sequenzen $\Gamma_n \Rightarrow \Delta_n$

(1) Wenn $\psi \in \Gamma^* \cap \Delta^*$, dann gibt es ein $n \in \mathbb{N}$, so dass $\psi \in \Gamma_n \cap \Delta_n$. Aber dann wäre $\Gamma_n \Rightarrow \Delta_n$ ein Axiom und somit ableitbar.

(2) Die Schritte (a), (b) in der Konstruktion garantieren, dass Γ^* alle Gleichungen $t = t$ enthält, und mit $t = t'$ und $\psi(t)$ auch $\psi(t')$, für alle atomaren Formeln $\psi(x)$.

(3) Wenn $\neg\psi \in \Gamma^*$, dann gibt es (da jeder Satz in der Aufzählung $\varphi_0, \varphi_1, \ldots$ unendlich oft vorkommt) ein hinreichend grosses n, so dass $\varphi_n = \neg\psi \in \Gamma_n$. Nach Schritt (c) der Konstruktion folgt, dass $\psi \in \Delta^*$. Der Fall, dass $\neg\psi \in \Delta^*$ wird analog behandelt.

(4) Wenn $\psi \vee \vartheta \in \Gamma^*$, dann gibt es ein n, so dass $\varphi_n = \psi \vee \vartheta \in \Gamma_n$. Nach Schritt ($d$) ist entweder ψ oder ϑ in Γ_{n+1}. Das Argument für $\psi \vee \vartheta \in \Delta^*$ ist analog.

(5) Wenn $\exists x \psi(x)$ in Γ^*, dann gibt es nach Schritt (e) ein c, so dass $\psi(c) \in \Gamma^*$. Wenn $\exists x \psi(x) \in \Delta^*$ und t ein beliebiger konstanter Term ist, dann gibt es hinreichend grosse n, so dass φ_n die Formel $\exists x \psi(x)$ und t_n der Term t ist. Nach Konstruktion ist $\psi(t_n) \in \Delta_{n+1}$.

□

Definition 5.10. Sei Γ^*, Δ^* ein Paar von Satzmengen welches die Eigenschaften (1)–(5) erfüllt. Dann heisst $\Gamma^* \cup \neg\Delta^*$ eine *Hintikka-Menge.*

Theorem 5.11 (Modell-Existenz-Satz). *Jede Hintikka-Menge besitzt ein Modell.*

Beweis. Sei $T = \Gamma^* \cup \neg\Delta^*$ eine Hintikka-Menge und Σ die Menge aller Atome in Γ^*. Nach Bedingung (2) ist Σ abgeschlossen unter Substitution. Wir behaupten, dass $\mathfrak{A}(\Sigma)$, die kanonische Struktur zu Σ, ein Modell von T ist. Dazu beweisen wir per Induktion über den Formelaufbau, dass für jeden Satz φ gilt:

$$\varphi \in \Gamma^* \implies \mathfrak{A}(\Sigma) \models \varphi$$
$$\varphi \in \Delta^* \implies \mathfrak{A}(\Sigma) \models \neg\varphi$$

(i) Für atomare Sätze ist dies bereits bewiesen (Lemma 5.8).

(ii) Sei $\varphi = \neg\psi$. Wenn $\varphi \in \Gamma^*$, dann ist $\psi \in \Delta^*$. Per Induktionsvoraussetzung folgt $\mathfrak{A}(\Sigma) \models \neg\psi$. Wenn $\varphi \in \Delta^*$, dann ist $\psi \in \Gamma^*$, also $\mathfrak{A}(\Sigma) \models \psi$ und daher $\mathfrak{A}(\Sigma) \models \neg\varphi$.

(iii) Sei $\varphi := \psi \vee \vartheta$. Wenn $\varphi \in \Gamma^*$, dann ist entweder ψ oder ϑ in Γ^* und damit nach Induktionsvoraussetzung wahr in $\mathfrak{A}(\Sigma)$. Wenn $\varphi \in \Delta^*$, dann sind ψ und ϑ in Δ^*, also $\mathfrak{A}(\Sigma) \models \neg\varphi$.

(iv) Sei $\varphi = \exists x\psi(x)$. Wenn $\varphi \in \Gamma^*$, dann gibt es ein t, so dass $\psi(t) \in \Gamma^*$. Also gilt per Induktionsvoraussetzung $\mathfrak{A}(\Sigma) \models \psi(t)$ und daher $\mathfrak{A}(\Sigma) \models \exists x\psi$. Wenn $\exists x\varphi \in \Delta^*$, dann ist $\psi(t) \in \Delta^*$ und daher per Induktionsvoraussetzung $\mathfrak{A}(\Sigma) \models \neg\psi(t)$ für alle t. Da jedes Element von $\mathfrak{A}(\Sigma)$ einen konstanten Term interpretiert, folgt $\mathfrak{A}(\Sigma) \models \neg\exists x\psi(x)$.

□

Wir sind ausgegangen von einer Satzmenge Φ und einer nicht aus Φ ableitbaren Sequenz $\Gamma \Rightarrow \Delta$. Wir haben daraus eine unendliche Folge von Sequenzen $\Gamma_n \Rightarrow \Delta_n$ konstruiert, und daraus eine Hintikka-Menge $T := \bigcup_{n\in\mathbb{N}} \Gamma_n \cup \bigcup_{n\in\mathbb{N}} \neg\Delta_n$ erhalten, welche $\Phi \cup \Gamma \cup \neg\Delta$ enthält. Wir haben schliesslich gezeigt, dass das kanonische Modell der Atome einer Hintikka-Menge ein Modell der gesamten Hinikka-Menge ist. Insbesondere folgt also, dass $\Phi \cup \Gamma \cup \neg\Delta$ erfüllbar ist. Damit ist der Vollständigkeitssatz bewiesen.

> **Überabzählbare Signaturen.** Wir haben hier den Vollständigkeitssatz nur für abzählbare Signaturen bewiesen. Er gilt aber auch für beliebige Signaturen (siehe etwa: H.-D Ebbinghaus, J. Flum, W. Thomas *Einführung in die Mathematsche Logik*, 4. Auflage, Spektrum Akademischer Verlag (1996), Kapitel V).

Die Menge aller Terme über einer abzählbaren Signatur ist selbst abzählbar. Das im Beweis des Vollständigkeitssatzes konstruierte Modell einer konsistenten Satzmenge ist also abzählbar. Damit erhalten wir unmittelbar eine interessante, rein semantische Folgerung.

Satz 5.12 (Löwenheim, Skolem). *Jede erfüllbare, abzählbare Satzmenge hat ein abzählbares Modell.*

Der Vollständigkeitssatz hat auch eine interessante *algorithmische* Konsequenz. Wie jeder Beweiskalkül erlaubt auch der Sequenzenkalkül die systematische Generierung aller ableitbaren Objekte. Aus dem Vollständigkeitssatz folgt demnach, dass es einen Algorithmus gibt, der alle allgemeingültigen FO(τ)-Sätze aufzählt. Dies bedeutet allerdings nicht, dass man einen Algorithmus zur Vefügung hätte, mit dem man zu jedem vorgelegten FO(τ)-Satz entscheiden könnte, ob dieser allgemeingültig ist: Sei etwa ψ der gegebene Satz. Man kann nun systematisch alle allgemeingültigen Sätze $\varphi_0, \varphi_1, \ldots$ aufzählen. Wenn ψ tatsächlich allgemeingültig ist, wird man irgendwann ein $\varphi_j := \psi$ erhalten und hat damit die richtige Antwort. Wenn aber ψ nicht allgemeingültig ist, dann kann man dies durch ein solches Aufzählungsverfahren nicht feststellen.

Wir werden im Kapitel die Begriffe der *rekursiv aufzählbaren* und der *entscheidbaren* Mengen genauer studieren und schliesslich zeigen, dass es *keinen* Algorithmus geben kann, welcher die Menge der allgemeingültigen Sätze der Prädikatenlogik entscheidet.

Schnitt-Elimination. Sequenzenkalküle gibt es in vielen verschiedenen Varianten. Interessant ist insbesondere die Erweiterung um die sogenannte *Schnittregel:*

$$\frac{\Gamma, \varphi \Rightarrow \Delta \quad \Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta}$$

Diese Regel ist eine Variante des *Modus Ponens*, welcher in andern Beweiskalkülen verwendet wird und die Ableitung von φ erlaubt, wenn vorher ψ und $\psi \to \varphi$ bewiesen wurden. Die Schnittregel erlaubt es, aus längeren Sequenzen kürzere abzuleiten. Beweise mit Schnittregel können sehr viel kürzer sein als solche ohne Schnitte, aber eine systematische Beweissuche und -analyse ist kaum mehr möglich. Gentzen formulierte seinen Sequenzenkalkül ursprünglich mit Schnittregel und bewies dann seinen berühmten *Schnitt-Elimationsssatz*, welcher besagt, dass beliebige Beweise durch solche ohne Schnitte simuliert werden können. Da wir hier direkt die Vollständigkeit des Sequenzenkalküls ohne Schnittregel bewiesen haben, kann man sich diesen (sehr aufwendigen) Beweis sparen.

5.4 Der Kompaktheitssatz

Der Vollständigkeitssatz schafft eine Brücke zwischen Syntax und Sematik der Prädikatenlogik und erlaubt es, Eigenschaften der Ableitungsbeziehung und der Konsistenz (also syntaktischer Begriffe) auf die Folgerungsbeziehung und die Erfüllbarkeit (also semantische Begriffe) zu übertragen. Die wichtigste Folgerung aus dem Vollständigkeitssatz ist der Kompaktheits- oder Endlichkeitssatz.

Satz 5.13 (Kompaktheitssatz der Prädikatenlogik). *Für jede Menge* $\Phi \subseteq \mathrm{FO}(\tau)$ *und jedes* $\psi \in \mathrm{FO}(\tau)$

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

(ii) Φ *ist erfüllbar genau dann, wenn jede endliche Teilmemge von* Φ *erfüllbar ist.*

Beweis. Aus der Definition der Ableitungsbeziehung folgen die entsprechenden syntaktischen Aussagen unmittelbar:

(i) $\Phi \vdash \psi$ genau dann, wenn $\Phi_0 \vdash \psi$ für eine endliche Teilmenge $\Phi_0 \subseteq \Phi$.

(ii) Φ ist konsistent genau dann, wenn jede endliche Teilmemge von Φ konsistent ist.

Da nach dem Vollständigkeitssatz eine Formelmenge erfüllbar ist genau dann, wenn sie konsistent ist, und die Folgerungsbeziehung $\models$ mit der Ableitungsbeziehung $\vdash$ zusammenfällt, ergeben sich die semantischen Aussagen des Kompaktheitssatzes. $\square$

Anwendungen des Kompaktheitssatzes. In Kapitel 4.1 haben wir gesehen, dass die Klasse aller Körper mit Charakteristik p endlich axiomatisierbar ist durch den Satz $\psi_{\text{Körper}} \wedge \chi_p$, wobei $\psi_{\text{Körper}}$ die Konjunktion der Körperaxiome und χ_p der Satz $\underbrace{1 + \cdots + 1}_{p \text{ mal}} = 0$ ist.

Für Körper der Charakteristik 0 haben wir das unendliche Axiomensystem

$$\Phi_0 = \{\psi_{\text{Körper}}\} \cup \{\neg\chi_p : p \text{ Primzahl}\}$$

angegeben. Aus dem Kompaktheitssatz können wir nun folgern, dass *jedes* Axiomensystem für diese Klasse unendlich sein muss.

Satz 5.14. *Die Klasse der Körper der Charakteristik 0 ist nicht endlich axiomatisierbar.*

Beweis. Sei $\psi \in \text{FO}(\tau_{ar})$ ein beliebiger Satz, welcher in allen Körpern der Charakteristik 0 gilt; also $\Phi_0 \models \psi$. Aus dem Kompaktheitssatz folgt, dass es eine Primzahl q gibt, so dass bereits

$$\{\psi_{\text{Körper}}\} \cup \{\neg\chi_p : p < q, p \text{ Primzahl}\} \models \psi.$$

Also gilt ψ auch in allen Körpern mit hinreichend grosser Charakteristik und axiomatisiert also nicht die Körper der Charakteristik 0. $\square$

Satz 5.15. *Sei $\Phi \subseteq \text{FO}(\tau)$ eine Satzmenge mit beliebig grossen endliche Modellen (d.h. für jedes $n \in \mathbb{N}$ gibt es ein Modell $\mathfrak{A} \models \Phi$ mit endlichem $\mathfrak{A}$ und $|\mathfrak{A}| > n$). Dann hat Φ auch ein unendliches Modell.*

Beweis. Sei $\Theta := \Phi \cup \{\varphi_{\geqslant n} : n \in \mathbb{N}\}$ wobei $\varphi_{\geqslant n} := \exists x_1 \cdots \exists x_n \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j$. Die Modelle von Θ sind also gerade die unendlichen Modelle von Φ.

Es genügt zu zeigen, dass jede endliche Teilmenge $\Theta_0 \subseteq \Theta$ erfüllbar ist, denn mit dem Kompaktheitssatz folgt dann, dass auch Θ erfüllbar ist. Für jedes endliche Θ_0 gibt es aber ein $n_0 \in \mathbb{N}$, so dass $\Theta_0 \subseteq \Phi \cup \{\varphi_{\geqslant n} : n \leq n_0\}$. Da nach Voraussetzung Φ beliebig grosse endliche Modelle hat, ist Θ_0 erfüllbar. $\square$

Korollar 5.16. *Die Klasse aller endlichen τ-Strukturen ist nicht axiomatisierbar in* FO.

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

Definition 5.17. Seien A, B zwei Mengen. Wir sagen, A ist mindestens so mächtig wie B (kurz $|A| \geq |B|$), wenn eine injektive Funktion $f : B \hookrightarrow A$ existiert.

Satz 5.18 (Aufsteigender Satz von Löwenheim-Skolem). Φ *besitze ein unendliches Modell. Dann gibt es zu jeder Menge M ein Modell $\mathfrak{D} \models \Phi$ über einem Universum D welches mindestens so mächtig wie M ist.*

Beweis. Sei $\Phi \subseteq \mathrm{FO}(\tau)$ und sei $\{c_m : m \in M\}$ eine Menge von paarweise verschiedenen Konstantensymbolen, welche nicht zu τ gehören. Setze

$$\Theta := \Phi \cup \{c_m \neq c_n : m, n \in M, m \neq n\}.$$

Wir zeigen, dass Θ erfüllbar ist. Wegen des Kompaktheitssatzes genügt es zu zeigen, dass für jede endliche Teilmengen $M_0 \subseteq M$ die Formelmenge

$$\Theta_0 := \Phi \cup \{c_m \neq c_n : m, n \in M_0, m \neq n\}$$

erfüllbar ist.

Nach Voraussetzung gibt es ein Modell $\mathfrak{B} \models \Phi$ mit unendlichem $\mathfrak{B}$. Da M_0 endlich ist, können wir in B paarweise verschiedene Elemente b_m für alle $m \in M_0$ auswählen. Sei $\mathfrak{A}$ die Expansion von $\mathfrak{B}$ durch die Konstanten $c_m^{\mathfrak{A}} := b_m$ für $m \in M_0$. Offensichtlich gilt $\mathfrak{A} \models \Theta_0$.

Damit ist gezeigt, dass Θ erfüllbar ist. Sei $\mathfrak{D}$ ein Modell von Θ mit Universum D. Die Abbildung $f : M \to D$ mit $f(m) = c_m^{\mathfrak{D}}$ ist injektiv, da für $m \neq n$ aus M gilt: $\mathfrak{D} \models c_m \neq c_n$. Da $\mathfrak{D} \models \Theta$ gilt insbesondere auch $\mathfrak{D} \models \Phi$. □

Wir erinnern daran, dass die *Theorie* $\mathrm{Th}(\mathfrak{A})$ einer τ-Struktur $\mathfrak{A}$ aus allen Sätzen $\psi \in \mathrm{FO}(\tau)$ mit $\mathfrak{A} \models \psi$ besteht, und dass zwei Strukturen $\mathfrak{A}, \mathfrak{B}$ elementar äquivalent sind (kurz $\mathfrak{A} \equiv \mathfrak{B}$), wenn sie dieselbe Theorie haben.

Lemma 5.19. $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\}$ *ist die kleinste axiomatisierbare Modellklasse, die* $\mathfrak{A}$ *enthält.*

Beweis. Offensichtlich ist $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\} = \mathrm{Mod}(\mathrm{Th}(\mathfrak{A}))$ und also axiomatisierbar. Wenn $\mathfrak{A} \models \Phi$ und $\mathfrak{B} \equiv \mathfrak{A}$, dann gilt offensichtlich auch $\mathfrak{B} \models \Phi$. Also gilt für alle $\Phi \subseteq \mathrm{FO}(\tau)$: Wenn $\mathfrak{A} \in \mathrm{Mod}(\Phi)$, dann ist $\{\mathfrak{B} : \mathfrak{A} \equiv \mathfrak{B}\} \subseteq \mathrm{Mod}(\Phi)$. □

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

Satz 5.20. *Sei* $\mathfrak{A}$ *eine unendliche Struktur. Dann gibt es eine Struktur* $\mathfrak{B}$ *mit* $\mathfrak{A} \equiv \mathfrak{B}$*, aber* $\mathfrak{A} \not\cong \mathfrak{B}$*. Insbesondere ist die Isomorphieklasse* $\{\mathfrak{B} : \mathfrak{A} \cong \mathfrak{B}\}$ *von* $\mathfrak{A}$ *nicht axiomatisierbar in der Prädikatenlogik.*

Beweis. $\mathrm{Th}(\mathfrak{A})$ besitzt ein unendliches Modell, und deshalb nach dem aufsteigenden Satz von Löwenheim-Skolem auch ein Modell $\mathfrak{B}$, das mindestens die Mächtigkeit der Potenzmenge $\mathcal{P}(A)$ von A hat. Nach Satz 1.2 ist $\mathfrak{B}$ nicht gleichmächtig zu $\mathfrak{A}$ und deshalb insbesondere auch nicht isomorph zu $\mathfrak{A}$. Da $\mathfrak{B} \models \mathrm{Th}(\mathfrak{A})$ (und $\mathrm{Th}(\mathfrak{A})$ vollständig ist) ist aber $\mathfrak{B}$ elementar äquivalent zu $\mathfrak{A}$. Also liegt in jeder axiomatisierbaren Modellklasse, welche $\mathfrak{A}$ enthält, auch eine zu $\mathfrak{A}$ nicht-isomorphe Struktur. □

Nichtstandardmodelle der Arithmetik. Die *Arithmetik* ist die Theorie $\mathrm{Th}(\mathfrak{N})$ der Struktur $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$. Ein *Nichtstandardmodell* der Arithmetik ist eine zu $\mathfrak{N}$ elementar äquivalente, aber nicht zu $\mathfrak{N}$ isomorphe $\{\tau_{ar}\}$-Struktur.

Aus dem aufsteigenden Satz von Löwenheim-Skolem folgt: Es gibt ein (überabzählbares) Nichtstandardmodell der Arithmetik. Ein schärferes Resultat liefert der folgende Satz von Skolem.

Satz 5.21 (Skolem). *Es gibt ein abzählbares Nichtstandardmodell der Arithmetik.*

Beweis. Sei $\Phi := \mathrm{Th}(\mathfrak{N}) \cup \{c \neq \boldsymbol{n} : n \in \mathbb{N}\}$, wobei c ein neues Konstantensymbol ist, $\boldsymbol{0} := 0$, und $\boldsymbol{n} := \underbrace{1 + \cdots + 1}_{n \text{ mal}}$ für $n \geq 1$.

Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ besitzt ein Modell $\mathfrak{A} = (\mathfrak{N}, c^{\mathfrak{A}})$ mit hinreichend grossem $c^{\mathfrak{A}} \in \mathbb{N}$. Also ist nach dem Kompaktheitssatz Φ erfüllbar und hat daher nach dem Satz von Löwenheim-Skolem sogar ein abzählbares Modell $\mathfrak{B}$. Sei $\mathfrak{C} = \mathfrak{B} \upharpoonright \tau_{ar}$ (das durch Weglassen von $c^{\mathfrak{B}}$ definierte Redukt von $\mathfrak{B}$). Da $\mathfrak{B} \models \mathrm{Th}(\mathfrak{N})$ ist $\mathfrak{N} \equiv (\mathfrak{B} \upharpoonright \tau_{ar})$.

Es bleibt zu zeigen, dass es keinen Isomorphismus $\pi : \mathfrak{N} \to (\mathfrak{B} \upharpoonright \tau_{ar})$ geben kann. Für jeden solchen Isomorphimus π müsste gelten, dass $\pi(n) = \pi(\boldsymbol{n}^{\mathfrak{N}}) = \boldsymbol{n}^{\mathfrak{B}}$ für alle $n \in \mathbb{N}$. Da π surjektiv ist, gibt es ein $k \in \mathbb{N}$, so dass $c^{\mathfrak{B}} = \pi(k) = \boldsymbol{k}^{\mathfrak{B}}$.

Damit erhalten wir einen Widerspruch: Einerseits gilt $\mathfrak{B} \models c = \boldsymbol{k}$, aber andererseits, da die Formel $c \neq \boldsymbol{k}$ in Φ enthalten ist, auch $\mathfrak{B} \models c \neq \boldsymbol{k}$. □

Übung 5.2. Sei $\mathfrak{A}$ ein abzählbares Nichtstandardmodell der Arithmetik, sei $\varphi(x, y)$ die Formel $x \neq y \wedge \exists z(x + z = y)$ und sei $(\mathfrak{A}, <^{\mathfrak{A}}) := (\mathfrak{A}, \varphi^{\mathfrak{A}})$.

(a) Zeigen Sie, dass $(\mathfrak{A}, <^{\mathfrak{A}})$ ein Modell von $\mathrm{Th}(\mathfrak{N}, <)$ ist (also ein abzählbares Nichtstandardmodell der geordneten Arithmetik).

(b) Zeigen sie, dass $(A, <^{\mathfrak{A}})$ keine Wohlordnung ist (also eine unendliche absteigende Kette enthält).

(c) Beschreiben Sie die Ordnungsstruktur von $(A, <^{\mathfrak{A}})$: Betrachten Sie die Ordnung $(B, <^B)$ mit $B = \mathbb{N} \times \{0\} \cup \mathbb{Z} \times \mathbb{Q}^{>0}$ und $(a, b) <^B (a', b')$, wenn $b < b'$ oder wenn $b = b'$ und $a < a'$; also informell: $(B, <^B)$ ist zusammengesetzt aus $(\mathbb{N}, <)$ und dahinter abzählbar vielen, dicht hintereinanderliegenden Kopien von $(\mathbb{Z}, <)$. Zeigen Sie, dass es eine Einbettung von $(B, <^B)$ in $(A, <^{\mathfrak{A}})$ gibt.

Übung 5.3. Zeigen Sie, dass es überabzählbar viele abzählbare Modelle der Arithmetik gibt. Hinweis: Sei $\varphi(x, y) := \exists z(x \cdot z = y)$. Die Primteiler eines Elements a eines Nichstandardmodells $\mathfrak{A}$ der Arithmetik seien die Primzahlen $p \in \mathbb{N}$, so dass $\mathfrak{A} \models \varphi[\boldsymbol{p}, a]$. Zeigen Sie, dass es zu jeder Menge Q von Primzahlen ein abzählbares Nichtstandardmodell $\mathfrak{A}$ der Arithmetik gibt, welches ein Element a enthält, dessen Primteiler genau die Elemente von Q sind.

Warum der Kompakheitssatz so heisst. Sei τ eine beliebige Signatur und S die Menge aller vollständigen τ-Theorien. Wir definieren eine Topologie auf S, deren Basis aus den Mengen $\mathcal{O}_\psi := \{T \in S : \psi \in S\}$ für alle Sätze $\psi \in FO(\tau)$ besteht. Man beachte, dass $\mathcal{O}_\psi \cap \mathcal{O}_\varphi = \mathcal{O}_{\psi \wedge \varphi}$. Ferner ist $S - \mathcal{O}_\psi = \{T \in S : \psi \notin T\} = \{T \in S : \neg\psi \in S\} = \mathcal{O}_{\neg\psi}$.

Die Basis der Topologie besteht also aus offen-abgeschlossenen Mengen. Zudem ist S hausdorffsch, d.h. je zwei verschiedene Punkte lassen sich durch disjunkte Umgebungen trennen. Zu zwei beliebigen vollständigen Theorien $T \neq T'$ gibt es nämlich einen Satz ψ mit $\psi \in T, \neg\psi \in T'$ und daher $T \in \mathcal{O}_\psi, T' \in \mathcal{O}_{\neg\psi}$ und natürlich $\mathcal{O}_\psi \cap \mathcal{O}_{\neg\psi} = \varnothing$.

Die offenen Mengen von S sind die Mengen der Form $\bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi$, die abgeschlossenen diejenigen der Form $\bigcap_{\varphi \in \Phi} \mathcal{O}_\varphi$, für beliebige Satzmengen $\Phi \subseteq \mathrm{FO}(\tau)$.

Der Kompaktheitssatz besagt nun, dass der topologische Raum S kompakt ist, d.h. dass jede offene Überdeckung von S eine endliche Teilüberdeckung besitzt. Dies zeigt man wie folgt:

Jede offene Überdeckung von S kann zu einer Überdeckung der Form $\bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi$ verfeinert werden, für eine geeignete Satzmenge $\Phi \subseteq \mathrm{FO}(\tau)$.

Also ist $\varnothing = S - \bigcup_{\varphi \in \Phi} \mathcal{O}_\varphi = \bigcap_{\varphi \in \Phi_0} \mathcal{O}_{\neg\varphi}$.

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

Kapitel 6

Das Entscheidungsproblem der mathematischen Logik

Das klassische Entscheidungsproblems der mathematischen Logik kann auf verschiedene, äquivalente Weisen formuliert werden:

Erfüllbarkeit: Man konstruiere einen Algorithmus, welcher zu jeder vorgelegten Formel der Prädikatenlogik entscheidet, ob sie erfüllbar ist oder nicht.

Gültigkeit: Man finde einen Algorithmus, welcher zu jeder Formel ψ der Prädikatenlogik entscheidet, ob sie allgemeingültig ist, d.h. ob jede zu ψ passende Interpretation ein Modell von ψ ist.

Beweisbarkeit: Man konstruiere einen Algorithmus, welcher zu jeder Formel $\psi \in \mathrm{FO}$ entscheidet, ob ψ (aus der leeren Hypothesenmenge) ableitbar ist. (Hier wird ein fester, vollständiger Beweiskalkül für die Prädikatenlogik zugrunde gelegt, z.B. der Sequenzenkalkül).

Die Äquivalenz dieser Probleme ist unmittelbar einsichtig: Eine Formel ψ ist erfüllbar genau dann, wenn $\neg\psi$ nicht allgemeingültig ist, und nach dem Vollständigkeitssatz ist eine Formel allgemeingültig genau dann, wenn sie ableitbar ist. Wir betrachten im Folgenden das Entscheidungsproblem als Erfüllbarkeitsproblem.

Das klassische Entscheidungsproblem wurde zu Beginn dieses Jahrhundert von Hilbert formuliert und war Teil seines formalistischen Programms zur Lösung der Grundlagenprobleme der Mathematik. Hilbert und Ackermann schrieben:

> *Das Entscheidungsproblem ist gelöst, wenn man ein Verfahren kennt, das bei einem vorgelegten logischen Ausdruck durch endlich viele Operationen die Entscheidung über die Allgemeingültigkeit bzw. Erfüllbarkeit erlaubt. (...) Das Entscheidungsproblem muss als das Hauptproblem der mathematischen Logik bezeichnet werden.*
>
> D. Hilbert, W. Ackermann, *Grundzüge der theoretischen Logik*, 1. Auflage, Berlin 1928, S. 73ff.

In der Tat hätte eine positive Lösung des Entscheidungsproblems weitreichende Folgen für die Mathematik. Man könnte dann, mindestens im Prinzip, zahlreiche offene Probleme der Mathematik (z.B. die Riemann-Hypothese) durch Anwendung des Entscheidungsalgorithmus lösen.

Für gewisse *Teilklassen* der Prädikatenlogik können solche Entscheidungsalgorithmen angegeben werden.

Übung 6.1. Man konstruiere einen Algorithmus, welcher das Erfüllbarkeitsproblem für Formeln löst, deren Signatur ausschliesslich aus monadischen (d.h. einstelligen) Relationssymbolen besteht. Hinweis: Man zeige, z.B. mit Hilfe des Ehrenfeucht-Fraïssé Spiels, dass jede erfüllbare Formel mit Quantorenrang m und q monadischen Relationssymbolen ein Modell mit höchstens $m2^q$ Elementen besitzt.

Übung 6.2. Zeigen sie, dass das Erfüllbarkeitsproblem entscheidbar ist für Formeln der Gestalt $\exists x_1 \cdots \exists x_r \forall y_1 \cdots \forall y_s \varphi$, wobei φ quantorenfrei und relational sein soll. Hinweis: Zeigen Sie, dass jeder erfüllbare Satz dieser Gestalt ein Modell mit höchstens r Elementen besitzt.

Übung 6.3. Zeigen Sie, das das Erfüllbarkeitsproblem für existentielle Formeln (mit beliebiger Signatur) entscheidbar ist.

Übung 6.4. Beurteilen Sie die Komplexität dieser Entscheidungsalgorithmen.

Andrerseits kann man das Erfüllbarkeitsproblem für die gesamte Prädikatenlogik auf gewisse Teilklassen reduzieren. Eine Formelmenge $X \subseteq \mathrm{FO}$ ist eine *Reduktionsklasse* (für Erfüllbarkeit), wenn ein Algorithmus existiert, welcher jeder Formel ψ der Prädikatenlogik eine Formel $\psi' \in X$ zuordnet, welche erfüllbar ist genau dann, wenn ψ erfüllbar ist. Wenn das Erfüllbarkeitsproblem für irgendeine Reduktionsklasse algorithmisch gelöst werden kann, dann also auch für die gesamte Prädikatenlogik. Der Satz über die Skolem-Normalform impliziert, dass die Menge aller *universellen Formeln in Pränex-Normalform* eine Reduktionsklasse ist.

Übung 6.5. Zeigen Sie, dass folgende Klassen Reduktionsklassen sind:

(a) die Klasse aller relationalen Formeln ohne Gleichheit;

(b) Die Klasse aller relationalen Formeln, welche ausschliesslich ein- und zweistellige Relationssymbole enthalten.

1936/37 haben Church und Turing unabhängig voneinander bewiesen, dass das Entscheidungsproblem nicht algorithmisch lösbar ist. Dazu ist eine Präzisierung des Algorithmusbegriffs notwendig.

6.1 Turingmaschinen, rekursive Aufzählbarkeit und Entscheidbarkeit

Wir behandeln hier *Turingmaschinen* als Beispiel für einen universellen Algorithmusbegriff. Andere Möglichkeiten wären etwa *while-Programme*, *Registermaschinen* oder *μ-rekursive Funktionen.*

Definition 6.1. Eine *Turingmaschine* ist gegeben durch ein 6-Tupel $M = (Q, \Sigma, \Gamma, q_0, F, \delta)$, bestehend aus

- einer endlichen Menge Q von *Zuständen*,
- einem endlichen *Arbeitsalphabet* Σ mit einem ausgezeichneten *Blank*-Symbol $\Box$,
- einem *Inputalphabet* $\Gamma \subseteq \Sigma - \{\Box\}$,

- einem *Anfangszustand* $q_0 \in Q$,
- einer Menge $F \subseteq Q$ von *Endzuständen*, und
- einer partiellen *Übergangsfunktion* $\delta : (Q - F) \times \Sigma \to Q \times \Sigma \times \{-1, 0, 1\}$.

Informell beschrieben, besteht eine Turingmaschine aus einer endlichen Kontrolleinheit, welche sich zu jedem Zeitpunkt in einem der Zustände $q \in Q$ befindet, einem Lese-Schreibkopf und einem einseitig unendlichen Band, eingeteilt in Felder $0, 1, 2 \ldots,$ welche Zeichen des Arbeitsalphabets enthalten. Zu Beginn der Berechnung steht auf einem Anfangsstück des Bandes die Eingabe, die restlichen Felder enthalten das Blank-Symbol $\square$, der Lese-Schreibkopf steht auf dem Feld 0 und die Kontrolleinheit ist im Anfangszustand q_0. In einem Rechenschritt kann die Turingmaschine, abhängig vom aktuellen Zustand und vom gerade gelesenen Symbol, den durch die Übergangsfunktion δ beschrieben lokalen Übergang vollziehen: sie nimmt einen neuen Zustand an, ändert das Symbol in dem Feld, auf dem sich der Lese-Schreibkopf gerade befindet und bewegt diesen um maximal ein Feld nach links oder rechts.

Definition 6.2. Eine *Konfiguration* (momentane Beschreibung) von M ist ein Tripel $C = (q, p, w)$, wobei $q \in Q, p \in \mathbb{N}, w \in \Sigma^*$ ist. Dabei bezeichnet p die Kopfposition und w die Bandinschrift, wobei auf den Feldern $i \geq |w|$ das Symbol $\square$ steht. Sei $\mathcal{C}$ die Menge der Konfigurationen von M. Die Übergangsfunktion δ definiert auch eine partielle Übergangsfunktion $\Delta : \mathcal{C} \to \mathcal{C}$ auf den Konfigurationen: Sei $\delta(q, a) = (q', a', m)$ und sei $w = w_0 \cdots w_{n-1}$ mit $w_p = a$, dann ist $\Delta(q, p, w) = (q', p + m, w')$ mit

$$w'_j := \begin{cases} w_j & \text{für } j \neq p \\ a' & \text{für } j = p. \end{cases}$$

$\Delta(C)$ ist die *(unmittelbare) Nachfolgekonfiguration* von C. Wir schreiben auch $C \vdash_M C'$, falls $\Delta(C) = C'$ und $C \vdash_M^* C'$, wenn Konfigurationen $C_0, \ldots, C_r \in \mathcal{C}$ existieren, so dass $C = C_0, C' = C_r$ und $C_i \vdash_M C_{i+1}$ für alle $i < r$.

Definition 6.3. Die *Anfangskonfiguration* von M auf $x \in \Gamma^*$ ist $C_0(x) := (q_0, 0, x)$. Eine Konfiguration $C = (q, p, w)$ ist eine *Endkonfiguration*, wenn $q \in F$. *M hält auf x*, wenn eine Endkonfiguration C_e existiert, so dass $C_0(x) \vdash_M^* C_e$. Die *Haltemenge* von M ist $L(M) := \{x \in \Gamma^* : M \text{ hält auf } x\}$. Die *Berechnung von M auf x* ist die (endliche oder unendliche Folge) $C_0, C_1, \ldots$ mit $C_0 = C_0(x)$ und $C_i \vdash_M C_{i+1}$ für alle i.

Dabei gibt es drei Möglichkeiten:

1. Die Berechnung von M auf x erreicht nach endlich vielen Schritten eine Endkonfiguration C_e, d.h. $C_0(x) \vdash_M^* C_e$ und daher $x \in L(M)$.
2. Die Berechnung von M auf x ist unendlich, und also $x \notin L(M)$.
3. Nach endlich vielen Schritten wird eine Konfiguration C erreicht ($C_0(x) \vdash_M^* C$) für die $\Delta(C)$ nicht definiert ist, welche aber auch keine Endkonfiguration ist. Die Berechnung von M auf x ist also endlich, aber $x \notin L(M)$. Wir sagen in diesem Fall, dass die Berechnung von M hängt.

Definition 6.4. Eine Sprache $L \subseteq \Gamma^*$ ist *rekursiv aufzählbar*, wenn eine Turingmaschine M existiert mit $L = L(M)$.

Bemerkung. $L = L(M)$ bedeutet nicht, dass M ein Entscheidungsverfahren für die Frage ist, ob $x \in L$. Wenn tatsächlich x in L ist, dann hält M auf x nach endlich vielen Schritten. Aber für $x \notin L$ kann die Berechnung von M unendlich sein.

In der Berechenbarkeitstheorie ist es (im Gegensatz zur sonst üblichen Praxis in der Mathematik) angemessen, *partielle* Funktionen zu betrachten, da Algorithmen nicht auf allen Eingaben halten und für einen gegebenen Algorithmus die Haltemenge auch nicht unbedingt bekannt ist. Im Rest dieses Kapitels sind daher Funktionen $f : \Gamma^* \to \Sigma^*$ in der Regel partielle Funktionen, der Definitionsbereich ist eine Teilmenge von Γ^*. Wenn der Definitionsbereich ganz Γ^* ist, dann nennen wir eine solche Funktion *total*.

Definition 6.5. Jede Turingmaschine M definiert eine partielle Funktion $f_M : \Gamma^* \to \Sigma^*$ mit Definitionsbereich $L(M)$. Dabei ist $f_M(x) = y$ genau dann, wenn y die Bandinschrift am Ende der Berechnung von M auf x ist (gefolgt von $\square\square\cdots$), d.h. wenn es eine Endkonfiguration $C_e = (q, p, y)$ gibt, so dass $C_0(x) \vdash_M^* C_e$. Wir nennen f_M *die von M berechnete Funktion.* Eine partielle Funktion f ist *turingberechenbar*, wenn eine Turingmaschine M existiert mit $f = f_M$.

Churchsche These. *Die im intuitiven Sinn algorithmisch berechenbaren Funktionen sind gerade die turingberechenbaren Funktionen.*

Es wurden viele andere Definitionen für einen formalen Algorithmusbegriff vorgeschlagen, z.B. durch μ-rekursive Funktionen, Registermaschinen oder while-Programme. All diese Definitionen haben sich als äquivalent erwiesen.

Wir benutzen im Folgenden die Churchsche These und beschränken uns darauf, Algorithmen informell zu beschreiben. Eine explizite Konstruktion von entsprechenden Turingmaschinen ist in allen Fällen möglich, allerdings etwas langwierig und nicht besonders interessant.

Satz 6.6 (Andere Beschreibung der rekursiven Aufzählbarkeit). $L \subseteq \Sigma^*$ *ist genau dann rekursiv aufzählbar, wenn eine Turingmaschine M existiert, welche L in folgendem Sinn aufzählt: Es gibt einen speziellen Ausgabezustand q_1 von M, so dass $L = \{y \in \Sigma^* : C_0(\lambda) \vdash_M^* (q_1, p, y)\}$, wobei mit λ das leere Wort bezeichnet wird.*

Beweis. Sei N eine Turingmaschine mit $L = L(N)$. Informell kann ein Aufzählungsalgorithmus M für L wie folgt beschrieben werden: Auf Input λ durchläuft M sukzessive alle $n \in \mathbb{N}$ und führt für jedes n folgende Teilprozedur aus: Für alle $y \in \Gamma^*$ der Länge $|y| \leq n$, simuliert M höchstens n Schritte der Berechnung von N auf y. Wenn dabei eine Endkonfiguration von N erreicht wird (d.h. wenn N auf y in höchstens n Schritten hält), dann schreibt M y auf das Band und geht in Zustand q_1 (d.h. M geht in eine Konfiguration (q_1, p, y)). Offensichtlich ist $L(N) = \{y : C_0(\lambda) \vdash_M^* (q_1, p, y)\}$.

Sei umgekehrt L durch M aufgezählt. Der folgende Algorithmus N hat als Haltemenge genau L: Auf Input y simuliert N die Berechnung des Aufzählungsalgorithmus M auf λ solange, bis eine Konfiguration (q_1, p, y) erreicht ist. Dann hält N. Offensichtlich ist $L(N) = L$ und daher L rekursiv aufzählbar. $\square$

Sei $L \subseteq \Gamma^*$. Die *charakteristische Funktion* von L ist $\chi_L : \Gamma^* \to \{0,1\}$ mit

$$\chi_L(x) = \begin{cases} 1 & \text{wenn } x \in L \\ 0 & \text{sonst.} \end{cases}$$

Definition 6.7. Eine Sprache $L \subseteq \Gamma^*$ ist *entscheidbar*, wenn χ_L turingberechenbar ist. Eine Turingmaschine M mit $f_M = \chi_L$ ist ein *Entscheidungsverfahren* für L.

Äquivalente Definition durch Akzeptoren. Ein *Turing-Akzeptor* ist eine Turingmaschine M deren Endzustände in zwei Klassen F^+ (akzeptierende Zustände) und F^- (verwerfende Zustände) eingeteilt sind. Endkonfigurationen von M sind akzeptierend bzw. verwerfend, wenn ihre Zustände es sind. M akzeptiert x (bzw. M verwirft x), wenn M auf x in einer akzeptierenden (bzw. verwerfenden) Endkonfiguration hält.

Lemma 6.8. *$L \subseteq \Gamma^*$ ist entscheidbar genau dann, wenn ein Turing-Akzeptor M existiert, welcher alle $x \in L$ akzeptiert und alle $x \in \Gamma^* - L$ verwirft.*

Sei $L \subseteq \Gamma^*$ und $\overline{L} := \Gamma^* - L$ das Komplement von L.

Satz 6.9. *L ist entscheidbar genau dann, wenn L und $\overline{L}$ rekursiv aufzählbar sind.*

Beweis. Sei $M = (Q, \Gamma, \Sigma, q_0, F, \delta)$ mit $F = F^+ \cup F^-$ ein Turing-Akzeptor, welcher L entscheidet. Setze $M^+ = (Q, \Gamma, \Sigma, q_0, F^+, \delta)$ und $M^- = (Q, \Gamma, \Sigma, q_0, F^-, \delta)$. Dann ist $L(M^+) = L$ und $L(M^-) = \overline{L}$.

Sei andererseits L und $\overline{L}$ rekursiv aufzählbar. Dann gibt es Turingmaschinen M^+ und M^-, so dass $L = L(M^+)$, $\overline{L} = L(M^-)$. Der folgende Algorithmus ist ein Entscheidungsverfahren für L: Auf Input x simuliere man parallel die Berechnungen von M^+ und M^- auf x, bis eine der beiden Turingmaschinen hält. Wenn M^+ hält, wird x akzeptiert, wenn M^- hält, wird x verworfen. □

6.2 Das Halteproblem

Eine Turingmaschine ist ein endliches Objekt. Daher können Turingmaschinen selbst als Wörter kodiert und damit als Inputs für Turingmaschinen verwendet werden. Wir fixieren eine Kodierung ρ, die jeder Turingmaschine M und jedem Input x für M ein Wort $\rho(M)$ bzw. $\rho(x)$ in $\{0,1\}^*$ so zuordnet, dass sich das Berechnungsverhalten von M auf x aus $\rho(M)$ und $\rho(x)$ effektiv erschliessen lässt. Die präzise Form einer solchen Kodierung ist unwichtig.

Es lässt sich dann eine universelle Turingmaschine U konstruieren, die angesetzt auf Input $\rho(M)\#\rho(x)$ die Berechnung von M auf x simuliert und genau dann hält, wenn M hält. U ist also ein Interpreter für Turingmaschinen. Die Menge

$$H = \{\rho(M)\#\rho(x) : x \in L(M)\}$$

ist dann gleich $L(U)$ und also rekursiv aufzählbar. H beschreibt das *Halteproblem für Turingmaschinen*: "Gegeben (Kodierungen von) M und x, entscheide ob M auf x hält." Wir werden zeigen, dass das Halteproblem unentscheidbar ist.

Wichtige Varianten des Halteproblems sind

Das Selbstanwendungsproblem: $H_0 := \{\rho(M) : M \text{ hält auf } \rho(M)\}$.

Das Halteproblem auf leerem Band: $H_\lambda := \{\rho(M) : M \text{ hält auf } \lambda\}$.

Wir beweisen zuerst mit einem Diagonalisierungsargument die Unentscheidbarkeit des Selbstanwendungsproblems.

Satz 6.10. *H_0 ist unentscheidbar.*

Beweis. Wir zeigen, dass $\overline{H_0}$ nicht rekursiv aufzählbar ist. Andernfalls gäbe es eine Turingmaschine M_0 so dass $\overline{H_0} = L(M_0)$. Daraus erhalten wir folgenden Widerspruch:

$$\begin{aligned} \rho(M_0) \in \overline{H_0} &\iff M_0 \text{ hält auf } \rho(M_0) && (\text{da } \overline{H_0} = L(M_0)) \\ &\iff \rho(M_0) \in H_0. && (\text{nach Definition von } H_0) \end{aligned}$$

Also ist $\overline{H_0}$ nicht rekursiv aufzählbar und H_0 daher nicht entscheidbar. □

Korollar 6.11. *H ist unentscheidbar.*

Beweis. Aus einem Entscheidungsverfahren für H erhält man sofort auch eines für H_0. □

Satz 6.12. *H_λ ist unentscheidbar.*

Beweis. Sei M eine Turingmaschine, x ein Input für M. Dann sei $N_{M,x}$ eine Turingmaschine, welche auf Input λ wie folgt operiert: Zuerst wird x auf das Band geschrieben, dann die Berechnung von M auf x simuliert. Also ist $\rho(N_{M,x}) \in H_\lambda$ genau dann, wenn $\rho(M)\#\rho(x) \in H$. Offensichtlich lässt sich $N_{M,x}$ aus M und x effektiv konstruieren, d.h. es gibt einen Algorithmus M', welcher auf Input $\rho(M)\#\rho(x)$ die Kodierung $\rho(N_{M,x})$ berechnet.

Wir nehmen nun an, dass es ein Entscheidungsverfahren M_λ für H_λ gibt. Durch Hintereinanderausführen von M' und M_λ erhalten wir ein Entscheidungsverfahren $M_\lambda \circ M'$ für H: $(M_\lambda \circ M')$ akzeptiert $\rho(M)\#\rho(x)$ genau dann, wenn M_λ $\rho(N_{M,x})$ akzeptiert, also genau dann, wenn $\rho(N_{M,x}) \in H_\lambda$. Wir haben gesehen, dass dies genau dann der Fall ist, wenn $\rho(M)\#\rho(x) \in H$.

Da H aber unentscheidbar ist, kann es also kein Entscheidungsverfahren für H_λ geben. □

Definition 6.13. Eine Sprache $A \subseteq \Gamma^*$ ist *reduzierbar* auf eine Sprache $B \subseteq \Sigma^*$ (kurz: $A \leq B$), wenn eine totale turingberechenbare Funktion $f : \Gamma^* \to \Sigma^*$ existiert, so dass für alle $x \in \Gamma^*$ gilt: $x \in A \iff f(x) \in B$.

Mit solchen Reduktionen lassen sich Aussagen über Entscheidbarkeit bzw. rekursive Aufzählbarkeit von einer Sprache auf eine andere übertragen.

Lemma 6.14. *Sei $A \leq B$. Wenn B entscheidbar (bzw. rekursiv aufzählbar) ist, dann auch A. Ist also A unentscheidbar, so auch B.*

Im Beweis von Satz 6.12 haben wir dies implizit bereits verwendet, denn wir haben die Unentscheidbarkeit von H_λ nachgewiesen, indem wir ein bereits bekanntes unentscheidbares Problem, nämlich H, auf H_λ reduziert haben.

Wir beweisen nun ein sehr allgemeines Unentscheidbarkeitsresultat, den Satz von Rice, welcher besagt, dass jede nicht-triviale Aussage über die von einem gegebenen Algorithmus berechnete Funktion unentscheidbar ist.

Sei $\mathcal{R}$ die Klasse aller turingberechenbaren Funktionen. Eine Teilmenge $\mathcal{S}$ ist nicht-trivial, wenn $\mathcal{S} \neq \varnothing$ und $\mathcal{S} \neq \mathcal{R}$.

Satz 6.15 (Rice). *Für jede nicht-triviale Menge $\mathcal{S} \subseteq \mathcal{R}$ von turingberechenbaren Funktionen ist die Menge* $\mathrm{code}(\mathcal{S}) := \{\rho(M) : f_M \in \mathcal{S}\}$ *unentscheidbar.*

Beweis. Sei Ω die überall undefinierte Funktion. Entweder ist $\Omega \in \mathcal{S}$ oder $\Omega \in \mathcal{R} - \mathcal{S}$.

Fall (1): $\Omega \in \mathcal{R} - \mathcal{S}$. Wir zeigen, dass H_λ auf $\mathrm{code}(\mathcal{S})$ reduzierbar ist. Da $\mathcal{S} \neq \varnothing$ können wir eine Turingmaschine N auswählen, so dass $f_N \in \mathcal{S}$. Jeder Turingmaschine M ordnen wir nun eine Turingmaschine M' zu, welche auf Input x wir folgt operiert: Zunächst ignoriert M' den Input und simuliert die Berechnung von M auf λ. Wenn diese hält, dann simuliert M' danach die Berechnung von N auf x.

Da N fest gewählt ist, ist die Transformation von $\rho(M)$ auf $\rho(M')$ effektiv berechenbar. M' berechnet die Funktion

$$f_{M'} = \begin{cases} f_N & \text{wenn } M \text{ auf } \lambda \text{ hält} \\ \Omega & \text{sonst.} \end{cases}$$

Also ist $\rho(M') \in \mathrm{code}(\mathcal{S})$ genau dann, wenn $\rho(M) \in H_\lambda$.

Damit ist gezeigt, dass $H_\lambda \leq \mathrm{code}(\mathcal{S})$. Da H_λ unentscheidbar ist, ist auch $\mathrm{code}(\mathcal{S})$ unentscheidbar.

Fall (2): Sei $\Omega \in \mathcal{S}$. Nach Fall (1) ist $\mathrm{code}(\mathcal{R} - \mathcal{S})$ unentscheidbar. Daraus folgt unmittelbar, dass auch $\mathrm{code}(\mathcal{S})$ unentscheidbar ist. □

Rekursive Untrennbarkeit.

Definition 6.16. Zwei disjunkte Sprachen $A, B \subseteq \Gamma^*$ sind *rekursiv untrennbar*, wenn keine entscheidbare Sprache $C \subseteq \Gamma^*$ existiert, so dass $A \subseteq C$ und $B \cap C = \varnothing$.

Wenn A und B rekursiv untrennbar sind, dann sind insbesondere beide Sprachen unentscheidbar. Sei

$$H_\lambda^+ := \{\rho(M) : M \text{ Akzeptor, } M \text{ akzeptiert } \lambda\}$$
$$H_\lambda^- := \{\rho(M) : M \text{ Akzeptor, } M \text{ verwirft } \lambda\}$$

Satz 6.17. *H_λ^+ und H_λ^- sind rekursiv untrennbar.*

Beweis. Wir nehmen an, $C \subseteq \{0,1\}^*$ sei eine Sprache mit $H_\lambda^+ \subseteq C$ und $H_\lambda^- \cap C = \varnothing$. Mit Hilfe des Satzes von Rice zeigen wir, dass C unentscheidbar ist.

Man kann jede Turingmaschine M effektiv in einen Turing-Akzeptor M' überführen, so dass M' x akzeptiert genau dann, wenn $f_M(x) = 1$, und M' x verwirft fenau dan, wenn $f_M(x) = 0$. Nun ist $\mathcal{S}_C := \{f_{M'} : \rho(M) \in C\}$ eine nicht-triviale Menge von turingberechenbaren Funktionen, denn $\{f_M : f_M(\lambda) = 1\} \subseteq \mathcal{S}_C$ und $\{f_M : f_M(\lambda) = 0\} \subseteq \mathcal{R} - \mathcal{S}_C$. Wenn C entscheidbar ist, dann auch $\mathrm{code}(\mathcal{S}_C)$; dies widerspricht aber dem Satz von Rice. □

Lemma 6.18. *Seien $A, B \subseteq \Gamma^*$ rekursiv untrennbar, X, Y zwei disjunkte Sprachen in Σ^*, und sei $f : \Gamma^* \to \Sigma^*$ eine totale turingberechenbare Funktion, so dass $f(A) \subseteq X$ und $f(B) \subseteq Y$. Dann sind auch X und Y rekursiv untrennbar.*

Beweis. Sei $Z \subseteq \Sigma^*$ eine entscheidbare Sprache mit $X \subseteq Z$ und $Y \cap Z = \varnothing$. Dann ist das Urbild $f^{-1}(Z)$ von Z eine entscheidbare Sprache in Γ^* mit $A \subseteq f^{-1}(Z)$ und $B \cap f^{-1}(Z) = \varnothing$, im Widerspruch zur rekursiven Untrennbarkeit von A und B. □

Wir schreiben $(A, B) \leq (X, Y)$ wenn eine Reduktion f wie in Lemma 6.18 existiert.

6.3 Die Unentscheidbarkeit der Prädikatenlogik

Sei $\tau_\infty = \bigcup_{n \in \mathbb{N}} R^n_\infty \cup F^n_\infty$, wobei $R^n_\infty = \{R^n_i : i \in \mathbb{N}\}$ eine Menge von n-stelligen Relationssymbolen und $F^n_\infty = \{f^n_i : i \in \mathbb{N}\}$ eine Menge von n-stelligen Funktionssymbolen ist. τ_∞ ist abzählbar und jede abzählbare Signatur kann als Teilmenge von τ_∞ aufgefasst werden. Wir beschränken uns in diesem Kapitel auf abzählbare Signaturen und identifizieren FO mit FO(τ_∞). Wenn $\tau \subseteq \tau_\infty$, dann ist FO$(\tau)$ eine Wortmenge über dem abzählbaren Alphabet Alph$(\tau) = \mathrm{VAR} \cup \tau \cup \{\neg, \wedge, \vee, \to, \leftrightarrow, \exists, \forall, (,), =\}$.

Um als Eingabe für Algorithmen (Turingmaschine) zu dienen, sollen Formeln als Wörter über einem *festen endlichen Alphabet* kodiert werden. Dieses Alphabet sei

$$\Gamma := \{R, f, x, 0, 1, [,], \} \cup \{\neg, \wedge, \vee, \to, \leftrightarrow, \exists, \forall, (,), =\}.$$

Für $i \in \mathbb{N}$ bezeichnen wir mit *bin* $i \in \{0,1\}^*$ die Binärdarstellung von i. Wir kodieren das Relationssymbol R^n_i durch das Wort $R[\mathit{bin}\ i][\mathit{bin}\ n]$, das Funktionssymbol f^n_i durch $f[\mathit{bin}\ i][\mathit{bin}\ n]$ und die Variable x_i durch $x[\mathit{bin}\ i]$. Damit können wir auf eindeutige Weise jeder Formel $\psi \in \mathrm{FO}(\tau_\infty)$ eine Kodierung durch ein Wort aus Γ^* zuordnen. Wir unterscheiden im folgenden nicht zwischen einer Formel und ihrer Kodierung und fassen damit FO als Teilmenge von Γ^* auf.

Für jede Formelklasse $X \subseteq \mathrm{FO}$ betrachten wir folgende Entscheidungsprobleme:

$$\begin{aligned}
\mathit{Sat}(X) &:= \{\psi \in X : \psi \text{ ist erfüllbar}\}\\
\mathit{Fin\text{-}sat}(X) &:= \{\psi \in X : \psi \text{ hat ein endliches Modell}\}\\
\mathit{Val}(X) &:= \{\psi \in X : \psi \text{ ist eine Tautologie}\}\\
\mathit{Non\text{-}sat}(X) &:= \{\psi \in X : \psi \text{ ist unerfüllbar}\}\\
\mathit{Inf\text{-}axioms}(X) &:= \{\psi \in X : \psi \text{ ist erfüllbar, hat aber nur unendliche Modelle}\}
\end{aligned}$$

Eine erfüllbare Formel ohne endliche Modelle ist ein *Unendlichkeitsaxiom.* Eine Formelklasse X hat die Endliche-Modell-Eigenschaft, wenn sie keine Unendlichkeitsaxiome enthält, d.h. wenn jede erfüllbare Formel aus X auch ein endliches Modell besitzt.

Für einige dieser Probleme ist unmittelbar einzusehen, dass sie rekursiv aufzählbar sind.

Satz 6.19 (Abstrakter Vollständigkeitssatz). *Die Klasse Val*(FO) *der allgemeingültigen Formeln der Prädikatenlogik ist rekursiv aufzählbar.*

Beweis. Dies folgt aus dem Vollständigkeitssatz, da $\{\psi \in \mathrm{FO} : \vdash \psi\}$ die Haltemenge des folgenden Algorithmus ist:

Auf Input ψ, werden für $n = 1, 2, 3, \ldots$ die endlich vielen Ableitungen erzeugt, die durch höchstens n Anwendungen von Regeln des Sequenzenkalküls unter Verwendung von Formeln der Länge $\leq n$ konstruiert werden können. Der Algorithmus hält, sobald die Sequenz $\varnothing \Rightarrow \psi$ abgeleitet wurde. $\square$

Satz 6.20. *Fin-sat*(FO) *ist rekursiv aufzählbar.*

Beweis. Eine Formel $\psi(x_1, \ldots, x_r)$, mit freien Variablen $x_1, \ldots, x_r$, ist erfüllbar genau dann, wenn ihr existentieller Abschluss $\exists x_1 \cdots \exists x_r \psi$ erfüllbar ist. Es reicht also, Sätze zu betrachten. Für jeden gegebenen Satz $\psi \in \mathrm{FO}$ ist die Menge $\tau(\psi)$ der tatsächlich in ψ vorkommenden Relations- und Funktionssymbole endlich. Daher ist für jedes $n \in \mathbb{N}$ auch die Menge $\mathrm{Str}_n(\tau(\psi))$ aller $\tau(\psi)$-Strukturen mit Universum $\{0, \ldots, n-1\}$ endlich, und wenn ψ überhaupt ein endliches Modell besitzt, dann auch eines in $\bigcup_{n \in \mathbb{N}} \mathrm{Str}_n(\tau(\psi))$. Offensichtlich ist die Modellbeziehung $\mathfrak{A} \models \psi$ für endliche $\mathfrak{A}$ und $\psi \in \mathrm{FO}$ entscheidbar.

Der folgende Algorithmus hat daher als Haltemenge gerade die endlich erfüllbaren Formeln: Gegeben eine Formel $\psi \in \mathrm{FO}$, konstruiere man sukzessive, für $n = 1, 2, \ldots$, alle Strukturen $\mathfrak{A} \in \mathrm{Str}_n(\tau(\psi))$ und prüfe, ob $\mathfrak{A}$ ein Modell (des existentiellen Abschlusses) von ψ ist. Sobald ein solches $\mathfrak{A}$ gefunden ist, hält der Algorithmus. $\square$

Übung 6.6. Zeigen Sie: Wenn $X \subseteq \mathrm{FO}$ entscheidbar ist, und die Endliche-Modell-Eigenschaft besitzt, dann ist $Sat(X)$ entscheidbar.

Satz 6.21 (Church, Turing). *Es gibt eine endliche Signatur $\tau \subseteq \tau_\infty$, so dass Sat*(FO($\tau$)) *– und damit auch Val*(FO(τ)) *– unentscheidbar ist.*

Wir beweisen hier ein allgemeineres Resultat, das den Satz von Church und Turing und ausserdem gleich auch die Unentscheidbarkeit des Erfüllbarkeitsproblems auf endlichen Strukturen impliziert.

Satz 6.22 (Trakhtenbrot). *Es gibt eine endliche Signatur $\tau \subseteq \tau_\infty$, so dass Fin-sat*(FO($\tau$)) *und Non-sat*(FO($\tau$)) *rekursiv untrennbar sind.*

Beweis. Wir werden eine effektive Konstruktion angeben, welche jedem Turing-Akzeptor M einen Satz $\psi_M \in \mathrm{FO}(\tau)$ zuordnet (für ein endliches $\tau \subseteq \tau_\infty$), so dass gilt:

(a) Wenn M das leere Wort akzeptiert, dann hat ψ_M ein endliches Modell.

(b) Wenn M das leere Wort verwirft, dann ist ψ_M unerfüllbar.

Mit dieser Reduktion ist gezeigt, dass $(H_\lambda^+, H_\lambda^-) \leq (\mathit{Fin\text{-}sat}(\mathrm{FO}(\tau)), \mathit{Non\text{-}sat}(\mathrm{FO}(\tau)))$. Da H_λ^+ und H_λ^- rekursiv untrennbar sind, folgt mit Lemma 6.18 die Behauptung.

Sei M ein Turing-Akzeptor mit Zustandsmenge $Q = \{q_0, \ldots, q_r\}$, Anfangszustand q_0, mit Alphabet $\Sigma = \{a_0, \ldots, a_s\}$ (wobei $a_0 = \square$), mit Endzustandsmenge $F = F^+ \cup F^-$ und mit der Übergangsfunktion δ.

Die zu konstruierende Formel ψ_M hat Signatur $\tau = \{0, f, q, p, w\}$, wobei 0 ein Konstantensymbol, f, q, p einstellige Funktionssymbole und w ein zweistelliges Funktionssymbol ist. Abkürzend schreiben wir $\boldsymbol{k}$ für den Term $f^k 0$ (k-malige Anwendung von f auf 0).

Die grundlegende Idee besteht darin, dass Modelle von ψ_M die Berechnung von M auf λ kodieren. Das *intendierte Modell* $\mathfrak{A}$ von ψ_M hat Universum der Form $A = \{0, 1, 2, \ldots, n\}$ oder $A = \mathbb{N}$ (je nachdem, ob die Berechnung von M auf λ endlich oder unendlich ist). Die Funktionssymbole werden wie folgt interpretiert:

- $f(t) = t + 1$, wenn $t + 1 \in A$, und $f(t) = t$, wenn t das letzte Element von A ist.
- $q(t) = i$ genau dann, wenn M sich zur Zeit t im Zustand q_i befindet.
- $p(t)$ ist die Kopfposition von M zur Zeit t.
- $w(s,t) = i$ genau dann, wenn zur Zeit t auf Feld s das Symbol a_i steht.

Konstruktion von ψ_M: Die gesuchte Formel hat die Gestalt

$$\psi_M := \text{START} \wedge \text{COMPUTE} \wedge \text{END}$$

wobei

(1) START $:= (q0 = 0 \wedge p0 = 0 \wedge \forall x\ w(x,0) = 0)$.

Diese Formel drückt aus, dass M sich zur Zeit 0 in der Inputkonfiguration auf λ befindet.

(2) Die zweite Teilformel soll den Fortgang der Berechnung von M formalisieren. Sie hat die Gestalt

$$\text{COMPUTE} = \varphi \wedge \bigwedge_{\delta:(q_i,a_j)\mapsto(q_k,a_\ell,m)} \forall y(\alpha_{i,j} \to \beta_{k,\ell,m}).$$

Dabei drückt

$$\varphi := \forall x \forall y (py \neq x \to w(x,fy) = w(x,y))$$

aus, dass die Bandinschrift auf nicht bearbeiteten Feldern unverändert bleibt, während die Implikation $\alpha_{i,j} \to \beta_{k,\ell,m}$ die von der Übergangsregel $\delta : (q_i,a_j) \mapsto (q_k,a_\ell,m)$ induzierten Änderungen formalisiert. Dabei besagt

$$\alpha_{ij} := (qy = \boldsymbol{i} \wedge w(py,y) = \boldsymbol{j})$$

dass M sich zur Zeit y im Zustand q_i befindet und das Symbol a_j liest, dass also zur Zeit y die besagte Übergangsregel zur Anwendung kommt. Die Formel $\beta_{k,\ell,m}$ besagt, dass zur Zeit $y+1$ die durch diese Regel bestimmten Änderungen realisiert sind. Dabei ist

$$\beta_{k,\ell,m} := (qfy = \boldsymbol{k} \wedge w(py,fy) = \boldsymbol{\ell} \wedge \text{MOVE}_m$$

$$\text{wobei MOVE}_m := \begin{cases} pfy = py & \text{für } m = 0 \\ pfy = fpy & \text{für } m = 1 \\ \exists z(fz = py \wedge pfy = z) & \text{für } m = -1. \end{cases}$$

(3) Schliesslich besagt die Formel

$$\mathrm{END} \;=\; \bigwedge_{\substack{\delta(q_i,a_j)\ \text{undef.}\\ q_i\notin F^+}} \forall y\, \neg\alpha_{ij}$$

dass die Berechnung nur durch eine akzeptierende Konfiguration beendet werden kann.

ψ_M hat die geforderten Eigenschaften:

(1) Offensichtlich ist ψ_M aus $\rho(M)$ effektiv konstruierbar.

(2) Wenn M das leere Wort akzeptiert, dann ist das intendierte Modell $\mathfrak{A}_M$ endlich, und es gilt in der Tat $\mathfrak{A}_M \models \psi_M$.

(3) Es bleibt zu zeigen, dass ψ_M unerfüllbar ist, wenn M das leere Wort verwirft. Sei $\mathfrak{B} = (B, 0, f, q, p, w)$ ein beliebiges Modell von ψ_M; wir weisen nach, dass $\mathfrak{B}$ die Berechnung von M auf λ kodiert und dass diese nie eine verwerfende Konfiguration erreicht. Die Abbildung $\pi : \mathbb{N} \to B$ mit $\pi(t) = \boldsymbol{t}^{\mathfrak{B}}$ ist ein Homomorphismus von $(\mathbb{N}, 0, succ)$ nach $(B, 0, f)$. Wir können daher jedes $t \in \mathbb{N}$ mit seinem Bild in $\mathfrak{B}$ identifizieren. Durch $\mathfrak{B}$ ist eine Folge $C_0, C_1, \ldots$ von Konfiguration kodiert; dabei ist $C_t = (q_i, j, w)$, mit $w = a_{i_0} \ldots a_{i_m} \in \Sigma^*$, wenn

   (a) $\mathfrak{B} \models q\boldsymbol{t} = \boldsymbol{i}$,

   (b) $\mathfrak{B} \models p\boldsymbol{t} = \boldsymbol{j}$,

   (c) für alle $k \leq m$, $\mathfrak{B} \models w(\boldsymbol{k}, \boldsymbol{t}) = \boldsymbol{i_k}$ und für alle $k > m$, $\mathfrak{B} \models w(\boldsymbol{k}, \boldsymbol{t}) = 0$.

   Da $\mathfrak{B} \models \psi_M$ gilt:

   - $C_0 = (q_0, 0, \lambda)$ (da $\mathfrak{B} \models$ START.)
   - Wenn C_t definiert ist, und keine akzeptierende Konfiguration beschreibt, dann ist auch C_{t+1} definiert und es gilt $C_t \vdash_M C_{t+1}$.

   Also ereicht die Berechnung von M auf λ keine verwerfende Konfiguration.

□

Da $Sat(\mathrm{FO}(\tau))$ die Menge der endlich erfüllbaren von der Menge der unerfüllbaren Formeln in $\mathrm{FO}(\tau)$ trennt, ist der Satz von Church und Turing eine unmittelbare Konsequenz des Satzes von Trakhtenbrot.

Übung 6.7. Zeigen Sie, dass auch die Paare *Inf-axioms*(FO) und *Fin-sat*(FO) bzw. *Inf-axioms*(FO) und *Non-sat*(FO) rekursiv untrennbar sind.

Man beachte aber folgenden wichtigen Unterschied zwischen *Sat*(FO) und *Fin-sat*(FO). Die endlich erfüllbaren Formeln sind rekursiv aufzählbar (Satz 6.20), nicht aber die erfüllbaren insgesamt. Da nämlich die Menge der Tautologien rekursiv aufzählbar ist und ψ genau dann unerfüllbar ist, wenn $\neg\psi$ eine Tautologie ist, ist die Menge der unerfüllbaren Formeln rekursiv aufzählbar. Wäre auch die Menge der erfüllbaren Formeln rekursiv aufzählbar, dann wäre sie nach Satz 6.9 sogar entscheidbar, im Widerspruch zum Satz von Church und Turing.

Andererseits erhalten wir aus der Tatsache, dass *Fin-sat*(FO) rekursiv aufzählbar, nicht aber entscheidbar ist, folgende wichtige Konsequenz.

Satz 6.23. *Die Menge* $\{\psi \in \mathrm{FO} : \models_{fin} \psi\}$ *der auf endlichen Strukturen allgemeingültigen Formeln ist nicht rekursiv aufzählbar. Es gibt also keinen korrekten und vollständigen Beweiskalkül für Gültigkeit auf endlichen Strukturen.*

Beweis. Wenn $\{\psi \in \mathrm{FO} : \models_{fin} \psi\}$ rekursiv aufzählbar wäre, dann auch das Komplement von *Fin-sat*(FO). Dann wäre aber *Fin-sat*(FO) entscheidbar, im Widerspruch zum Satz von Trakhtenbrot.

Die zweite Behauptung folgt aus der Tatsache, dass jeder Beweiskalkül ein effektives Aufzählungsverfahren für die Menge der ableitbaren Formeln ergibt. Ein korrekter und vollständiger Beweiskalkül für Gültigkeit im Endlichen würde also implizieren, dass $\{\psi \in \mathrm{FO} : \models_{fin} \psi\}$ rekursiv aufzählbar wäre. □

Die Logik auf endlichen Strukturen unterscheidet sich daher in ganz wesentlichen Punkten von der Logik auf beliebigen (endlichen und unendlichen) Strukturen. Neben dem Vollständigkeitssatz gelten auch viele andere wichtige Sätze der klassischen Logik nicht mehr, wenn die Betrachtung auf endliche Strukturen eingeschränkt wird. Insbesondere trifft dies auf den Kompaktheitssatz zu.

Übung 6.8. Zeigen Sie, dass der Kompaktheitssatz nicht gilt, wenn nur endliche Strukturen betrachtet werden: Konstruieren Sie eine unendliche Formelmenge Φ, so dass jede endliche Teilmenge von Φ ein endliches Modell besitzt, nicht aber Φ selbst.

Die Logik auf endlichen Strukturen ist von Bedeutung für Anwendungen in der Informatik, z.B. für die Komplexitätstheorie und für Datenbanken.

6.4 Der Gödelsche Unvollständigkeitssatz

Wir beweisen in diesem letzten Abschnitt der Vorlesung den berühmten Unvollständigkeitssatz von Gödel, welcher besagt, dass es kein vollständiges und korrektes Beweissystem für die Arithmetik gibt. Aus Zeitgründen können wir dieses Resultat nur sehr knapp behandeln, und müssen insbesondere darauf verzichten, selbstbezügliche Aussagen (arithmetische Sätze, welche ihre eigenen Unbeweisbarkeit behaupten) und den zweiten Gödelschen Unvollständigkeitssatzes zu behandeln (es gibt keinen mathematischen Beweis für die Widerspruchsfreiheit der Mathematik gibt, es sei denn die Mathematik sei widerspruchsvoll).

Die *Arithmetik* ist die Theorie $\mathrm{Th}(\mathfrak{N})$ der Struktur $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$. Der Gödelsche Unvollständigkeitssatz ist eine Konsequenz der *Unentscheidbarkeit der Arithemetik.* Um die Unentscheidbarkeit von $\mathrm{Th}(\mathfrak{N})$ nachzuweisen, werden wir zeigen, dass Berechnungen von Turingmaschinen durch natürliche Zahlen kodiert werden können, und dass diese Kodierungen durch arithmetische Formeln definierbar sind. Dazu wird es notwendig sein, Folgen beliebiger Länge (von natürlichen Zahlen, von Symbolen oder von Konfiguration von Turingmaschinen) durch natürliche Zahlen zu kodieren.

Dazu verwenden wir das folgendes klassische Resultat über Kongruenzen.

Satz 6.24 (Chinesischer Restsatz). *Seien $q_1, \dots, q_n$ paarweise teilerfremd und sei $q = \prod_{i=1}^n q_i$. Dann ist die Funktion*

$$\begin{aligned} F : \mathbb{Z}_q &\to \mathbb{Z}_{q_1} \times \dots \times \mathbb{Z}_{q_n} \\ a &\mapsto (a_1, \dots, a_n) \quad \textit{mit} \quad a \equiv a_j \pmod{q_j} \end{aligned}$$

eine Bijektion von $\mathbb{Z}_q$ nach $\mathbb{Z}_{q_1} \times \dots \times \mathbb{Z}_{q_n}$.

Beweis. Da $\mathbb{Z}_q$ und $\mathbb{Z}_{q_1} \times \dots \times \mathbb{Z}_{q_n}$ endlich sind und gleich viele Elemente enthalten, reicht es zu zeigen, dass F injektiv ist. Seien $a, a' \in \mathbb{Z}_q$ so dass $a \equiv a' \pmod{q_j}$ für $j = 1, \dots, n$. Also wird $a - a'$ von allen q_j geteilt und daher, da die q_j paarweise teilerfremd sind, auch von deren Produkt q. Also ist $a \equiv a' \pmod{q}$. □

Die Kodierung beliebig langer Folgen durch einzelne Zahlen wird durch die Gödelsche β-Funktion geleistet.

Lemma 6.25 (β-Lemma von Gödel). *Es gibt eine totale Funktion $\beta : \mathbb{N}^3 \to \mathbb{N}$, so dass gilt:*

(i) Zu jeder endlichen Folge $(a_0, \dots, a_n)$ über $\mathbb{N}$ gibt es $a, b \in \mathbb{N}$ so dass $\beta(a, b, j) = a_j$, für alle $j \leq n$.

(ii) β ist definierbar in $\mathfrak{N}$, d.h. es gibt eine Formel $\varphi_\beta(x, y, z, v)$, so dass gilt:

$$\mathfrak{N} \models \varphi_\beta[a, b, j, c] \iff \beta(a, b, j) = c.$$

Beweis. Setze $\beta(x, y, z) := x \pmod{y(z+1)+1}$. Offensichtlich ist β definiert durch die Formel

$$\varphi_\beta(x, y, z, v) := v < y(z+1) + 1 \land \exists u (x = uy(z+1) + u + v).$$

Es bleibt zu zeigen, dass wir für alle n und alle $a_0, \dots, a_n$ geeignete Zahlen $a, b \in \mathbb{N}$ finden können, so dass $a \equiv a_j \pmod{b(j+1)+1}$ für $j = 0, \dots, n$. Wir setzten $b := m!$ für $m = \max(n, a_0, \dots, a_n)$.

Behauptung. *Für $0 \leq i < j \leq n$ sind $1 + (i+1)b$ und $1 + (j+1)b$ teilerfremd.*

Andernfalls gibt es ein $p > 1$, welches $1 + (i+1)b$ und $1 + (j+1)b$ teilt. Dann teilt p auch $(j-i)b$, ist aber andererseits kein Teiler von b (sonst könnte p nicht $1 + (i+1)b$ teilen). Also ist p ein Teiler von $j - i$, also $p \leq n$. Dies ist aber unmöglich, da b von von jeder Zahl $\leq n$ geteilt wird. Damit ist die Behauptung bewiesen.

Aus dem Chinesischen Restsatz folgt jetzt die Existenz eines $a < \prod_{j=1}^n (b(j+1)+1)$ so dass $a \equiv a_j \pmod{b(j+1)+1}$ für alle $j =\leq n$. □

Sei M eine Turingmaschine mit Zustandsmenge $Q = \{q_0, \dots, q_r\}$, Anfangszustand q_0 und mit Alphabet $\Sigma = \{a_0, \dots, a_s\}$, wobei $a_0 = \square$.

Ein Tripel $(i, p, a) \in \mathbb{N}^3$ kodiert (mit Parameter b) eine Konfiguration von M, wenn $i \leq r$ einen Zustand beschreibt, und wenn a die Kodierung einer Inschrift $a_{i_0} \cdots a_{i_m} \in \Sigma^*$ im Sinn des β-Lemmas ist, d.h., wenn $\beta(a, b, j) = i_j$ für $j = 0, \dots, m$.

Man beachte, dass das leere Wort λ durch 0 kodiert werden kann, die Anfangskonfiguration von M auf λ also durch $(0, 0, 0)$.

Lemma 6.26. *Es gibt eine Formel* $\alpha(x, y, z, x', y, z', v) \in \mathrm{FO}(\tau_{ar})$*, so dass für alle* $b \in \mathbb{N}$ *und (mit Parameter* b*) kodierten Konfigurationen* (i, p, a) *bzw* (i', p', a') *gilt:*

$$(i, p, a) \vdash_M (i', p', a') \iff \mathfrak{N} \models \alpha[i, p, a, i', p', a', b].$$

Beweis. Wir halten zunächst fest, dass die Formel $\varphi_\beta(z, v, y, \boldsymbol{i})$ besagt, dass das y-te Zeichen der durch z mit Parameter v kodierten Bandinschrift das Symbol a_i ist.

Doe gewünschte Formel ist ähnlich aufgebaut, wie die Teilformel COMPUTE im Beweis des Satzes von Trakhtenbrot. Eine erste Teilformel drückt aus, dass die durch z und z' kodierten Inschriften auf nicht bearbeiteten Feldern übereinstimmen, und eine zweite Teilformel drückt aus, dass die Konfiguration (x', y', z') durch die von einer δ-Übergangsregel induzierten lokalen Änderungen aus der Konfiguartion (x, y, z) hervorgeht.

$$\begin{aligned} \alpha(x, y, z, x'y, z', v) := {} & \forall y'' \forall w (y'' \neq y \to (\varphi_\beta(z, v, y'', w) \leftrightarrow \varphi_\beta(z', v, y'', w)) \\ & \wedge \bigvee_{\delta:(q_i, a_j) \mapsto (q_k, a_\ell, m)} (x = \boldsymbol{i} \wedge \varphi_\beta(z, v, y, \boldsymbol{j}) \wedge x' = \boldsymbol{k} \wedge \varphi_\beta(z', v, y, \boldsymbol{\ell}) \wedge y' = y + m). \end{aligned}$$

□

Satz 6.27. $\mathrm{Th}(\mathfrak{N})$ *ist unentscheidbar.*

Beweis. Wir reduzieren das Halteproblem auf leerem Band auf $\mathrm{Th}(\mathfrak{N})$. Zu diesem Zweck konstruieren wir auf effektive Weise für jede Turingaschine M eine Formel $\psi_M(x, y, z, x', y', z') \in \mathrm{FO}(\tau_{ar})$, so dass für alle $b \in \mathbb{N}$ und alle (mit Parameter b) kodierten Konfigurationen (i, p, a) bzw (i', p', a') gilt:

$$(i, p, a) \vdash_M^* (i', p', a') \iff \mathfrak{N} \models \psi_M[i, p, a, i', p', a'].$$

Daraus erhalten wir unmittelbar die gewünschte Reduktion: M hält auf λ genau dann wenn

$$\mathfrak{N} \models \exists x \exists y \exists z (\psi_M(0, 0, 0, x, y, z) \wedge \bigwedge_{q_i \in F} x = \boldsymbol{i}.$$

Um ψ_M zu konstruieren formuliere man die Aussage $(i, p, a) \vdash_M^* (i', p', a')$ auf folgende Weise um:

Es gibt eine Folge $u = (u_0, u_1, u_2, \dots, u_{3s}, u_{3s+1}, u_{3s+2})$ *mit*

(1) $(u_0, u_1, u_2) = (i, p, a)$.

(2) $(u_{3s}, u_{3s+1}, u_{3s+2}) = (i', p', a')$.

(3) Für alle $m < s$ *gilt:* $(u_{3m}, u_{3m+1}, u_{3m+2}) \vdash_M (u_{3m+3}, u_{3m+4}, u_{3m+5})$.

Es ist nicht schwierig einzusehen, dass diese Aussage mit Hilfe der β-Funktion in $\mathrm{FO}(\tau_{ar})$ ausgedrückt werden kann. □

Übung 6.9. Konstruieren Sie die Formel ψ_M explizit.

Um die Bedeutung des soeben bewiesenen Resultats besser zu verstehen führen wir den Begriff der rekursiven Axiomatisierbarkeit einer Theorie ein.

Definition 6.28. Eine Theorie T ist *rekursiv axiomatisierbar*, wenn eine entscheidbare Menge $\Phi \subseteq T$ von Axiomen existiert, so dass $T = \Phi^{\models} := \{\psi : \Phi \models \psi\}$.

Satz 6.29. *Sei T eine vollständige Theorie. Dann sind die folgenden Aussagen äquivalent.*

(1) T ist rekursiv axiomatisierbar.

(2) Es gibt ein rekursiv aufzählbares Axiomensystem Φ, so dass $T = \Phi^{\models}$.

(3) T ist rekursiv aufzählbar.

(4) T ist entscheidbar.

Beweis. (1) $\Rightarrow$ (2): Trivial.

(2) $\Rightarrow$ (3): Wenn Φ rekursiv aufzählbar ist, dann auch die Menge aller endlichen $\Phi_0 \subseteq \Phi$. (Sei M ein Algorithmus mit Haltemenge $L(M) = \Phi$. Gegeben $\Phi_0 = \{\varphi_1, \dots, \varphi_m\}$ wende man M nacheinander auf $\varphi_1, \dots, \varphi_n$ an und halte wenn M auf allen φ_i hält.)

Indem man systematsch alle endlichen $\Phi_0 \subseteq \Phi$ und alle im Sequenzenkalkül ableitbaren Sequenzen der Form $\Phi_0 \Rightarrow \psi$ aufzählt, erhält man ein Aufzählungsverfahren für T.

(3) $\Rightarrow$ (4): T ist vollständig, also ist $\psi \notin T$ genau dann, wenn $\neg\psi \in T$. Mit T ist also auch das Komplement von T rekursiv aufzählbar. Also ist T entscheidbar.

(4) $\Rightarrow$ (1): Wähle $\Phi = T$.

□

Korollar 6.30. *Die Arithmetik* $\mathrm{Th}(\mathfrak{N})$ *ist nicht rekursiv axiomatisierbar.*

Definition 6.31. Ein *abstraktes Beweissystem* für (eine beliebige Sprache) $T \subseteq \Gamma^*$ ist ein Paar (B, F) mit folgenden Eigenschaften:

(1) $B \subseteq \Sigma^*$ ist entscheidbar;

(2) $F : B \to \Gamma^*$ ist eine totale berechenbare Funktion.

Dabei sei B die Menge aller Beweise des Systems; es ist also entscheidbar, ob ein gegebenes Wort $b \in \Sigma^*$ ein Beweis ist. Die Funktion F ordnet jedem Beweis b das von ihm bewiesene Wort $F(b)$ zu. Mit $\mathrm{Bew}(B, F)$ bezeichnen wir die Gesamtheit der vom System (B, F) bewiesenen Objekte:

$$\mathrm{Bew}(B, F) := \{y \in \Gamma^* : \text{es gibt ein } b \in B \text{ mit } F(b) = y\}.$$

Ein Beweissystem (B, F) ist *korrekt* für T, wenn $\mathrm{Bew}(B, F) \subseteq T$ (nur Objekte aus T werden bewiesen) und *vollständig* für T, wenn $\mathrm{Bew}(B, F) \supseteq T$ (alle Objekte aus T werden bewiesen).

Aus der Entscheidbarkeit von B und der Berechenbarkeit von F folgt unmittelbar, dass $\mathrm{Bew}(B,F)$ rekursiv aufzählbar ist.

Sei $T \subseteq \mathrm{FO}(\tau)$ eine Theorie und Φ ein entscheidbares Axiomensystem für T. Dann ist (B,F) mit

$$B = \{\Phi_0 \Rightarrow \psi : \Phi_0 \subseteq \Phi \text{ und } \Phi_0 \Rightarrow \psi \text{ ist ableitbar im Sequenzenkalkül}\}$$
$$F(\Phi_0 \Rightarrow \psi) := \psi$$

ein korrektes und vollständiges Beweissystem für T.

Satz 6.32 (Gödelscher Unvollständigkeitssatz). *Jedes korrekte Beweissystem für* $\mathrm{Th}(\mathfrak{N})$ *ist unvollständig.*

Beweis. Andernfalls wäre $\mathrm{Th}(\mathfrak{N})$ rekursiv aufzählbar und daher auch entscheidbar. □

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*