Logik in der Informatik
PD Dr. Kurt Sieber
Universität Siegen
SS 2003

Vorlesungsmitschrift von
Lars Weiser

E-Mail: lars.weiser@student.uni-siegen.de
Homepage URL: http://www.stud.uni-siegen.de/lars.weiser/

4. Dezember 2003

Anmerkung

Bei dem vorliegenden Skriptum handelt es sich um die Mitschrift der Vorlesung Logik in der Informatik von Herrn Dr. Kurt Sieber, die er im Rahmen einer einsemestrigen Hauptstudiumsveranstaltung im SS 2003 an der Universität Siegen gehalten hat. Das Skriptum weicht jedoch an einigen Stellen vom originalen Wortlaut ab.
Ein besonderer Dank gilt an dieser Stelle Herrn Dr. Sieber, der die Kapitel 1 bis 7 Korrektur las und mir an der ein oder anderen Stelle einen guten Tip zu LaTeX gegeben hat.

Siegen, im Dezember 2003 *Lars Weiser*

Literatur

Zur Nacharbeitung und Vertiefung des Stoffes wurde folgendes Büchlein empfohlen:

H.-D. Ebbinghaus / J. Flum / W. Thomas *Einführung in die mathematische Logik.* Springer-Verlag

Inhaltsverzeichnis

Kapitel 1

Motivation

„Logik ist die Anatomie des Denkens.“
John Locke (1632-1704)

Inhalt:

Mathematische Logik und ihre Anwendungen in der Informatik

Gegenstand der mathematischen Logik:

Die „Sprache der Mathematik“ (Definitionen, Sätze, Beweise, Schlußregeln, etc.) wird formalisiert und wird damit selbst zum Gegenstand mathematischer Betrachtungen.

Verschiedene Logiken

Man differenziert im wesentlichen zwischen den folgenden Logiken:

- *Aussagenlogik*: nur die bekannten Junktoren $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
- *Prädikatenlogik*: zusätzlich: Variablen, Quantoren $\forall, \exists$ sowie optional Gleichheit $\equiv$
  - *erster Stufe*: nur Quantoren über Elementen
  - *zweiter Stufe*: auch Quantoren über Eigenschaften (oder Teilmengen) von Elementen
  - *höherer Stufe*: Quantoren über Mengen von Mengen usw.
- *Temporale Logik*: Einführung eines Zeitbegriffs, z.B. *„von nun an gilt“* $\rightsquigarrow$ Aussagen über den Verlauf von Programmen (wichtig für parallele Prozesse)
- *Logiken für Programmverifikation*: z.B. Hoare-Logik

Wir behandeln hier zunächst: *Prädikatenlogik erster Stufe*

Ursprüngliche Motivation (Mathematik)

Die gesamte Mathematik sollte auf eine präzise formale Grundlage gestellt werden. Man hatte Widersprüche in der „naiven Mengenlehre“ entdeckt, z.B. RUSSELSCHES[1] Paradox: *Sei A die Menge aller Mengen B, die sich nicht selbst als Element enthalten, also*

$$A =_{\text{def}} \{B \mid B \text{ Menge}, B \notin B\}$$

Die Frage ist nun: $A \in A$? Wir betrachten hierzu die Fälle

1. $A \in A \Rightarrow A \notin A$ *Widerspruch*
2. $A \notin A \Rightarrow A \in A$ *Widerspruch*

Also muß der Widerspruch schon in der Definition von A liegen. (Populärwissenschaftliche Version der Antinomie: *„Der Barbier rasiert alle Männer, die sich nicht selbst rasieren.“*)

Heutige Motivation (Informatik)

Durch die Formalisierung lassen sich Beweise auf Rechnern ausführen (nicht unbedingt finden) $\rightsquigarrow$ verschiedene Anwendungen, wie z.B.

- *Logische Programmiersprachen* (`PROLOG`)
- *Theorem Proving* (maschinelles Beweisen von mathematischen Sätzen)
- *Programm-Verifikation* (auch parallele Prozesse, Protokolle)
- *Künstliche Intelligenz* (wissensbasierte Systeme)

[1] BERTRAND RUSSEL (18721970), engl. Philosoph und Mathematiker, schuf unter anderem zusammen mit ALFRED NORTH WHITEHEAD die „Principia Mathematica“

Kapitel 2

Prädikatenlogik erster Stufe

„Der Beginn der Weisheit ist die Definition der Begriffe.“
Sokrates (470-399 v.Chr.)

2.1 Syntax der Prädikatenlogik erster Stufe (mit Gleichheit)

2.1.1 Der Zeichenvorrat

Der *Zeichenvorrat* ist ein für allemal vorgegeben:

- eine abzählbar unendliche Menge $X = \{v_0, v_1, v_2, \ldots\}$, deren Elemente wir *Variablen* nennen.
- die *logischen Zeichen*
  - $\neg$ *Negation*: „Nicht...“
  - $\wedge$ *Konjunktion*: „... und...“
  - $\vee$ *Disjunktion*: „... oder ...“
  - $\rightarrow$ *Implikation*: „Wenn..., dann gilt...“
  - $\leftrightarrow$ *Äquivalenz*: „... genau dann, wenn gilt...“
  - $\forall$ *Allquantor*: „Für alle... gilt...“
  - $\exists$ *Existenzquantor*: „Es gibt (mindestens) ein..., so daß gilt...“
  - $\equiv$ *Gleichheitszeichen*
- *Hilfszeichen*: „(“, „)“, „,“, „.“

Bemerkung 2.1.1. *Zur Erinnerung: Eine Menge M heißt* abzählbar*, falls $M = \emptyset$ oder eine surjektive Abbildung $f : \mathbb{N} \longrightarrow M$ existiert. Ist $M \neq \emptyset$ und gibt es keine surjektive Abbildung $f : \mathbb{N} \longrightarrow M$, so heißt M* überabzählbar*.*

Definition 2.1.1 (Signatur). *Eine* Signatur *(oder* Symbolmenge*) S für die Prädikatenlogik erster Stufe besteht aus:*

- *einer Menge R_n für jedes $n \geq 1$, ein Element $r \in R_n$ heißt* Relationszeichen *(oder* Prädikatzeichen*) der Stelligkeit n;*
- *einer Menge F_n für jedes $n \geq 1$, ein Element $f \in F_n$ heißt* Funktionszeichen *der Stelligkeit n*
- *einer Menge C, ein Element $c \in C$ heißt* Konstante

Bemerkung 2.1.2. *In der Literatur werden gelegentlich Konstanten auch als nullstellige Funktionen betrachtet und behandelt.*

All diese Mengen müssen paarweise disjunkt sein, d.h. für jedes Zeichen ist eindeutig festgelegt, ob es sich um eine Variable, eine Konstante,... handelt und welche Stelligkeit es besitzt (in der Praxis nicht immmer erwünscht: *Überladen von Operatoren*). Ansonsten keine Einschränkungen an diese Mengen, d.h. sie dürfen

- *leer* sein
- *unendlich* sein (sogar *überabzählbar*)

„Typisch“ ist die folgende Situation: S besteht nur aus *endlich vielen* Zeichen, d.h. nur endlich viele der Mengen R_n, F_n, C sind $\neq \emptyset$, und die sind alle endlich.

Beispiel 2.1.1. *Die Signatur $S^<_{\mathrm{Ar}}$ (*Signatur der Arithmetik*) besteht aus:*

- $C = \{0, 1\}$
- $F_2 = \{+, *\}$
- $R_2 = \{<\}$
- $F_n = R_n = \emptyset$ *für alle* $n \neq 2$

oder kürzer: $S^<_{\mathrm{Ar}} = \{0, 1, +, *, <\}$ mit den üblichen Stelligkeiten

2.1.2 Terme und Formeln

Definition 2.1.2 (Term). *Sei S eine Signatur. Die* Menge T^S aller Terme *über S ist induktiv definiert durch:*

(a) Jedes $x \in X$ liegt in T^S, also $X \subseteq T^S$

(b) Jedes $c \in C$ liegt in T^S ($C \subseteq T^S$)

(c) Wenn $f \in F_n$ und $t_1, \ldots, t_n \in T^S$, dann auch $f(t_1, \ldots, t_n) \in T^S$

Beispiel 2.1.2. *Für $S = S^<_{\mathrm{Ar}}$ ist z.B. $*(+(v_3, 1), +(0, v_1)) \in T^S$*

Definition 2.1.3 (Formel). *Sei S eine Signatur. Die* Menge L^S aller Formeln *(oder* Ausdrücke*) über S ist induktiv definiert durch:*

(a) Wenn $t_1, t_2 \in T^S$, dann $t_1 \equiv t_2 \in L^S$

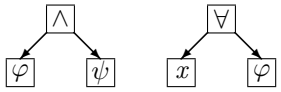
(b) Wenn $t_1, \ldots, t_n \in T^S$, dann $r(t_1, \ldots, t_n) \in L^S$

(c) Wenn $\varphi \in L^S$, dann $\neg\varphi \in L^S$

(d) Wenn $\varphi, \psi \in L^S$, dann: $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$, $\varphi \leftrightarrow \psi \in L^S$

(e) Wenn $\varphi \in L^S$, $x \in X$, dann: $\forall x.\, \varphi \in L^S$, $\exists x.\, \varphi \in L^S$

Bemerkung 2.1.3. *Es handelt sich hier um abstrakte Syntax, d.h. wir nehmen an, daß wir die (Baum-) Struktur der Terme und Formeln kennen, z.B.*



Die Formeln aus (a) und (b) heißen „atomar". L^S heißt die Sprache der Prädikatenlogik (1. Stufe) *über der Signatur S.*

Beispiel 2.1.3. *Sei $S = S^{<}_{\mathrm{Ar}}$. Dann sind:*

(a) $<(v_1, +(v_3, 1))$,

(b) $\forall v_1.\, \exists v_2.\, <(v_1, v_2)$,

(c) $\forall v_1.\, \forall v_2.\, \exists v_3.\, <(v_1, v_3) \wedge\ <(v_3, v_2)$,

(d) $\forall v_1.\, \exists v_2.\, 0 \equiv 1$

Formeln, also Elemente der Sprache L^S.

Bezeichnung 2.1.1. *Vereinbarung zur* konkreten Syntax *(für die Beispiele):*

- *Anstelle von $v_1, v_2, \ldots$ benutzen wir auch andere Kleinbuchstaben $x, y, z, \ldots$*
- *Wenn es üblich ist, benutzen wir Infixnotation für Funktions- und Relationszeichen, z.B. für $+, -, *, <, \ldots$ und die üblichen Prioritäten*
- *Prioritäten für die logischen Zeichen:*
  - *Das Gleichheitszeichen $\equiv$ bindet am stärksten,*
  - *dann folgt das Negationszeichen $\neg$,*
  - *dann $\wedge, \vee$; beide sind linksassoziativ und besitzen gleiche Priorität,*
  - *dann folgen $\to$ und $\leftrightarrow$, und*
  - *Quantoren $\forall, \exists$ binden am schwächsten, d.h ihr Gültigkeitsbereich erstreckt sich soweit wie möglich nach rechts*

- $\forall x_1, \ldots, x_n. \varphi$ *steht für* $\forall x_1, \ldots, \forall x_n. \varphi$, $\exists x_1, \ldots, x_n. \varphi$ *für* $\exists x_1, \ldots, \exists x_n. \varphi$
- $\bigwedge_{i=1}^{n} \varphi_i$ *steht für* $\varphi_1 \wedge \ldots \wedge \varphi_n$
- $\bigvee_{i=1}^{n} \varphi_i$ *steht für* $\varphi_1 \vee \ldots \wedge \varphi_n$

Beispiel 2.1.4. *Beispiele sind:*

(a) $\forall x, y, z. x < y \wedge y < z \rightarrow x < z$

(b) $(\forall x. \exists y. x < y) \rightarrow \exists y. 0 < y$

2.1.3 Freie Variablen

Definition 2.1.4 ((Frei vorkommende Variable). *Für jeden Term* $t \in T^S$ *sei* $var(t) \subseteq X$ *die* Menge aller in t vorkommenden Variablen*. Für jede Formel* $\varphi \in L^S$ *sei* $frei(\varphi) \subseteq X$ *durch Induktion über die Größe von* φ *wie folgt definiert:*

(a) $frei(t_1 \equiv t_2) = var(t_1) \cup var(t_2)$

(b) $frei(r(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} var(t_i)$

(c) $frei(\neg\varphi) = frei(\varphi)$

(d) $frei(\varphi \wedge \psi) = frei(\varphi \vee \psi) = frei(\varphi \rightarrow \psi) = frei(\varphi \leftrightarrow \psi) = frei(\varphi) \cup frei(\psi)$

(e) $frei(\forall x. \varphi) = frei(\exists x. \varphi) = frei(\varphi) \setminus \{x\}$

$frei(\varphi)$ *heißt die* Menge der in φ frei vorkommenden Variablen.

Bezeichnung 2.1.2. *Kommt eine Variable in einer Formel* nicht frei *vor, so nennt man dieses Vorkommen auch* gebunden.

Beispiel 2.1.5. $frei(x < 0 \wedge \forall y. \exists y. x < y \wedge y < z) = \{x, z\}$

Definition 2.1.5. *(a) Eine Formel* φ *heißt* abgeschlossen *(oder* Satzform*, engl.:* sentence*), wenn* $frei(\varphi) = \emptyset$*, sonst heißt* φ offen.

(b) L_n^S *sei die* Menge aller Formeln $\varphi \in L^S$ *mit* $frei(\varphi) = \{v_0, \ldots, v_{n-1}\}$. *Insbesondere ist* L_0^S *die* Menge aller abgeschlossenen Formeln.

2.2 Semantik der Prädikatenlogik erster Stufe

2.2.1 Strukturen und Belegungen

Es muß festgelegt werden:

- ein *„Grundbereich“*, aus dem die Werte der Konstanten und Variablen genommen werden, und über dem die Funktionen und Relationen definiert sind.
- die *Bedeutung* der Konstanten, Funktions- und Relationszeichen

Definition 2.2.1 (Struktur). *Sei S eine Signatur. Eine* S-Struktur *(oder auch* S-Algebra*) ist ein Paar $\mathcal{A} = (A, \alpha)$, wobei gilt:*

(a) A ist eine nichtleere Menge, man bezeichnet A als Grundbereich *(oder* Träger, Trägermenge, Universum*) der Struktur $\mathcal{A}$*

(b) α ist eine auf S definierte Abbildung, für die gilt:

1. *$\alpha(c) \in A$ für jedes $c \in C$*
2. *$\alpha(f) : A^n \longrightarrow A$ für jedes $f \in F_n$*
3. *$\alpha(r) \subseteq A^n$ für jedes $r \in R_n$*

Bezeichnung 2.2.1. *Statt $\alpha(c)$, $\alpha(f)$, $\alpha(r)$ schreibt man kurz: $c^{\mathcal{A}}$, $f^{\mathcal{A}}$, $r^{\mathcal{A}}$. Wenn $S = \{s_1, \ldots, s_m\}$ endlich ist, schreibt man eine S-Struktur $\mathcal{A}$ auch in der Form $\mathcal{A} = (A, s_1^{\mathcal{A}}, \ldots, s_m^{\mathcal{A}})$.*

Beispiel 2.2.1. *Mögliche $S_{\mathrm{Ar}}^{<}$-Strukturen sind:*

(a) $\mathcal{N} = (\mathbb{N}, 0^{\mathcal{N}}, 1^{\mathcal{N}}, +^{\mathcal{N}}, *^{\mathcal{N}}, <^{\mathcal{N}})$ mit

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ *die* Menge der natürlichen Zahlen,
- $0^{\mathcal{N}} = 0$ *(die Zahl* 0*),*
- $1^{\mathcal{N}} = 1$ *(die Zahl* 1*),*
- $+^{\mathcal{N}} : \mathbb{N}^2 \longrightarrow \mathbb{N}$ *die gewöhnliche Addition auf* $\mathbb{N}$*,*
- $*^{\mathcal{N}} : \mathbb{N}^2 \longrightarrow \mathbb{N}$ *die gewöhnliche Multiplikation auf* $\mathbb{N}$ *und*
- $<^{\mathcal{N}} = \{(m, n) \in \mathbb{N} \mid m < n\}$ *die „Kleiner als“-Relation*

(b) $\mathcal{Z} = (\mathbb{Z}, 0^{\mathcal{Z}}, 1^{\mathcal{Z}}, \ldots)$ mit

- $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ *die* Menge der ganzen Zahlen *und*
- $0^{\mathcal{Z}}$, $1^{\mathcal{Z}}, \ldots$ *wie üblich*

Ähnlich: $\mathcal{Q} = (\mathbb{Q}, \ldots)$ und $\mathcal{R} = (\mathbb{R}, \ldots)$

(c) $\mathcal{A} = (\wp(\mathbb{N}), 0^{\mathcal{A}}, 1^{\mathcal{A}}, +^{\mathcal{A}}, *^{\mathcal{A}}, <^{\mathcal{A}})$ mit

- $0^{\mathcal{A}} = \emptyset$*,*
- $1^{\mathcal{A}} = \mathbb{N}$*,*
- $+^{\mathcal{A}} = \cup$*,*
- $*^{\mathcal{A}} = \cap$ *und*
- $<^{\mathcal{A}} = \subseteq$

Jetzt müssen noch Werte für die Variablen bereitgestellt werden. Dazu die folgende

Definition 2.2.2 (Belegung, Interpretation). *Sei S eine Signatur.*

(a) *Eine zur S-Struktur* $\mathcal{A} = (A, \alpha)$ passende Belegung *ist eine (totale) Funktion* $\beta : X \longrightarrow A$.

(b) *Eine* S-Interpretation *ist ein Paar* $\mathcal{I} = (\mathcal{A}, \beta)$, *wobei* $\mathcal{A}$ *eine S-Struktur ist.*

Bemerkung 2.2.1. *„Interpretation" wird in der Literatur oft als Synonym für „Struktur" oder für den „Abbildungsteil"* α *einer Struktur benutzt.*

Überblick: drei Ebenen

Ebene	**Syntax**	**Semantik**
1	*Logische Zeichen*	*fest vorgegeben*
2	*Zeichen der Signatur*	*durch die Struktur* $\mathcal{A}$ *festgelegt*
3	*Variablen*	*durch die Belegung* β *festgelegt*

Bezeichnung 2.2.2. *(a) Seien* A, B *Mengen,* $f : A \longrightarrow B$ *eine Funktion,* $a \in A$, $b \in B$. *Dann sei* $f[b/a]$ *diejenige Funktion* $g : A \longrightarrow B$ *mit:*

$$g(c) = \begin{cases} f(c), & \text{falls } c \neq a \\ b, & \text{sonst} \end{cases}$$

d.h. $f[b/a]$ *ist die Funktion, die sich von* f *nur darin unterscheidet, daß sie an der Stelle* a *den Wert* b *annimmt (Speziell:* $\beta[a/x]$, *falls* $x \in X$, $a \in A$*).*

(b) Wenn $\mathcal{I} = (\mathcal{A}, \beta)$, *dann sei* $\mathcal{I}[a/x]$ *die Interpretation* $(\mathcal{A}, \beta[a/x])$. *Alternative Schreibweisen:* β^a_x, $\beta[x := a]$, $\beta[x/a]$, $\beta[x \leftarrow a], \ldots$

2.2.2 Gültigkeit und Modelle

Ziel: „Auswertung" von Termen und Formeln in einer Interpretation

Definition 2.2.3. *Sei* S *eine Signatur,* $\mathcal{A} = (A, \alpha)$ *eine S-Struktur und* $\mathcal{I} = (\mathcal{A}, \beta)$ *eine zugehörige Interpretation, d.h.* $\beta : X \longrightarrow A$. *Dann ordnen wir jedem Term* $t \in T^S$ *einen Wert* $\mathcal{I}(t) \in A$ *durch folgende Induktion über die Größe von* t *zu:*

(a) $\mathcal{I}(x) = \beta(x)$ *für jedes* $x \in X$

(b) $\mathcal{I}(c) = c^{\mathcal{A}}$ *für jedes* $c \in C$

(c) $\mathcal{I}(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n))$ *für jedes* $f \in F_n$

Beispiel 2.2.2. $S = S^{<}_{\mathrm{Ar}}$, $\mathcal{I} = (\mathcal{N}, \beta)$ *mit* $\beta(x) = 3$, $\beta(y) = 5$. *Dann ist* $\mathcal{I}((x + 1) * y) = *^{\mathcal{N}}(+^{\mathcal{N}}(3, 1), 5) = 20$.

Definition 2.2.4. *Sei* S *Signatur,* $\mathcal{A}$ *und* $\mathcal{I}$ *wie vorher. Dann ordnen wir jeder Formel* $\varphi \in L^S$ *einen* Wahrheitswert $\mathcal{I}(\varphi) \in \{true, false\}$ *zu, durch folgende Induktion über die Größe von* φ*:*

(a) $\mathcal{I}(t_1 \equiv t_2) = \mathit{true} :\Leftrightarrow \mathcal{I}(t_1) = \mathcal{I}(t_2)$, *Gleichheit in* A

(b) $\mathcal{I}(r(t_1, \ldots, t_n)) = \mathit{true} :\Leftrightarrow (\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n)) \in r^{\mathcal{A}}$

(c) $\mathcal{I}(\neg\varphi) = \mathit{true} :\Leftrightarrow \mathcal{I}(\varphi) = \mathit{false}$

(d) $\mathcal{I}(\varphi \wedge \psi) = \mathit{true} :\Leftrightarrow \mathcal{I}(\varphi) = \mathit{true}$ *und* $\mathcal{I}(\psi) = \mathit{true}$

$\mathcal{I}(\varphi \vee \psi) = \mathit{true} :\Leftrightarrow \mathcal{I}(\varphi) = \mathit{true}$ *oder* $\mathcal{I}(\psi) = \mathit{true}$

$\mathcal{I}(\varphi \to \psi) = \mathit{true} :\Leftrightarrow \mathcal{I}(\varphi) = \mathit{false}$ *oder* $\mathcal{I}(\psi) = \mathit{true}$

$\mathcal{I}(\varphi \leftrightarrow \psi) = \mathit{true} :\Leftrightarrow \mathcal{I}(\varphi) = \mathcal{I}(\psi)$, *Gleichheit auf* $\{\mathit{true}, \mathit{false}\}$

(e) $\mathcal{I}(\forall x.\, \varphi) = \mathit{true} :\Leftrightarrow \mathcal{I}[a/x](\varphi) = \mathit{true}$ *für alle* $a \in A$

$\mathcal{I}(\exists x.\, \varphi) = \mathit{true} :\Leftrightarrow$ *es existiert ein* $a \in A$ *mit* $\mathcal{I}[a/x](\varphi) = \mathit{true}$

Bezeichnung 2.2.3. *Für* $\mathcal{I}(\varphi) = \mathit{true}$ *schreibt man auch:* $\mathcal{I} \models \varphi$ *(oder* $\models_{\mathcal{I}} \varphi$ *oder* $\mathcal{A}, \beta \models \varphi$ *oder* $\models_{\mathcal{A},\beta} \varphi$*). Man hat dafür folgende Sprechweisen:*

- φ gilt *in* $\mathcal{I}$
- φ *ist* gültig *in* $\mathcal{I}$
- $\mathcal{I}$ erfüllt φ
- $\mathcal{I}$ *ist* Modell *von (für)* φ

Beispiel 2.2.3. *Hier zwei Beispiele:*

(a) *Sei* $S = S_{\mathrm{Ar}} = \{0, 1, +, *\}$, *sei* $\mathcal{N} = (\mathbb{N}, \ldots)$ *die übliche Struktur und sei* $\varphi \in L^S$ *die Formel* $\exists y.\, x \equiv y * y$. *Für welche Belegungen* $\beta : X \longrightarrow \mathbb{N}$ *gilt* $\mathcal{N}, \beta \models \varphi$*?*

$$\begin{aligned}
\mathcal{N}, \beta \models \varphi \quad &\Leftrightarrow \quad \textit{es ex. ein } n \in \mathbb{N} \textit{ mit } \mathcal{N}, \beta[n/y] \models x \equiv y * y \\
&\Leftrightarrow \quad \textit{es ex. ein } n \in \mathbb{N} \textit{ mit } (\mathcal{N}, \beta[n/y])(x) = (\mathcal{N}, \beta[n/y])(y * y) \\
&\Leftrightarrow \quad \textit{es ex. ein } n \in \mathbb{N} \textit{ mit } \beta[n/y](x) = \beta[n/y](y) *^{\mathcal{N}} \beta[n/y](y) \\
&\Leftrightarrow \quad \textit{es ex. ein } n \in \mathbb{N} \textit{ mit } \beta(x) = n *^{\mathcal{N}} n \\
&\Leftrightarrow \quad \beta(x) \textit{ ist eine Quadratzahl}
\end{aligned}$$

(b) *Sei* $S = S_{\mathrm{Ar}}$ *und* $\mathcal{N}$ *wie in (a). Sei* φ *die Formel* $\exists z.\, \neg z \equiv 0 \wedge x + z \equiv y$. *Dann gilt für jedes* $\beta : X \longrightarrow \mathbb{N}$*:*

$$\begin{aligned}
\mathcal{N}, \beta \models \varphi \quad &\Leftrightarrow \quad \textit{es ex. ein } n \in \mathbb{N} \textit{ mit } \mathcal{N}, \beta[n/z] \models \neg z \equiv 0 \wedge x + z \equiv y \\
&\Leftrightarrow \quad \textit{es ex. ein } n \in \mathbb{N} \textit{ mit } n \neq 0 \textit{ und } \beta(x) + n = \beta(y) \\
&\Leftrightarrow \quad \beta(x) < \beta(y)
\end{aligned}$$

Lehre aus den Beispielen:
Bei vorgegebener S-Struktur $\mathcal{A} = (A, \alpha)$ kann man eine Formel $\varphi \in L^S$ als Aussage über die (Belegungen der) frei vorkommenden Variablen betrachten.

Definition 2.2.5 (Definitierbarkeit). *Sei S eine Signatur, $\mathcal{A} = (A, \alpha)$ eine S-Struktur und $n \geq 1$.*

(a) Eine Formel $\varphi \in L^S$ definiert *die Relation $R \subseteq A^n$, wenn gilt:*

$$R = \{(\beta(v_0), \ldots, \beta(v_{n-1})) \mid \beta : X \longrightarrow A \text{ und } \mathcal{A}, \beta \models \varphi\}$$

$R \subseteq A^n$ heißt definierbar *in $\mathcal{A}$, wenn ein $\varphi \in L^S_n$ existiert, das R definiert.*

(b) Eine Formel $\varphi \in L^S_{n+1}$ definiert *die (partielle) Funktion $f : A^n \rightharpoonup A$, wenn φ die Relation*

$$graph(f) =_{\text{def}} \{(a_1, \ldots, a_n, f(a_1, \ldots, a_n)) \mid a_1, \ldots, a_n \in A\}$$

definiert. $f : A^n \rightharpoonup A$ heißt definierbar*, wenn es eine Formel $\varphi \in L^S_{n+1}$ gibt, die die Funktion f definiert.*

Bemerkung 2.2.2. *Oft bezeichnet man* partielle Funktionen *auch als* funktionale Relationen*. Einstellige Relationen können auch als deskriptive Eigenschaften eines Elements aufgefaßt werden.*

Beispiel 2.2.4. *(a) $R = \{n^2 \mid n \in \mathbb{N}\}$ ist definierbar in der S_{Ar}-Struktur $\mathcal{N}$ durch die Formel*

$$\exists v_1.\, v_0 \equiv v_1 * v_1$$

(b) $R = \{(m, n) \in \mathbb{N}^2 \mid m \leq n\}$ ist definierbar in der S_{Ar}-Struktur $\mathcal{N}$ durch

$$\exists v_2.\, v_0 + v_2 \equiv v_1$$

(c) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto n^2$ ist definiert durch $v_1 \equiv v_0 * v_0$

(d) $div : \mathbb{N}^2 \rightharpoonup \mathbb{N}$ mit

$$div(m, n) = \begin{cases} \text{der ganzzahlige Quotient von } m \text{ durch } n, & \text{falls } n \neq 0 \\ \text{undefiniert}, & \text{sonst} \end{cases}$$

*Es gilt (*Zahlentheorie*): Wenn $n \neq 0$, dann existieren eindeutige Zahlen $q, r \in \mathbb{N}$ mit $r < n$ und $m = q \cdot n + r$. Also ist div definierbar in der S_{Ar}-Struktur $\mathcal{N}$ durch*

$$\exists v_3.\, v_3 < v_1 \wedge v_0 \equiv v_2 * v_1 + v_3$$

q bezeichnet den ganzzahligen Quotienten und r den Rest der ganzzahligen Division $\frac{m}{n}$.

(e) Sei $exp : \mathbb{N}^2 \longrightarrow \mathbb{N}$, $(m, n) \mapsto m^n$. Frage: ist exp definierbar? Versuch: $\exists a_0, \ldots, a_n.\, a_0 = 1$ und für alle $i \in \{0, \ldots, n-1\}$ gilt: $a_{i+1} = m \cdot a_i$ und das Ergebnis ist a_n.

Beispiel (e) läßt sich so nicht in der Prädikatenlogik erster Stufe formulieren, da die Anzahl der $\exists$-quantifizierten Variablen vom Argument n abhängen müßte. Wir werden später sehen: exp ist definierbar in $\mathcal{N}$. Es gilt sogar der folgende

Satz 2.2.1. *Alle* rekursiv aufzählbaren *Relationen* $R \subseteq \mathbb{N}^n$ *und alle* (partiellen) berechenbaren *Funktionen* $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$ *sind definierbar in der* S_{Ar}*-Struktur* $\mathcal{N}$ *(„in der Arithmetik“) (und darüber hinaus noch „viele“ andere Relationen:* Arithmetische Hierarchie*)*

Bemerkung 2.2.3. *Dabei ist die Multiplikation wichtig. Sie erlaubt eine Kodierung von Zahlenfolgen als Zahlenpaare* $\rightsquigarrow$ *Man kann das Ein- und Ausgabeverhalten eines* `WHILE`*-Programms durch eine Formel beschreiben* $\rightsquigarrow$ *Alle Mengen und Funktionen, die durch* `WHILE`*-Programme „definiert“ werden können, sind auch durch Formeln definierbar.*

Bisher:
Beispiele von Formeln, die für manche Belegungen wahr sind

Jetzt:
Formeln, die „immer wahr“ sind, d.h. unabhängig von der Belegung oder sogar unabhängig von der Struktur und der Belegung

Definition 2.2.6 (Gültigkeit). *Sei* S *eine Signatur und* $\varphi \in L^S$*.*

(a) φ *heißt* gültig in der S-Struktur $\mathcal{A} = (A, \alpha)$*, wenn* $\mathcal{A}, \beta \models \varphi$ *für alle* $\beta : X \longrightarrow A$*. Man schreibt dann:* $\mathcal{A} \models \varphi$ *oder* $\models_{\mathcal{A}} \varphi$ *und sagt auch wieder:* $\mathcal{A}$ *ist* Modell *von/für* φ*.*

(b) φ *heißt* allgemeingültig*, wenn* $\mathcal{I} \models \varphi$ *für alle* S*-Interpretationen* $\mathcal{I}$ *(d.h.* $\mathcal{A} \models \varphi$ *für alle* S*-Strukturen* $\mathcal{A}$*). Schreibweise:* $\models \varphi$

(c) φ *heißt* erfüllbar*, wenn eine* S*-Interpretation* $\mathcal{I}$ *existiert mit* $\mathcal{I} \models \varphi$*.*

(d) φ *heißt* erfüllbar *in der* S*-Struktur* $\mathcal{A}$*, wenn es eine zugehörige Belegung* β *gibt mit* $(\mathcal{A}, \beta) \models \varphi$

Beispiel 2.2.5. *(a) Für die* $S^{<}_{\mathrm{Ar}}$*-Struktur* $\mathcal{N} = (\mathbb{N}, \ldots)$ *gilt z.B.:*

$$\mathcal{N} \models \forall x, y.\, \neg y \equiv 0 \rightarrow \exists q, r.\, x \equiv q * y + r \wedge r < y$$

Denn: diese Formel drückt aus, daß wir in $\mathbb{N}$ *die Division mit Rest durchführen können.*

(b) Sei $S_{\ddot{A}q} = \{\sim\}$*,* $\sim$ *zweistelliges Relationszeichen. Sei* $\varphi_{\ddot{A}q}$ *die Formel:*

$$(\forall x.\, x \sim x) \wedge (\forall x, y.\, x \sim y \rightarrow y \sim x) \wedge (\forall x, y, z.\, x \sim y \wedge y \sim z \rightarrow x \sim z)$$

und sei $\mathcal{A} = (A, \alpha)$ *eine* $S_{\ddot{A}q}$*-Struktur. Dann gilt:*

$$\begin{aligned} \mathcal{A} \models \varphi_{\ddot{A}q} \quad &\Leftrightarrow \quad \sim^{\mathcal{A}} \textit{ ist } \text{reflexiv, symmetrisch } \textit{und } \text{transitiv} \\ &\Leftrightarrow \quad \sim^{\mathcal{A}} \textit{ ist eine } \text{Äquivalenzrelation } \textit{auf der Trägermenge } A. \end{aligned}$$

Also: Die Modelle von φ sind genau die Strukturen $(A, \sim^{\mathcal{A}})$, wobei $\sim^{\mathcal{A}}$ Äquivalenzrelation auf A ist. Ähnlich kann man (mit jeweils passender Signatur S) eine Formel $\varphi \in L^S$ angeben, deren Modelle

- *genau die* partiellen Ordnungen[1] *sind ($S_{PO} = \{\leq\}$)*
- *genau die* Gruppen *sind ($S_{Gr} = \{e, \star\}$)*
- *genau die* Ringe *sind ($S_{Rg} = S_{\mathrm{Ar}} = \{0, 1, +, *\}$)*
- *genau die* Körper *sind ($S_{Kp} = S_{\mathrm{Ar}} = \{0, 1, +, *\}$)*

(c) Sei S eine beliebige Signatur, $n \geq 1$. Sei $\varphi_{>n}$ die Formel:

$$\exists v_0, \ldots, v_n. \bigwedge_{i=0}^{n-1} \bigwedge_{j=i+1}^{n} \neg v_i \equiv v_j$$

Dann gilt für jede Struktur $\mathcal{A} = (A, \alpha)$:

$$\begin{aligned} \mathcal{A} \models \varphi_{>n} \quad &\Leftrightarrow \quad \text{es ex. } a_0, \ldots, a_n \in A, a_i \neq a_j \text{ f.a. } i, j \in \{0, \ldots, n\} \text{ mit } i < j \\ &\Leftrightarrow \quad \text{es ex. paarweise verschiedene Elemente } a_0, \ldots, a_n \in A \\ &\Leftrightarrow \quad |A| > n \end{aligned}$$

Ähnlich konstruiert man für jedes $n \geq 1$ eine Formel $\varphi_{\leq n}$, deren Modelle genau die Strukturen $\mathcal{A} = (A, \alpha)$ sind mit $|A| \leq n$ oder eine Formel $\varphi_{=n}$, deren Modelle genau die Strukturen mit n Elementen sind.

(d) Gibt es eine Formel

- *$\varphi_{<\infty}$, die genau die Strukturen mit endlicher Trägermenge als Modelle hat?*
- *φ_{∞}, die genau die Strukturen mit unendlicher Trägermenge als Modell hat?*

Wir sehen später: diese Formeln gibt es nicht!
Allgemeine Fragestellung: welche Eigenschaften von Strukturen lassen sich durch Formeln der Prädikatenlogik erster Stufe ausdrücken?

(e) Beispiele für allgemeingültige Formeln:

- $\varphi \vee \neg\varphi$
- $\varphi \to \varphi$
- $(\varphi_1 \vee \varphi_2 \to \psi) \leftrightarrow ((\varphi_1 \to \psi) \wedge (\varphi_2 \to \psi))$
- $((\exists x. \varphi) \to \psi) \leftrightarrow (\forall x. \varphi \to \psi)$, *falls* $x \notin$ *frei*(ψ)

Manche Begriffe werden von einzelnen Formeln auf *Formelmengen* verallgemeinert. Dies führt zur folgenden

[1] Halbordnungen

Definition 2.2.7 (Modell). *Sei S eine Signatur, $\Phi \subseteq L^S$.*

(a) Eine S-Interpretation $\mathcal{I}$ heißt Modell *von/für Φ (oder: $\mathcal{I}$* erfüllt *Φ), wenn $\mathcal{I} \models \varphi$ für alle $\varphi \in \Phi$. Schreibweise: $\mathcal{I} \models \Phi$*

(b) Eine S-Struktur $\mathcal{A}$ heißt Modell *von Φ, wenn $\mathcal{A} \models \varphi$ für alle $\varphi \in \Phi$. Schreibweise: $\mathcal{A} \models \Phi$*

(c) Φ heißt erfüllbar*, wenn es eine Interpretation $\mathcal{I}$ gibt mit $\mathcal{I} \models \Phi$.*

Beispiel 2.2.6. *Hier zunächst einige* pathologische *Fälle*

(a) Die Modelle von $\Phi = \emptyset$ sind alle *Interpretationen bzw. Strukturen.*

(b) Sei $\Phi = \{\varphi\}$. Dann gilt:

$$\begin{aligned} \mathcal{I} \models \{\varphi\} &\Leftrightarrow \mathcal{I} \models \varphi \text{ bzw.} \\ \mathcal{A} \models \{\varphi\} &\Leftrightarrow \mathcal{A} \models \varphi \end{aligned}$$

(c) Sei $\Phi = \{\varphi_1, \ldots, \varphi_n\}$. Dann gilt

$$\begin{aligned} \mathcal{I} \models \{\varphi_1, \ldots, \varphi_n\} &\Leftrightarrow \mathcal{I} \models \varphi_i \text{ für } i = 1, \ldots, n \\ &\Leftrightarrow \mathcal{I} \models \varphi_1 \wedge \ldots \wedge \varphi_n \end{aligned}$$

(d) $\Phi = L^S$. Dann gilt: Φ hat keine *Modelle, denn Φ enthält z.B. $\neg x \equiv x$ und diese Formel ist für* keine *Interpretation erfüllt.*

(e) Sei $\Phi = \{\varphi_{>n} \mid n \geq 1\}$. Dann gilt für jede Struktur $\mathcal{A} = (A, \alpha)$:

$$\begin{aligned} \mathcal{A} \models \Phi &\Leftrightarrow \mathcal{A} \models \varphi_{>n} \text{ für alle } n \geq 1 \\ &\Leftrightarrow |A| > n \text{ für alle } n \geq 1 \\ &\Leftrightarrow |A| \text{ ist unendlich.} \end{aligned}$$

Also haben wir eine Formelmenge Φ gefunden, deren Modelle genau die unendlichen Strukturen *sind. Wir werden später noch sehen, daß es* keine *Formelmenge Φ gibt, deren Modelle genau die* endlichen Strukturen *sind. Eine allgemeine Frage ist: welche Klassen von Strukturen lassen sich durch Mengen Φ von Formeln erster Stufe charakterisieren?*

Bemerkung 2.2.4. *In Beispiel (e) funktioniert dies nur für Strukturen $\mathcal{A}$ mit abgeschlossenen Formeln, z.B.: Sei*

$$\Phi = \{\forall x.\, x \sim x, \forall x, y.\, x \sim y \to y \sim x, \forall x, y, z.\, x \sim y \wedge y \sim z \to x \sim z\}$$

Dann gilt wieder $\mathcal{A} \models \Phi \Leftrightarrow \sim^{\mathcal{A}}$ ist eine Äquivalenzrelation.

Lemma 2.2.1. *Sei S eine Signatur, $\mathcal{A}$ eine Struktur und $\varphi \in L^S$, $x \in X$. Dann gilt:*

(a) $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{A} \models \forall x.\, \varphi$

(b) $\models \varphi \Leftrightarrow \models \forall x.\, \varphi$

Beweis.

(a) Sei $\mathcal{A} = (A, \alpha)$

„$\Rightarrow$“*: Dann gilt:*

$$\begin{aligned} \mathcal{A} \models \varphi &\Rightarrow \mathcal{A}, \beta \models \varphi \text{ für alle } \beta : X \longrightarrow A \\ &\Rightarrow \mathcal{A}, \beta[a/x] \models \varphi \text{ für alle } \beta : X \longrightarrow A \text{ und alle } a \in A \\ &\Rightarrow \mathcal{A}, \beta \models \forall x.\, \varphi \text{ für alle } \beta : X \longrightarrow A \\ &\Rightarrow \mathcal{A} \models \forall x.\, \varphi \end{aligned}$$

„$\Leftarrow$“*: Für jedes* $\beta : X \longrightarrow A$ *gilt:*

$$\begin{aligned} \mathcal{A}, \beta \models \forall x.\, \varphi &\Rightarrow \mathcal{A}, \beta[a/x] \models \varphi \text{ für alle } a \in A \\ &\overset{a=\beta(x)}{\Rightarrow} \mathcal{A}, \beta \models \varphi \end{aligned}$$

Also folgt $\mathcal{A} \models \forall x.\, \varphi \Rightarrow \mathcal{A} \models \varphi$

(b) folgt sofort aus (a)

□

Lemma 2.2.2 (Koinzidenzlemma). *Sei* S *eine Signatur,* $\mathcal{A} = (A, \alpha)$ *eine* S*-Struktur und* $\beta_1, \beta_2 : X \longrightarrow A$*.*

(a) Wenn β_1 *und* β_2 *auf* $var(t)$ *übereinstimmen, dann gilt:* $(\mathcal{A}, \beta_1)(t) = (\mathcal{A}, \beta_2)(t)$

(b) Wenn β_1 *und* β_2 *auf* $frei(\varphi)$ *übereinstimmen, dann gilt:* $(\mathcal{A}, \beta_1)(\varphi) = (\mathcal{A}, \beta_2)(\varphi)$

Beweis. *Induktion über die Größe von* t *bzw. von* φ*: Einzig interessante Induktionsschritt: Quantoren. Sei also* φ *von der Form* $\forall x.\, \psi$*. Wenn* β_1*,* β_2 *auf* $frei(\varphi)$ *übereinstimmen, dann stimmen* $\beta_1[a/x]$ *und* $\beta_2[a/x]$ *auf* $frei(\varphi) \cup \{x\}$ *überein, also auf* $frei(\psi) \subseteq frei(\varphi) \cup \{x\}$*. Also gilt:*

$$\begin{aligned} \mathcal{A}, \beta_1 \models \forall x.\, \psi &\Leftrightarrow \mathcal{A}, \beta_1[a/x] \models \psi \text{ für alle } a \in A \\ &\overset{I.A.}{\Leftrightarrow} \mathcal{A}, \beta_2[a/x] \models \psi \text{ für alle } a \in A \\ &\Leftrightarrow \mathcal{A}, \beta_2 \models \forall x.\, \psi \end{aligned}$$

Analog zeigt man dies für den Existenzquantor $\exists$*.* □

2.3 Logische Folgerung und logische Äquivalenz

Frage: Was bedeutet „φ *folgt aus* Φ“? ($\varphi \in L^S$, $\Phi \subseteq L^S$)

Intuition: „*Immer wenn alle Formeln aus* Φ *gelten, gilt auch* φ*.*“

Definition 2.3.1 (Logische Folgerung). *Sei S Signatur, $\Phi \subseteq L^S$, $\varphi \in L^S$. Dann heißt φ* (logische) Folgerung *von Φ (oder: φ* folgt *aus Φ), wenn für jede Interpretation $\mathcal{I}$ mit $\mathcal{I} \models \Phi$ auch $\mathcal{I} \models \varphi$ gilt. Schreibweise: $\Phi \models \varphi$, statt $\{\psi\} \models \varphi$ schreibt man $\psi \models \varphi$.*

Bemerkung 2.3.1. *Vorsicht: in manchen Büchern findet man: ...,* wenn für jede Struktur $\mathcal{A}$ mit $\mathcal{A} \models \Phi$ auch $\mathcal{A} \models \varphi$ gilt. *Die beiden Definitionen sind nicht äquivalent, falls freie Variablen vorkommen.*

Beispiel 2.3.1. *Zunächst wieder zwei pathologische Beispiele*

(a) $\Phi = \emptyset$*: Es gilt:*

$$\begin{aligned} \emptyset \models \varphi \quad &\Leftrightarrow \quad \text{für jedes } \mathcal{I} \text{ mit } \mathcal{I} \models \emptyset \text{ gilt } \mathcal{I} \models \varphi \\ &\Leftrightarrow \quad \text{für jedes } \mathcal{I} \text{ gilt } \mathcal{I} \models \varphi \\ &\Leftrightarrow \quad \models \varphi \end{aligned}$$

Also: die logischen Folgerungen von $\emptyset$ sind nur die allgemeingültigen Formeln.

(b) Φ *nicht erfüllbar:*

$$\Phi \models \varphi \quad \Leftrightarrow \quad \underbrace{\text{für alle } \underbrace{\mathcal{I} \text{ mit } \mathcal{I} \models \Phi}_{\text{solche } \mathcal{I} \text{ gibt es nicht}} \text{ gilt } \mathcal{I} \models \varphi}_{\text{gilt immer}}$$

$$\Leftrightarrow \quad \varphi \in L^S$$

„Ex falsum quod libet[2]“

(c) Sei $\Phi = \{\mathit{refl}, \mathit{symm}, \mathit{trans}\}$*, wobei*

- $\mathit{refl} = \forall x.\, x \sim x$ *(hier: „=“ bedeutet syntaktische Gleichheit),*
- $\mathit{symm} = \forall x, y.\, x \sim y \to y \sim x$*,*
- $\mathit{trans} = \forall x, y, z.\, x \sim y \wedge y \sim z \to x \sim z$

Dann gilt:

$$\Phi \models \varphi \quad \Leftrightarrow \quad \varphi \text{ ist für alle Äquivalenzrelationen erfüllt}$$

Z.B.: $\varphi = \forall x, y.\, (\exists z.\, x \sim z \wedge y \sim z) \to (\forall z.\, x \sim z \leftrightarrow y \sim z))$

Ähnlich: Φ = Menge der Gruppenaxiome. Dann gilt:

$$\Phi \models \varphi \quad \Leftrightarrow \quad \varphi \text{ ist eine Formel, die in allen Gruppen gilt}$$

(d) Sei $\Phi = \{\mathit{refl}, \mathit{trans}, \mathit{symm}, x \sim y, x \sim z\}$*. Dann gilt:* $\Phi \models y \sim z$

[2] Aus dem Lateinischen: *„Aus Falschem kann alles geschlossen werden“*

(e) Gegenbeispiel: $\{trans, symm\} \not\models refl$.

Zu zeigen: es ex. ein $\mathcal{I}$ *mit* $\mathcal{I} \models \{trans, symm\}$, *aber* $\mathcal{I} \not\models refl$
Man wähle $\mathcal{A} = (A, \sim^{\mathcal{A}})$ *mit* A *beliebig und* $\sim^{\mathcal{A}} = \emptyset$. *Die* leere Relation *ist transitiv und symmetrisch, aber nicht reflexiv.*

Ähnlich: $\{refl, trans\} \not\models symm$ *bzw.* $\{refl, symm\} \not\models trans$.
Beweis: Übung

Lemma 2.3.1. *Sei* S *eine Signatur,* $\varphi_1, \ldots, \varphi_n \in L^S$. *Dann gilt:*

$$\{\varphi_1, \ldots, \varphi_n\} \models \varphi \Leftrightarrow \models \varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \varphi$$

Beweis. *Klar!* □

Lemma 2.3.2. *Sei* S *eine Signatur,* $\Phi \subseteq L^S$, $\varphi \in L^S$. *Dann gilt:* $\Phi \models \varphi \Leftrightarrow \Phi \cup \{\neg\varphi\}$ *nicht erfüllbar (insbesondere:* $\models \varphi \Leftrightarrow \neg\varphi$ *nicht erfüllbar)*

Beweis.

$$\begin{aligned}
\Phi \models \varphi \quad &\Leftrightarrow \quad \text{für alle } \mathcal{I} \text{ mit } \mathcal{I} \models \Phi \text{ gilt } \mathcal{I} \models \varphi \\
&\Leftrightarrow \quad \text{es ex. keine Interpretation } \mathcal{I} \text{ mit } \mathcal{I} \models \Phi \text{ und } \mathcal{I} \not\models \varphi \\
&\Leftrightarrow \quad \text{es ex. keine Interpretation } \mathcal{I} \text{ mit } \mathcal{I} \models \Phi \text{ und } \mathcal{I} \models \neg\varphi \\
&\Leftrightarrow \quad \Phi \cup \{\neg\varphi\} \text{ nicht erfüllbar}
\end{aligned}$$

□

Bemerkung 2.3.2. *Statt* nicht erfüllbar *sagt man* unerfüllbar.

Definition 2.3.2 (Logische Äquivalenz). *Seien* $\varphi, \psi \in L^S$. φ *und* ψ *heißen* (logisch) äquivalent, *wenn* $\varphi \models \psi$ *und* $\psi \models \varphi$. *Schreibweise:* $\varphi \doteq \psi$

Lemma 2.3.3. *Es gilt stets:* $\varphi \doteq \psi \Leftrightarrow \models \varphi \leftrightarrow \psi$ $(\Leftrightarrow \mathcal{I}(\varphi) = \mathcal{I}(\psi)$ *für alle* $\mathcal{I})$

Beweis. *Klar!* □

Lemma 2.3.4. *Für alle* $\varphi, \psi \in L^S$ *gilt:*

(a) $\varphi \wedge \psi \doteq \neg(\neg\varphi \vee \neg\psi)$

(b) $\varphi \rightarrow \psi \doteq \neg\varphi \vee \psi$

(c) $\varphi \leftrightarrow \psi \doteq (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$

(d) $\forall x.\, \varphi \doteq \neg\exists x.\, \neg\varphi$

Beweis. *Nachrechnen!*

□

Korollar 2.3.1. *Zu jeder Formel* $\varphi \in L^S$ *läßt sich eine Formel* $\varphi^* \in L^S$ *konstruieren mit* $\varphi \doteq \varphi^*$, *die nur noch die logischen Zeichen* $\neg$, $\vee$, $\exists$ *und* $\equiv$ *enthält* $\rightsquigarrow$ *In theoretischen Betrachtungen können wir annehmen, daß die Formeln nur mit den logischen Zeichen* $\neg$, $\vee$, $\exists$ *und* $\equiv$ *aufgebaut sind (insbesondere im Kalkül).*

2.4 Homomorphismen, Isomorphismen, Unterstrukturen

Idee: Ein *Homomorphismus* ist eine Abbildung zwischen zwei Strukturen (über der gleichen Signatur), die mit den Funktions- und Relationszeichen „verträglich“ ist.

Definition 2.4.1 (Homomorphismus). *Sei S eine Signatur, $\mathcal{A}_1 = (A_1, \alpha_1)$, $\mathcal{A}_2 = (A_2, \alpha_2)$ zwei S-Strukturen und $\pi : A_1 \longrightarrow A_2$*

(a) π heißt (schwacher) Homomorphismus *von $\mathcal{A}_1$ nach $\mathcal{A}_2$, wenn*

(1) $\pi(c^{\mathcal{A}_1}) = c^{\mathcal{A}_2}$ für alle $c \in C$

(2) $\pi(f^{\mathcal{A}_1}(a_1, \ldots, a_n)) = f^{\mathcal{A}_2}(\pi(a_1), \ldots, \pi(a_n))$ für alle $f \in F_n$ und $a_1, \ldots, a_n \in A_1$

(3) Wenn $(a_1, \ldots, a_n) \in r^{\mathcal{A}_1}$, dann ist $(\pi(a_1), \ldots, \pi(a_n)) \in r^{\mathcal{A}_2}$ für alle $r \in R_n$ und $a_1, \ldots, a_n \in A_1$

(b) π heißt starker Homomorphismus*, falls $(a_1, \ldots, a_n) \in r^{\mathcal{A}_1}$ genau dann, wenn $(\pi(a_1), \ldots, \pi(a_n)) \in r^{\mathcal{A}_2}$ für alle $r \in R_n$ und $a_1, \ldots, a_n \in A_1$*

(c) Ein starker Homomorphismus, der bijektiv ist, heißt Isomorphismus *Zwei Strukturen $\mathcal{A}_1$ und $\mathcal{A}_2$ heißen* isomorph*, wenn ein Isomorphismus zwischen ihnen existiert.*

Bemerkung 2.4.1. *Ein Homomorphismus ist also strukturerhaltend. Die Umkehrabbildung eines Isomorphismus ist natürlich wieder ein Isomorphismus, wie man sich leicht überlegt. Bei isomorphen Strukturen hat man die Intuition, daß diese im „wesentlichen gleich“ sind.*

Lemma 2.4.1 (Isomorphie-Lemma). *Seien $\mathcal{A}_1 = (A_1, \alpha_1)$ und $\mathcal{A}_2 = (A_2, \alpha_2)$ zwei isomorphe S-Strukturen. Dann gilt für alle abgeschlossenen Formeln $\varphi \in L^S$:*

$$\mathcal{A}_1 \models \varphi \Leftrightarrow \mathcal{A}_2 \models \varphi$$

Beweis. *Sei $\pi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ ein Homomorphismus und $\mathcal{I} = (\mathcal{A}_1, \beta)$ eine Interpretation für $\mathcal{A}_1$. Dann ist $\mathcal{I}^\pi =_{\text{def}} (\mathcal{A}_2, \pi \circ \beta)$ eine Interpretation für $\mathcal{A}_2$ (denn wg. $\beta : X \longrightarrow A_1$ gilt $\pi \circ \beta : X \longrightarrow A_2$). Wir zeigen: wenn π ein Isomorphismus ist, dann gilt:*

(a) $\pi(\mathcal{I}(t)) = \mathcal{I}^\pi(t)$ für alle $t \in T^S$

(b) $\mathcal{I}(\varphi) = \mathcal{I}^\pi(\varphi)$ für alle $\varphi \in L^S$

(a) Beweis durch Induktion über die Größe von t bzw. φ:
$\underline{t = x}$:

$$\begin{aligned} \pi(\mathcal{I}(x)) &= \pi(\beta(x)) \\ &= (\pi \circ \beta)(x) \\ &= \mathcal{I}^\pi(x) \end{aligned}$$

$\underline{t = c:}$

$$\begin{aligned} \pi(\mathcal{I}(c)) &= \pi(c^{\mathcal{A}_1}) \\ &= c^{\mathcal{A}_2} \\ &= \mathcal{I}^\pi(c) \end{aligned}$$

$\underline{t = f(t_1, \ldots, t_n):}$

$$\begin{aligned} \pi(\mathcal{I}(f(t_1, \ldots, t_n))) &= \pi(f^{\mathcal{A}_1}(\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n))) \\ &= f^{\mathcal{A}_2}(\pi(\mathcal{I}(t_1)), \ldots, \pi(\mathcal{I}(t_n))) \text{ (da } \pi \text{ Hom.)} \\ &\overset{I.A.}{=} f^{\mathcal{A}_2}(\mathcal{I}^\pi(t_1), \ldots, \mathcal{I}^\pi(t_n)) \\ &= \mathcal{I}^\pi(f(t_1, \ldots, t_n)) \end{aligned}$$

(b) Induktion über die Größe von φ:

$\underline{\varphi = t_1 \equiv t_2:}$

$$\begin{aligned} \mathcal{I}(\varphi) = \mathit{true} &\Leftrightarrow \mathcal{I}(t_1) = \mathcal{I}(t_2) \\ &\Leftrightarrow \pi(\mathcal{I}(t_1)) = \pi(\mathcal{I}(t_2)) \text{ („}\Leftarrow\text{“ weil } \pi \text{ injektiv)} \\ &\overset{(a)}{\Leftrightarrow} \mathcal{I}^\pi(t_1) = \mathcal{I}^\pi(t_2) \\ &\Leftrightarrow \mathcal{I}^\pi(\varphi) = \mathit{true} \end{aligned}$$

$\underline{\varphi = r(t_1, \ldots, t_n):}$

$$\begin{aligned} \mathcal{I}(\varphi) = \mathit{true} &\Leftrightarrow (\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n)) \in r^{\mathcal{A}_1} \\ &\Leftrightarrow (\pi(\mathcal{I}(t_1)), \ldots, \pi(\mathcal{I}(t_n))) \in r^{\mathcal{A}_2} \text{ (da } \pi \text{ starker Hom.)} \\ &\overset{(a)}{\Leftrightarrow} (\mathcal{I}^\pi(t_1), \ldots, \mathcal{I}^\pi(t_n)) \in r^{\mathcal{A}_2} \\ &\Leftrightarrow \mathcal{I}^\pi(\varphi) = \mathit{true} \end{aligned}$$

$\underline{\varphi = \neg\psi:}$

$$\begin{aligned} \mathcal{I}(\varphi) = \mathit{true} &\Leftrightarrow \mathcal{I}(\psi) = \mathit{false} \\ &\overset{\text{I.A}}{\Leftrightarrow} \mathcal{I}^\pi(\psi) = \mathit{false} \\ &\Leftrightarrow \mathcal{I}^\pi(\varphi) = \mathit{true} \end{aligned}$$

$\underline{\varphi = \varphi_1 \vee \varphi_2:}$

$$\begin{aligned} \mathcal{I}(\varphi) = \mathit{true} &\Leftrightarrow \mathcal{I}(\varphi_1) = \mathit{true} \text{ oder } \mathcal{I}(\varphi_2) = \mathit{true} \\ &\overset{\text{I.A}}{\Leftrightarrow} \mathcal{I}^\pi(\varphi_1) = \mathit{true} \text{ oder } \mathcal{I}^\pi(\varphi_2) = \mathit{true} \\ &\Leftrightarrow \mathcal{I}^\pi(\varphi) = \mathit{true} \end{aligned}$$

$\underline{\varphi = \exists x.\, \psi:}$

$$\begin{aligned} \mathcal{I}(\varphi) = \mathit{true} &\Leftrightarrow \text{es ex. ein } a \in A_1 \text{ mit } \mathcal{I}[a/x](\psi) = \mathit{true} \\ &\overset{\text{I.A}}{\Leftrightarrow} \text{es ex. ein } a \in A_1 \text{ mit } \underbrace{(\mathcal{I}[a/x])^\pi(\psi)}_{=(\mathcal{A}_1, \beta[a/x])^\pi)} = \mathit{true} \end{aligned}$$

Und $(\mathcal{A}_1, \beta[a/x])^\pi) = (\mathcal{A}_2, \pi \circ (\beta[a/x]))$. *Nochmal ordentlicher: Für* $\mathcal{I} = (\mathcal{A}_1, \beta)$ *gilt:*

$$\begin{aligned} \mathcal{I}[a/x] = (\mathcal{A}_1, \beta[a/x]),\ \textit{also} & \\ (\mathcal{I}[a/x])^\pi &= (\mathcal{A}_2, \pi \circ (\beta[a/x])) \\ &= (\mathcal{A}_2, (\pi \circ \beta)[\pi(a)/x]) \\ &= \mathcal{I}^\pi[\pi(a)/x] \end{aligned}$$

Also:

$$\begin{aligned} \mathcal{I}(\varphi) = \textit{true} &\Leftrightarrow \textit{ es ex. ein } a \in A_1 \textit{ mit } \mathcal{I}^\pi[\pi(a)/x](\psi) = \textit{true} \\ &\overset{(*)}{\Leftrightarrow} \textit{ es ex. ein } b \in A_2 \textit{ mit } \mathcal{I}^\pi[b/x](\psi) = \textit{true} \\ &\Leftrightarrow \mathcal{I}^\pi(\underbrace{\exists x.\, \psi}_{=\varphi}) = \textit{true} \end{aligned}$$

(*): „⇒“ ist klar, „⇐“ da π *surjektiv, läßt sich jedes* $b \in A_2$ *in der Form* $\pi(a)$ *darstellen. Damit ist (b) bewiesen. Aus (b) folgt die Behauptung des Lemmas:*

$$\begin{aligned} \mathcal{A}_1 \models \varphi &\Leftrightarrow \textit{ für alle } \beta : X \longrightarrow A_1 \textit{ gilt: } (A_1, \beta)(\varphi) = \textit{true} \\ &\overset{(b)}{\Leftrightarrow} \textit{ für alle } \beta : X \longrightarrow A_1 \textit{ gilt: } (\mathcal{A}_2, \pi \circ \beta)(\varphi) = \textit{true} \\ &\overset{(**)}{\Leftrightarrow} \textit{ für alle } \beta' : X \longrightarrow A_2 \textit{ gilt: } (\mathcal{A}_2, \beta')(\varphi) = \textit{true} \\ &\Leftrightarrow \mathcal{A}_2 \models \varphi \end{aligned}$$

(**): „⇐“ ist klar. „⇒“: da π *surjektiv ist, hat jede Belegung* $\beta' : X \longrightarrow A_2$ *die Form* $\pi \circ \beta$.

□

Bemerkung 2.4.2. *Teil (a) des Lemmas gilt bereits für (schwache) Homomorphismen. Abschwächungen von Teil (b) gelten für schwache bzw. starke Homomorphismen.*

Ausblick:
Das Isomorphie-Lemma (S.17) besagt, daß in isomorphen S-Strukturen die gleichen Formeln $\varphi \in L^S$ gelten.

Frage:
„Gilt auch die Umkehrung? D.h. sind zwei S-Strukturen, in denen die gleichen Formeln $\varphi \in L^S$ gelten, stets isomorph?“. Anders ausgedrückt: „Ist eine S-Struktur durch die in ihr geltenden Formeln $\varphi \in L^S$ bis auf Isomorphie eindeutig charakterisiert?“.

Wir werden sehen, daß dies im Allgemeinen nicht gilt, z.B. gibt es zur S_{Ar}-Struktur $\mathcal{N} = (\mathbb{N}, \ldots)$ eine S_{Ar}-Struktur $\mathcal{N}^* = (\mathbb{N}^*, \ldots)$, in der die gleichen

Formeln $\varphi \in L^{S_{\mathrm{Ar}}}$ gelten, die aber nicht zu $\mathcal{N}$ isomorph ist. Das liegt daran, daß wir nur Formeln erster Stufe betrachten, d.h. daß wir das Induktionsprinzip nicht formulieren können. Mit dem Induktionsprinzip läßt sich $\mathcal{N}$ nämlich eindeutig bis auf Isomorphie charakterisieren. In $\mathcal{N}^*$ gilt das Induktionsprinzip nicht, weil $\mathcal{N}^*$ „unendlich große“ Elemente enthält. $\mathcal{N}^*$ bezeichnet man als *Nichtstandard-Modell der Arithmetik*.

Ähnlich: Zum S_{Ar}-Modell $\mathcal{R} = (\mathbb{R}, \ldots)$ der reellen Zahlen. $\mathcal{R}^* = (\mathbb{R}^*, \ldots)$ mit „unendlich großen“ und „unendlich kleinen“ Zahlen ($\rightsquigarrow$ *Nichtstandard-Analysis*).

Definition 2.4.2. *Sei S eine Signatur, seien $\mathcal{A}_1 = (A_1, \alpha_1)$ und $\mathcal{A}_2 = (A_2, \alpha_2)$ zwei S-Strukturen. $\mathcal{A}_1$ heißt* Unterstruktur *(oder:* Substruktur*) von $\mathcal{A}_2$ (Schreibweise: $\mathcal{A}_1 \subseteq \mathcal{A}_2$), wenn gilt:*

(a) $A_1 \subseteq A_2$

(b) $c^{\mathcal{A}_1} = c^{\mathcal{A}_2}$ *für jedes* $c \in C$

$f^{\mathcal{A}_1}$ *ist die Einschränkung von* $f^{\mathcal{A}_2}$ *auf* A_1^n *für jedes* $f \in F_n$

$r^{\mathcal{A}_1}$ *ist die Einschränkung von* $r^{\mathcal{A}_2}$ *auf* A_1^n *(d.h.* $r^{\mathcal{A}_1} = r^{\mathcal{A}_2} \cap A_1^n$*) für jedes* $r \in R_n$

Beispiel 2.4.1. *Seien $\mathcal{N} = (\mathbb{N}, \ldots)$, $\mathcal{Z} = (\mathbb{Z}, \ldots)$, $\mathcal{Q} = (\mathbb{Q}, \ldots)$ und $\mathcal{R} = (\mathbb{R}, \ldots)$ die üblichen S_{Ar}- (oder $S_{\mathrm{Ar}}^{<}$-)Strukturen. Dann gilt die Hierarchie:*

$$\mathcal{N} \subseteq \mathcal{Z} \subseteq \mathcal{Q} \subseteq \mathcal{R}$$

(weil z.B. $+^{\mathcal{N}}$, $*^{\mathcal{N}}$ und $<^{\mathcal{N}}$ die Einschränkungen von $+^{\mathcal{Z}}$, $*^{\mathcal{Z}}$ und $<^{\mathcal{Z}}$ sind).

Bemerkung 2.4.3. *Eine Formel, die in $\mathcal{A}_2$ gilt, muß nicht in jeder Unterstruktur $\mathcal{A}_1$ gelten, z.B.: $\forall x, y.\, \neg y \equiv 0 \rightarrow \exists z.\, y * z \equiv x$ (Existenz des Quotienten) ist gültig in $\mathcal{Q}$ und $\mathcal{R}$, aber nicht in $\mathcal{N}$ oder $\mathcal{Z}$. Umgekehrt genauso: die Negation dieser Formel ist gültig in $\mathcal{N}$ und $\mathcal{Z}$, aber nicht in $\mathcal{Q}$ oder $\mathcal{R}$. $\rightsquigarrow$ Idee: Existenzquantor verbieten $\rightsquigarrow$ Problem: $\exists P(\ldots)$ läßt sich durch $\neg\forall\neg P(\ldots)$ ausdrücken $\rightsquigarrow$ Beide Quantoren $\exists$, $\forall$ verbieten!*

Lemma 2.4.2. *Seien $\mathcal{A}_1 = (A_1, \alpha_1)$ und $\mathcal{A}_2 = (A_2, \alpha_2)$ zwei S-Strukturen mit $\mathcal{A}_1 \subseteq \mathcal{A}_2$, und sei $\beta : X \longrightarrow A_1$ (d.h. β ist eine Belegung, die zu beiden Strukturen paßt). Dann gilt:*

(a) $(\mathcal{A}_1, \beta)(t) = (\mathcal{A}_2, \beta)(t)$ *für alle* $t \in T^S$

(b) $(\mathcal{A}_1, \beta)(\varphi) = (\mathcal{A}_2, \beta)(\varphi)$ *für alle quantorenfreien* $\varphi \in L^S$.

(c) Wenn $\mathcal{A}_2 \models \varphi$, dann $\mathcal{A}_1 \models \varphi$ für alle quantorfreien $\varphi \in L^S$ (Die Umkehrung gilt im allgemeinen nicht!).

Beweis. *Analog zum Beweis des Isomorphie-Lemmas (denn $\pi : A_1 \longrightarrow A_2$, $a \mapsto a$ ist ein injektiver starker Homomorphismus).* □

Definition 2.4.3 (Universelle Formeln). *Die Menge aller* universelle Formeln *über der Signatur S ist induktiv definiert durch:*

(a) Jede quantorenfreie Formel ist universell.

(b) Wenn φ und ψ universelle Formeln sind, dann sind auch $\varphi \wedge \psi$ und $\varphi \vee \psi$ universell.

(c) Wenn φ universell ist, dann ist auch $\forall x.\, \varphi$ universell.

(Intuition: die Konstrukte „$\exists$“ und „$\neg \ldots \forall$“ sind verboten!)

Lemma 2.4.3 (Unterstruktur-Lemma). *Seien $\mathcal{A}_1 = (A_1, \alpha_1)$ und $\mathcal{A}_2 = (A_2, \alpha_2)$ zwei S-Strukturen mit $\mathcal{A}_1 \subseteq \mathcal{A}_2$. Dann gilt für jede universelle Formel $\varphi \in L^S$: Wenn $\mathcal{A}_2 \models \varphi$, dann auch $\mathcal{A}_1 \models \varphi$.*

Beweis. *Durch Induktion über die Größe von t bzw. φ zeigt man, daß für alle Belegungen $\beta : X \longrightarrow A_1$ gilt:*

(a) $(\mathcal{A}_1, \beta)(t) = (\mathcal{A}_2, \beta)(t)$ für alle $t \in T^S$

(b) Wenn $\mathcal{A}_2, \beta \models \varphi$, dann $\mathcal{A}_1, \beta \models \varphi$ für alle universellen Formeln φ

(a) und der Induktionsanfang von (b) gelten nach Lemma 2.4.2 (S.20). Also ist nur noch der Induktionsschritt für (b) zu zeigen:
$\underline{\varphi \wedge \psi}$:

$$\begin{array}{rcl} \mathcal{A}_2, \beta \models \varphi \wedge \psi & \Rightarrow & \mathcal{A}_2, \beta \models \varphi \text{ und } \mathcal{A}_2, \beta \models \psi \\ & \overset{\text{I.A}}{\Rightarrow} & \mathcal{A}_1, \beta \models \varphi \text{ und } \mathcal{A}_1, \beta \models \psi \\ & \Rightarrow & \mathcal{A}_1, \beta \models \varphi \wedge \psi \end{array}$$

$\underline{\varphi \vee \psi}$:

$$\begin{array}{rcl} \mathcal{A}_2, \beta \models \varphi \vee \psi & \Rightarrow & \mathcal{A}_2, \beta \models \varphi \text{ oder } \mathcal{A}_2, \beta \models \psi \\ & \overset{\text{I.A}}{\Rightarrow} & \mathcal{A}_1, \beta \models \varphi \text{ oder } \mathcal{A}_1, \beta \models \psi \\ & \Rightarrow & \mathcal{A}_1, \beta \models \varphi \vee \psi \end{array}$$

$\underline{\forall x.\, \varphi}$:

$$\begin{array}{rcl} \mathcal{A}_2, \beta \models \forall x.\, \varphi & \Rightarrow & \mathcal{A}_2, \beta[a/x] \models \varphi \text{ für alle } a \in A_2, \text{ also erst recht für alle } a \in A_1 \\ & \overset{\text{I.A}}{\Rightarrow} & \mathcal{A}_1, \beta[a/x] \models \varphi \text{ für alle } a \in A_1 \text{ (denn jedes } \beta[a/x] \text{ paßt zu } \mathcal{A}_1) \\ & \Rightarrow & \mathcal{A}_1, \beta \models \forall x.\, \varphi \end{array}$$

Damit ist (b) bewiesen. Aus (b) folgt schließlich die Behauptung des Lemmas:

$$\begin{array}{rcl} \mathcal{A}_2 \models \varphi & \Rightarrow & \mathcal{A}_2, \beta \models \varphi \text{ für alle } \beta : X \longrightarrow A_2, \text{ also erst recht für alle } \beta : X \longrightarrow A_1 \\ & \overset{\text{(b)}}{\Rightarrow} & \mathcal{A}_1, \beta \models \varphi \text{ für alle } \beta : X \longrightarrow A_1 \\ & \Rightarrow & \mathcal{A}_1 \models \varphi \end{array}$$

□

2.5 Substitution

Idee: Bei gegebener Struktur $\mathcal{A}$ kann man die eine Formel φ als Aussage über die (Belegungen der) in φ frei vorkommenden Variablen auffassen, z.B. in der S_{Ar}-Struktur $\mathcal{N}$:

$$\exists z.\, x * z \equiv y$$

bedeutet „x teilt y“. Die Substitution ist ein syntaktisches Verfahren, um die „gleiche Aussage“ über „andere Elemente“ zu machen, z.B. erhalten wir „$x+1$ teilt $y+1$“ durch naives Einsetzen:

$$\exists z.\, (x+1) * z \equiv y+1$$

(wobei die syntaktische Struktur der Formel erhalten bleiben muß !).

Weiteres Beispiel: „$y+1$ teilt $x+1$“ erhalten wird durch „simultanes Einsetzen“:

$$\exists z.\, (y+1) * z \equiv x+1$$

Aber: das naive Einsetzen geht schief, wenn durch das Einsetzen neue Bindungen entstehen, z.B. „$x+1$ teilt $z+1$“ erhält man nicht durch

$$\exists z.\, (x+1) * z \equiv z+1$$

(schon deshalb nicht, weil nur noch x frei vorkommt) $\rightsquigarrow$ Deshalb Umbenennung:

$$\exists z'.\, (x+1) * z' \equiv z+1$$

Das motiviert die folgende

Definition 2.5.1 (Substitution). *Sei S eine Signatur, seien $x_0, \ldots, x_r \in X$ paarweise verschieden und seien $u_0, \ldots u_r \in T^S$.*

(1) Für jeden Term $t \in T^S$ sei $t[u_0, \ldots, u_r/x_0, \ldots, x_r] \in T^S$ (oder kurz: $t[\bar{u}/\bar{x}]$) induktiv definiert durch:

(a) $c[\bar{u}/\bar{x}] =_{\mathrm{def}} c$

(b)

$$x[\bar{u}/\bar{x}] = \begin{cases} u_i, & \textit{falls } x = x_i \\ x, & \textit{falls } x \notin \bar{x} \end{cases}$$

(c) $f(t_1, \ldots, t_n)[\bar{u}/\bar{x}] =_{\mathrm{def}} f(t_1[\bar{u}/\bar{x}], \ldots, t_n[\bar{u}/\bar{x}])$

(2) Für jede Formel $\varphi \in L^S$ sei

$\varphi[u_0, \ldots, u_r/x_0, \ldots, x_r]$ (kurz: $\varphi[\bar{u}/\bar{x}]$) definiert durch:

(a) $(t_1 \equiv t_2)[\bar{u}/\bar{x}] =_{\mathrm{def}} t_1[\bar{u}/\bar{x}] \equiv t_2[\bar{u}/\bar{x}]$

(b) $r(t_1, \ldots, t_n)[\bar{u}/\bar{x}] =_{\mathrm{def}} r(t_1[\bar{u}/\bar{x}], \ldots, t_n[\bar{u}/\bar{x}])$

(c) $(\neg\varphi)[\bar{u}/\bar{x}] =_{\mathrm{def}} \neg(\varphi[\bar{u}/\bar{x}])$

(d) $(\varphi \vee \psi)[\bar{u}/\bar{x}] =_{\text{def}} \varphi[\bar{u}/\bar{x}] \vee \psi[\bar{u}/\bar{x}]$

(e)

$$(\exists x.\, \varphi)[\bar{u}/\bar{x}] =_{\text{def}} \begin{cases} \exists z.\, \varphi[z/x][\bar{u}\backslash u_i/\bar{x}\backslash x_i], & \textit{falls } x = x_i \\ \exists z.\, \varphi[z/x][\bar{u}/\bar{x}], & \textit{falls } x \notin \bar{x} \end{cases}$$

wobei z eine Variable ist, die nicht in $u_0, \ldots, u_r$ und φ vorkommt (man kann $z = x$ wählen, wenn x nicht in $u_0, \ldots, u_r$ vorkommt, ansonsten sei z die erste Variable in der Aufzählung $v_0, v_1, \ldots$ die nicht in $u_0, \ldots, u_r$ vorkommt).

Sprechweise: $t[\bar{u}/\bar{x}]$ bzw. $\varphi[\bar{u}/\bar{x}]$ entsteht aus t bzw. φ durch simultane Substitution *von $\bar{u}$ für $\bar{x}$.*

Beispiel 2.5.1. *Hier einige Beispiele*

(a) $(\exists z.\, x * z \equiv y)[x+1, y+1/x, y] = \exists z.\, (x+1) * z \equiv y+1$

(b) $(\exists z.\, x * z \equiv y)[y+1, x+1/x, y] = \exists z.\, (y+1) * z \equiv x+1$

(c) $(\exists z.\, x * z \equiv y)[x+1, z+1/x, y] = \exists z'.\, (x+1) * z' \equiv z+1$

Bemerkung 2.5.1. *Warnung: (b) ist nicht dasselbe wie*

$$((\exists z.\, x * z \equiv y)[y+1/x])[x+1/y] = \exists z.\, ((x+1)+1) * z \equiv x+1$$

d.h. simultane Substitution ist nicht dasselbe wie mehrere aufeinanderfolgende Substitutionen.

Lemma 2.5.1 (Substitutionslemma). *Seien S, $\bar{x}$ und $\bar{u}$ wie in der Definition, und sei $\mathcal{I} = (\mathcal{A}, \beta)$ eine S-Interpretation. Dann gilt für alle $t \in T^S$ bzw. $\varphi \in L^S$:*

(a) $\mathcal{I}(t[\bar{u}/\bar{x}]) = \mathcal{I}[\mathcal{I}(\bar{u})/\bar{x}](t)$

(b) $\mathcal{I}(\varphi[\bar{u}/\bar{x}]) = \mathcal{I}[\mathcal{I}(\bar{u})/\bar{x}](\varphi)$

wobei $\mathcal{I}[\mathcal{I}(\bar{u})/\bar{x}] =_{\text{def}} \mathcal{I}[\mathcal{I}(u_0)/x_0] \ldots [\mathcal{I}(u_r)/x_r]$. (In Worten: $\varphi[\bar{u}/\bar{x}]$ ist genau dann erfüllt, wenn φ für die Werte $\mathcal{I}(u_0), \ldots, \mathcal{I}(u_r)$ erfüllt ist.)

Beweis. *Hier nicht: den genauen Beweis möge der Leser führen!* □

Beispiel 2.5.2. *Sei $\varphi = \exists z.\, x * z \equiv y$. Dann gilt:*

$$\mathcal{N}, \beta \models \varphi \quad \Leftrightarrow \quad \beta(x) \textit{ teilt } \beta(y)$$

Dann gilt für alle $u, v \in T^{S_{\text{Ar}}}$:

$$\begin{array}{lll} (\mathcal{N}, \beta)(\varphi[u, v/x, y]) = \textit{true}) & \overset{\textit{Lemma 2.5.1}}{\Leftrightarrow} & (\mathcal{N}, \beta[(\mathcal{N}, \beta)(u), (\mathcal{N}, \beta)(v)/x, y])(\varphi) = \textit{true} \\ & \Leftrightarrow & (\mathcal{N}, \beta)(u) \textit{ teilt } (\mathcal{N}, \beta)(v) \end{array}$$

Korollar 2.5.1. *Es gilt stets:*

(a) $\forall x.\, \varphi \models \varphi[t/x]$ (Instanziierung)

(b) $\forall x.\, \varphi \doteq \forall y.\, \varphi[y/x]$ *falls* $y \notin \mathit{frei}(\varphi)$

Beweis.

(a) *Sei $\mathcal{I}$ eine Interpretation mit $\mathcal{I} \models \forall x.\, \varphi$, d.h. $\mathcal{I}[a/x] \models \varphi$ für alle a, insbesondere $\mathcal{I}[\mathcal{I}(t)/x] \models \varphi$, d.h. nach dem Substitutionslemma (S.23) $\mathcal{I} \models \varphi[t/x]$.*

(b) *Für alle Interpretationen $\mathcal{I}$ gilt:*

$$
\begin{array}{rcl}
\mathcal{I}(\forall x.\, \varphi) = \mathit{true} & \Leftrightarrow & \text{für alle } a \text{ gilt: } \mathcal{I}[a/x](\varphi) = \mathit{true} \\
\mathcal{I}(\forall y.\, \varphi[y/x]) = \mathit{true} & \Leftrightarrow & \text{für alle } a \text{ gilt: } \mathcal{I}[a/y](\varphi[y/x]) = \mathit{true} \\
& \overset{\text{Lemma 2.5.1}}{\Leftrightarrow} & \underbrace{\mathcal{I}[a/y][\underbrace{\mathcal{I}[a/y](y)}_{=a}/x](\varphi) = \mathit{true}}_{\overset{(*)}{=} \mathcal{I}[a/x](\varphi)}
\end{array}
$$

(*) gilt nach Koinzidenzlemma (S.14), da $y \notin \mathit{frei}(\varphi)$.

□

Kapitel 3

Ein Kalkül für die Prädikatenlogik erster Stufe

„Je mehr Käse, desto mehr Löcher.
Je mehr Löcher, desto weniger Käse.
Also: Je mehr Käse, desto weniger Käse! Oder?“
ARISTOTELES (384-322 v.Chr.)

Bisher:
Gültigkeit $\models \varphi$ und logische Folgerung $\Phi \models \varphi$ sind präzise definiert, aber um sie im Einzelfall zu zeigen, benutzen wir die übliche mathematische „Beweistechnik(en)“.

Jetzt:
Einführung von *Axiomen* und *Ableitungsregeln*, mit denen wir solche Beweise in kleine syntaktische Schritte zerlegen könnnen.

Hier: Kalkül, der mit sogenannten *Sequenzen* arbeitet.

3.1 Der Sequenzenkalkül Σ

Definition 3.1.1 (Sequenz). *Eine* Sequenz *ist eine nichtleere Folge $\varphi_0 \dots \varphi_n \; \varphi$ ($n \geq 0$) von Formeln (aus L^S). $\varphi_0 \dots \varphi_n$ heißt* Antezedens *der Sequenz, φ heißt das* Sukzedens *der Sequenz.*

Intuition: Eine Sequenz $\varphi_0 \dots \varphi_n \; \varphi$ soll bedeuten, daß φ unter den Annahmen $\varphi_0 \dots \varphi_n$ gilt.

Definition 3.1.2. *Eine Sequenz $\varphi_0 \dots \varphi_n \; \varphi$ heißt* gültig *(oder* korrekt*), wenn*

$$\{\varphi_0, \dots, \varphi_n\} \models \varphi$$

Bezeichnung 3.1.1. *Für beliebige (eventuell leere) Folgen von Formeln benutzen wir Metavariablen* $\Gamma, \Delta, \ldots$*, d.h. eine Sequenz können wir dann in der Form* $\Gamma\ \varphi$ *schreiben.*

3.1.1 Die Axiome und Regeln des Kalküls Σ

Antezedensregel (Ant)

$$\frac{\Gamma \quad \varphi}{\Gamma' \quad \varphi}$$

falls $\Gamma \subseteq \Gamma'$ (d.h. jedes Element von Γ kommt auch in Γ' vor; die Häufigkeit und die Anordnung der Formeln spielt keine Rolle).

Voraussetzungsregel (Vor)

$$\frac{}{\Gamma \quad \varphi}$$

falls $\varphi \in \Gamma$ (d.h. falls φ in Γ vorkommt.)

Fallunterscheidungsregel (FU)

$$\frac{\begin{array}{lll}\Gamma & \psi & \varphi\\ \Gamma & \neg\psi & \varphi\end{array}}{\Gamma \qquad \varphi}$$

(Um φ zu zeigen, genügt es, φ einmal unter der Annahme ψ und dann unter der Annahme $\neg\psi$ zu zeigen.)

Widerspruchsregel (Wid)

$$\frac{\begin{array}{lll}\Gamma & \neg\varphi & \psi\\ \Gamma & \neg\varphi & \neg\psi\end{array}}{\Gamma \qquad \varphi}$$

(Um φ zu zeigen, genügt es, $\neg\varphi$ zum Widerspruch zu führen.)

Regel $\vee$-Einführung im Antezedens ($\vee$ A)

$$\frac{\begin{array}{lll}\Gamma & \varphi & \chi\\ \Gamma & \psi & \chi\end{array}}{\Gamma \quad \varphi \vee \psi \quad \chi}$$

(Um χ unter der Annahme $\varphi \vee \psi$ zu zeigen, zeigt man, daß χ in jedem der beiden Fälle gilt.)

Regel $\vee$-Einführung im Sukzedens ($\vee$ S)

(a) *(b)*

$$\frac{\Gamma \quad \varphi}{\Gamma \quad \varphi \vee \psi} \qquad \frac{\Gamma \quad \psi}{\Gamma \quad \varphi \vee \psi}$$

(Um $\varphi \vee \psi$ zu beweisen, genügt es (a) φ zu beweisen oder (b) ψ zu beweisen.)

Regel ∃-Einführung im Antezedens (∃A)

$$\frac{\Gamma \quad \varphi[y/x] \quad \psi}{\Gamma \quad \exists x.\,\varphi \quad \psi}$$

falls y nicht frei in Γ, $\exists x.\,\varphi$, ψ vorkommt (um ψ unter der Annahme $\exists x.\,\varphi$ zu beweisen, sagt man „Sei y ein Element, für das φ gilt“ und beweist dann φ. Dabei muß y ein „neuer Name“ sein).

Regel ∃-Einführung im Sukzedens (∃ S)

$$\frac{\Gamma \quad \varphi[t/x]}{\Gamma \quad \exists x.\,\varphi}$$

(Um $\exists x.\,\varphi$ zu beweisen, genügt es einen „Beispielterm“ t anzugeben, für den φ gilt.)

Reflexivität der Gleichheit (≡)

$$\frac{}{t \equiv t}$$

Substitutionsregel der Gleichheit (Sub)

$$\frac{\Gamma \qquad\qquad \varphi[t/x]}{\Gamma \quad t \equiv t' \quad \varphi[t'/x]}$$

(Wenn φ für t gilt, dann folgt unter der zusätzlichen Annahme $t \equiv t'$, daß φ auch für t' gilt.)

Definition 3.1.3 (Ableitung). *(a) Eine* Ableitung *(oder ein* formaler Beweis*) im Sequenzenkalkül ist eine endliche Folge von Sequenzen*

$$\begin{array}{ll} \Gamma_0 & \varphi_0 \\ \vdots & \vdots \\ \Gamma_m & \varphi_m \end{array}$$

so, daß für $i = 0, \ldots, m$ gilt:

- *entweder $\Gamma_i\ \varphi_i$ ist ein Axiom*
- *oder $\Gamma_i\ \varphi_i$ entsteht durch einer Ableitungsregel aus früheren Sequenzen (d.h. aus Sequenzen $\Gamma_k\ \varphi_k$ mit $k < i$)*

(b) Eine Sequenz $\Gamma\ \varphi$ heißt ableitbar *(oder* formal beweisbar*, wenn es eine Ableitung gibt, in der sie als letzte Zeile steht. Schreibweise:* $\vdash \Gamma\ \varphi$

(c) Sei $\Phi \subseteq L^S$ und $\varphi \in L^S$. φ heißt ableitbar *aus Φ, wenn es $\varphi_0, \ldots, \varphi_n \in \Phi$ gibt mit $\vdash \varphi_0 \ldots \varphi_n\ \varphi$. Schreibweise:* $\Phi \vdash \varphi$

Beispiel 3.1.1. *Hier zwei Beispiele*

(a) *„Tertium non datur“*[1]*:* $\vdash \varphi \vee \neg\varphi$

Formaler Beweis:

1.	φ	φ	*wegen (Vor)*
2.	φ	$\varphi \vee \neg\varphi$	*mit (∨ S)(a) aus 1.*
3.	$\neg\varphi$	$\neg\varphi$	*wegen (Vor)*
4.	$\neg\varphi$	$\varphi \vee \neg\varphi$	*mit (∨ S)(b) aus 3.*
5.		$\varphi \vee \neg\varphi$	*mit (FU) aus 2. und 4. (mit leerem* Γ*)*

(b) *„Symmetrie“*

Ableitung:

1.	$t_1 \equiv t_1$		*wegen (≡)*
2.	$t_1 \equiv t_2$	$t_2 \equiv t_1$	*mit (Sub) aus 1. (mit* $\varphi = x = t_1$ *wobei* x *neu und* $\Gamma = \emptyset$*)*

3.2 Abgeleitete Regeln (derived rules)

Sequenzen, die man bereits formal bewiesen hat, kann man von da an als Axiome benutzen, z.B.:

- „Tertium non datur“ (TND): $\varphi \vee \neg\varphi$

Allgemeiner:
Wenn man eine Sequenz $\Gamma\ \varphi$ aus anderen Sequenzen $\Gamma_1\ \varphi_1, \ldots, \Gamma_k\ \varphi_k$ abgeleitet hat, dann kann man von da an die Regel

$$\frac{\begin{array}{cc}\Gamma_1 & \varphi_1\\ \vdots & \vdots\\ \Gamma_k & \varphi_k\end{array}}{\begin{array}{cc}\Gamma & \varphi\end{array}}$$

verwenden. Solche Regeln nennt man *abgeleitete Regeln.*

Beispiel 3.2.1. *Hier einige Beispiele für abgeleitete Regeln*

(1) ***Modifizierte Widerspruchsregel (Wid')***

$$\frac{\begin{array}{cc}\Gamma & \psi\\ \Gamma & \neg\psi\end{array}}{\begin{array}{cc}\Gamma & \varphi\end{array}}$$

Wenn Γ *schon einen Widerspruch „enthält“, dann folgt jede Formel* φ *aus* Γ*.*

Idee: Man nimmt in den Prämissen jeweils $\neg\varphi$ *zum Antezedens hinzu und wendet dann (Wid) an.*

Formaler Beweis:

1.	Γ		ψ	*Prämisse*
2.	Γ		$\neg\psi$	*Prämisse*
3.	Γ	$\neg\varphi$	ψ	*mit (Ant) aus 1.*
4.	Γ	$\neg\varphi$	$\neg\psi$	*mit (Ant) aus 2.*
5.	Γ		φ	*mit (Wid) aus 4.*

[1] Aus dem Lateinischen: *„Ein Drittes ist ausgeschlossen“*

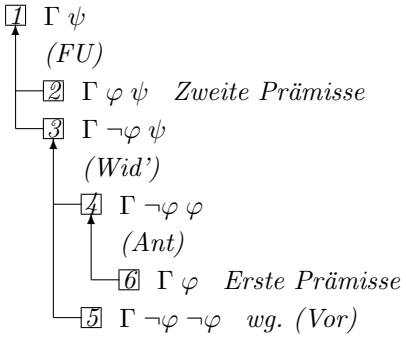
(2) ***Kettenschlußregel (KS)***

$$\frac{\Gamma \quad \varphi \qquad \Gamma \quad \varphi \quad \psi}{\Gamma \quad \psi}$$

Um ψ zu beweisen, beweist man zunächst ein „Lemma“ φ und zeigt dann, daß ψ unter der (zusätzlichen) Annahme φ gilt.

Idee: Fallunterscheidung nach φ. Wenn φ gilt, so greift die zweite Prämisse. Wenn φ nicht gilt, so gelangt man mit der ersten Prämisse zum Widerspruch.

„Rückwärtsbeweis“: (Man geht vom Ziel aus, hier von der Konklusion, wendet die Regel(n) rückwärts an, erhält „Teilziele“ usw. bis zu Axiomen und Prämissen).



(3) ***Kontraposition (KP)***

(a)
$$\frac{\Gamma \quad \varphi \quad \psi}{\Gamma \quad \neg\psi \quad \neg\varphi}$$

(b)
$$\frac{\Gamma \quad \neg\varphi \quad \neg\psi}{\Gamma \quad \psi \quad \varphi}$$

(c)
$$\frac{\Gamma \quad \neg\varphi \quad \psi}{\Gamma \quad \neg\psi \quad \varphi}$$

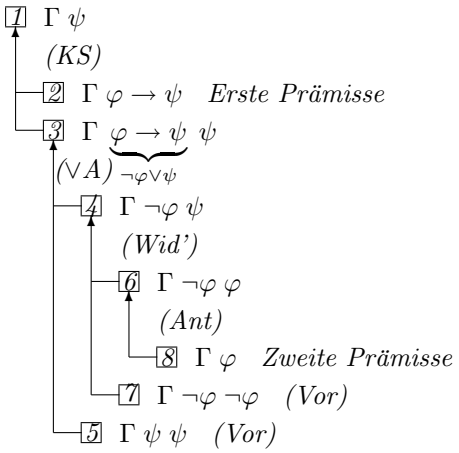
(d)
$$\frac{\Gamma \quad \varphi \quad \neg\psi}{\Gamma \quad \psi \quad \neg\varphi}$$

Formaler Beweis: Übung!

(4) ***Modus Ponens (MP)***

$$\frac{\Gamma \quad \varphi \to \psi \qquad \Gamma \quad \varphi}{\Gamma \quad \psi}$$

Formaler Beweis:



(5) ***Modifizierter Modus Ponens (MP')***

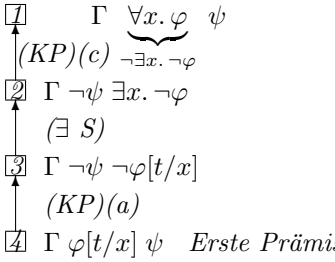
$$\frac{\Gamma \quad \varphi \vee \psi \qquad \Gamma \quad \neg\varphi}{\Gamma \quad \psi}$$

Formaler Beweis: *Analog zu (MP)*

(6) ***Allquantor im Antezedens (∀ A)***

$$\frac{\Gamma \quad \varphi[t/x] \quad \psi}{\Gamma \quad \forall x.\, \varphi \quad \psi}$$

Formaler Beweis:

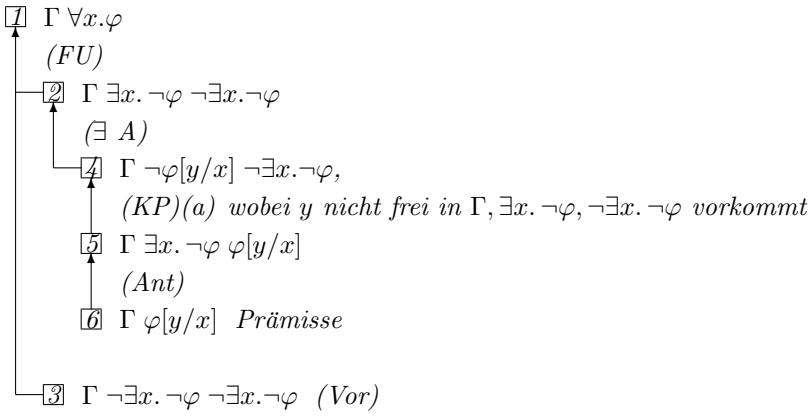


(7) ***Allquantor im Sukzedens (∀ S)***

$$\frac{\Gamma \quad \varphi[y/x]}{\Gamma \quad \forall x.\, \varphi} \quad \textit{falls } y \textit{ nicht frei vorkommt in } \Gamma \textit{ und } \forall x.\, \varphi$$

Spezialfall: $\dfrac{\Gamma \quad \varphi}{\Gamma \quad \forall x.\, \varphi}$ *falls* x *nicht frei in* Γ *und* $\forall x.\, \varphi$

Formaler Beweis:



3.3 Korrektheit des Sequenzenkalküls

Ziel: Es soll gezeigt werden, daß „Ableitbarkeit“ (bzw. formale Beweisbarkeit) und „logische Folgerung“ übereinstimmen, d.h. daß für alle $\Phi \subseteq L^S$ und $\varphi \in L^S$ gilt:

$$\Phi \vdash \varphi \Leftrightarrow \Phi \models \varphi$$

Die Richtung „$\Rightarrow$“ bezeichnet man als *Korrektheit* des Kalküls (engl.: *soundness*): jede ableitbare Formel ist auch logische Folgerung, d.h. man kann nichts „falsches“ ableiten. Die Richtung „$\Leftarrow$“ bezeichnet man als *Vollständigkeit* des Kalküls: jede logische Folgerung von Φ ist ableitbar aus Φ.

Satz 3.3.1 (Korrektheit des Sequenzenkalküls). *Sei S eine Signatur, $\Phi \subseteq L^S$ und $\varphi \in L^S$. Dann gilt:*

$$\textit{wenn } \Phi \vdash \varphi, \textit{ dann } \Phi \models \varphi$$

(insbesondere: wenn $\vdash \varphi$, dann $\models \varphi$.)

Beweis. *Es genügt zu zeigen, daß jede ableitbare Sequenz gültig ist, d.h daß aus $\vdash \varphi_0 \dots \varphi_n \varphi$ stets $\{\varphi_0, \dots, \varphi_n\} \models \varphi$ folgt, denn*

$$\begin{aligned} \Phi \vdash \varphi \quad &\overset{\text{Def. von } \vdash}{\Leftrightarrow} \quad \text{es ex. } \varphi_0, \dots, \varphi_n \in \Phi \text{ mit } \vdash \varphi_0 \dots \varphi_n \varphi \\ &\overset{\text{oben}}{\Rightarrow} \quad \text{es. ex.} \varphi_0, \dots, \varphi_n \in \Phi \text{ mit } \{\varphi_0, \dots, \varphi_n\} \models \varphi \\ &\overset{\text{erst recht}}{\Rightarrow} \quad \Phi \models \varphi \end{aligned}$$

Um nun zu zeigen, daß jede ableitbare Sequenz gültig ist, genügt es zu zeigen:

- *jedes Axiom ist gültig*
- *jede Ableitungsregel erhält die Gültigkeit, d.h. wenn all ihre Prämissen gültig sind, dann ist auch ihre Konklusion gültig.*

Im einzelnen:

- *(Ant)* Z.zg.: *Wenn* $\Gamma \subseteq \Gamma'$ *und* $\Gamma \models \varphi$, *dann auch* $\Gamma' \models \varphi$ *(klar per Definition von* $\models$*)*
- *(Vor)* Z.zg.: *Wenn* $\varphi \in \Gamma$, *dann* $\Gamma \models \varphi$ *(klar per Definition von* $\models$*)*
- *(Wid)* Z.zg.: *Wenn* $\Gamma \cup \{\neg\varphi\} \models \psi$ *und* $\Gamma \cup \{\neg\varphi\} \models \neg\psi$, *dann* $\Gamma \models \varphi$

  Angenommen $\Gamma \not\models \varphi$, *d.h. es existiert ein* $\mathcal{I}$ *mit* $\mathcal{I} \models \Gamma$ *und* $\underbrace{\underbrace{\mathcal{I} \not\models}_{\mathcal{I} \models \neg\varphi} \varphi}_{\mathcal{I} \models \Gamma \cup \{\neg\varphi\}}$

  Mit den Prämissen folgt dann $\mathcal{I} \models \psi$ *und* $\mathcal{I} \models \neg\psi$, *Widerspruch! Also muß doch, wie erwartet,* $\Gamma \models \varphi$ *gelten.*
- *(*$\vee A$*)* Z.zg.: *Wenn* $\Gamma \cup \{\varphi\} \overset{1)}{\models} \chi$ *und* $\Gamma \cup \{\psi\} \overset{2)}{\models} \chi$, *dann* $\Gamma \cup \{\varphi \vee \psi\} \models \chi$

  Sei $\mathcal{I} \models \Gamma \cup \{\varphi \vee \psi\}$, *d.h.* $\mathcal{I} \models \Gamma$ *und* $\mathcal{I} \models \varphi \vee \psi$ *(d.h.* $\mathcal{I} \models \varphi$ *oder* $\mathcal{I} \models \psi$*)*

  1. Fall:

  $\mathcal{I} \models \varphi$, *also* $\mathcal{I} \models \Gamma \cup \{\varphi\}$. *Dann folgt* $\mathcal{I} \models \chi$ *nach 1)*

  2. Fall:

  $\mathcal{I} \models \psi$, *also* $\mathcal{I} \models \Gamma \cup \{\psi\}$. *Dann folgt* $\mathcal{I} \models \chi$ *nach 2)*
- *(*$\vee S$*) ist klar!*
- *(*$\exists A$*)* Z.zg.: *Wenn* $\Gamma \cup \{\varphi[y/x]\} \models \psi$, *dann* $\Gamma \cup \{\exists x.\, \varphi\} \models \psi$ *(wobei* y *nicht frei in* Γ, $\exists x.\, \varphi$ *und* ψ *vorkommt).*

  Sei $\mathcal{I} \models \Gamma \cup \{\exists x.\, \varphi\}$, *d.h.* $\mathcal{I} \models \Gamma$ *und* $\mathcal{I} \models \exists x.\, \varphi$ *(d.h. es existiert ein* $a \in A$ *mit* $\mathcal{I}[a/x] \models \varphi$*). Wir betrachten die Interpretation* $\mathcal{I}[a/y]$*:*
  Da $\mathcal{I} \models \Gamma$ *folgt mit dem Koinzidenzlemma (weil ja* $y \notin$ *frei*(Γ)*):* $\mathcal{I}[a/y] \models \Gamma$
  Weiter gilt: $\mathcal{I}[a/y](\varphi[y/x]) \overset{\text{Lemma } 2.5.1}{=} \mathcal{I}[a/y][\underbrace{\mathcal{I}[a/y](y)}_{a}/x](\varphi) \overset{(*)}{=} \mathcal{I}[a/x](\varphi) =$ *true*
  Bemerkung zu (*):

  - *Im Falle* $y = x$ *ist* $\mathcal{I}[a/y][a/x] = \mathcal{I}[a/x]$
  - *Im Falle* $y \neq x$ *greift das Koinzidenzlemma (S.14), weil dann ja* $y \notin$ *frei*(φ)

  Also insgesamt erhalten wir dann: $\mathcal{I}[a/y] \models \Gamma \cup \{\varphi[y/x]\}$. *Nach Voraussetzung folgt dann:* $\mathcal{I}[a/y] \models \psi$. *Daraus folgt* $\mathcal{I} \models \psi$ *nach Koinzidenzlemma, weil* $y \notin$ *frei*(ψ)

- *(∃S)* *Z.zg.:* *Wenn* $\Gamma \models \varphi[t/x]$*, dann* $\Gamma \models \exists x.\, \varphi$

  Sei $\mathcal{I} \models \Gamma$*. Nach Voraussetzung folgt dann* $\mathcal{I} \models \varphi[t/x]$*, also nach dem Substitutionslemma:* $\mathcal{I}[\mathcal{I}(t)/x] \models \varphi$*. Also existiert ein* $a \in A$ *mit* $\mathcal{I}[a/x] \models \varphi$ *und damit* $\mathcal{I} \models \exists.x\, \varphi$

- *(≡)* *Z.zg.:* $\models t \equiv t$ *(Klar!)*

- *(Sub)* *Z.zg.:* *Wenn* $\Gamma \models \varphi[t/x]$*, dann auch* $\Gamma \cup \{t \equiv t'\} \models \varphi[t'/x]$

  Sei $\mathcal{I} \models \Gamma \cup \{t \equiv t'\}$*, d.h.* $\mathcal{I} \models \Gamma$ *und* $\mathcal{I}(t) = \mathcal{I}(t')$*. Dann gilt nach Voraussetzung auch* $\mathcal{I} \models \varphi[t/x]$*, also nach dem Substitutionslemma* $\mathcal{I}[\underbrace{\mathcal{I}(t)}_{=\mathcal{I}(t')}/x] \models \varphi$*. Also wieder nach dem Substitutionslemma:* $\mathcal{I} \models \varphi[t'/x]$*.*

□

3.4 Beispiel einer Ableitung im Sequenzenkalkül

Zunächst: Einige weitere abgeleitete Regeln (aber ohne Beweis).

Regel ∧-Einführung im Antezedens (∧ A)

$$\frac{\Gamma \quad \varphi \quad \psi \qquad \chi}{\Gamma \qquad \varphi \wedge \psi \quad \chi}$$

Regel ∧-Einführung im Sukzedens (∧ S)

$$\frac{\begin{array}{ll}\Gamma & \varphi \\ \Gamma & \psi\end{array}}{\Gamma \quad \varphi \wedge \psi}$$

Regel →-Einführung im Sukzedens (→ S)

$$\frac{\Gamma \quad \varphi \quad \psi}{\Gamma \qquad \varphi \rightarrow \psi}$$

Regel ↔-Einführung im Sukzedens (↔ S)

$$\frac{\begin{array}{ll}\Gamma & \varphi \rightarrow \psi \\ \Gamma & \psi \rightarrow \varphi\end{array}}{\Gamma \quad \varphi \leftrightarrow \psi}$$

Reflexivität der Gleichheit (Refl)

$$\frac{}{\Gamma \quad t \equiv t}$$

Symmetrie der Gleichheit (Symm)

$$\frac{\Gamma \quad t_1 \equiv t_2}{\Gamma \quad t_2 \equiv t_1}$$

Transitivität der Gleichheit (Trans)

$$\frac{\begin{array}{ll}\Gamma & t_1 \equiv t_2 \\ \Gamma & t_2 \equiv t_3\end{array}}{\Gamma \quad t_1 \equiv t_3}$$

Modifizierte Substitutionsregel (Sub')

$$\frac{\Gamma \qquad\quad \varphi[t'/x]}{\Gamma \quad t \equiv t' \quad \varphi[t/x]}$$

Funktionsverträglichkeit der Gleichheit für $f \in F_n$ (Fkt)

$$\frac{\begin{array}{ll}\Gamma & t_1 \equiv t'_1 \\ \vdots & \vdots \\ \Gamma & t_n \equiv t'_n\end{array}}{\Gamma \quad f(t_1, \ldots, t_n) \equiv f(t'_1, \ldots, t'_n)}$$

Relationsverträglichkeit der Gleichheit für $r \in R_n$ (Rel)

$$\frac{\begin{array}{ll}\Gamma & r(t_1, \ldots, t_n) \\ \Gamma & t_1 \equiv t'_1 \\ \vdots & \vdots \\ \Gamma & t_n \equiv t'_n\end{array}}{\Gamma \quad r(t'_1, \ldots, t'_n)}$$

Es wird jetzt gezeigt, daß für jede Äquivalenzrelation $\sim$ die Formel

$$\varphi = \forall x.\, \forall y.\, (\exists z.\, x \sim z \wedge y \sim z) \rightarrow (\forall z.\, x \sim z \rightarrow y \sim z)$$

gilt, d.h. es wird die Sequenz $\Gamma\ \varphi$ hergeleitet, wobei Γ aus den Formeln

$$\begin{array}{lcl}\text{refl} & = & \forall x.\, x \sim x \\ \text{symm} & = & \forall y.\, x \sim y \rightarrow y \sim x \\ \text{trans} & = & \forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \rightarrow x \sim z\end{array}$$

besteht.

Bemerkung 3.4.1. *Eine Sequenz $\varphi_0 \ldots \varphi_n\, \varphi$ wird hier (zur besseren Lesbarkeit) in der Form $[\varphi_n, \ldots, \varphi_0] \Rightarrow \varphi$ geschrieben.*

(1) $[\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z]$
$\Rightarrow \forall x.\, \forall y.\, (\exists z.\, x \sim z \wedge y \sim z) \to (\forall z.\, x \sim z \to y \sim z)$
Mit Regel ($\forall$ S) aus (2)

(2) $[\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z]$
$\Rightarrow \forall y.\, (\exists z.\, x \sim z \wedge y \sim z) \to (\forall z.\, x \sim z \to y \sim z)$
Mit Regel ($\forall$ S) aus (3)

(3) $[\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z]$
$\Rightarrow (\exists z.\, x \sim z \wedge y \sim z) \to (\forall z.\, x \sim z \to y \sim z)$
Mit Regel ($\to$ S) aus (4)

(4) $[\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$\exists z.\, x \sim z \wedge y \sim z]$
$\Rightarrow \forall z.\, x \sim z \to y \sim z$
Mit Regel ($\forall$ S) aus (5)

(5) $[\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$\exists z.\, x \sim z \wedge y \sim z]$
$\Rightarrow x \sim z \to y \sim z$
Mit Regel ($\to$ S) aus (6)

(6) $[\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$\exists z.\, x \sim z \wedge y \sim z,$
$x \sim z]$
$\Rightarrow y \sim z$
Mit Regel (Ant) aus (7):
Umordnen des Antezedens

(7) $[x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$\exists z.\, x \sim z \wedge y \sim z]$
$\Rightarrow y \sim z$
Mit Regel ($\exists$ A) aus (8)

(8) $[x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya \wedge y \sim ya]$
$\Rightarrow y \sim z$
Mit Regel ($\wedge$ A) aus (9)

(9) $[x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya]$
$\Rightarrow y \sim z$
Mit Regel (KS) aus (10) und (26):
Als „Lemma“ führen wir $y \sim x$ ein.

(10) $[x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya]$
$\Rightarrow y \sim x$
Mit Regel (KS) aus (11) und (17):
Als „Lemma“ führen wir $ya \sim x$ ein.

(11) $[x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya]$
$\Rightarrow ya \sim x$
Mit Regel (Ant) aus (12):
Umordnen des Antezedens

(12) $[\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x]$
$\Rightarrow ya \sim x$
Mit Regel ($\forall$ A) aus (13):
Die Variable wird mit x instantiiert.

(13) $[\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall y.\, x \sim y \to y \sim x]$
$\Rightarrow ya \sim x$
Mit Regel (∀ A) aus (14):
Wir instantiieren die ∀-quantifizierte Variable mit ya.

(14) $[\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya,$
$x \sim z,$
$\forall x.\, x \sim x,$
$x \sim ya \to ya \sim x]$
$\Rightarrow ya \sim x$
Mit Regel (MP) aus (15) und (16):
Als „Lemma“ führen wir $x \sim ya$ ein.

(15) $[\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya,$
$x \sim z,$
$\forall x.\, x \sim x,$
$x \sim ya \to ya \sim x]$
$\Rightarrow x \sim ya \to ya \sim x$
Mit Regel (Vor)

(16) $[\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim z,$
$x \sim ya,$
$y \sim ya,$
$\forall x.\, x \sim x,$
$x \sim ya \to ya \sim x]$
$\Rightarrow x \sim ya$
Mit Regel (Vor)

(17) $[x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya,$
$ya \sim x]$
$\Rightarrow y \sim x$
Mit Regel (Ant) aus (18):
Umordnen des Antezedens

(18) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z]$
$\Rightarrow y \sim x$
Mit Regel ($\forall$ A) aus (19):
Wir instantiieren die $\forall$-quantifizierte Variable mit y.

(19) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall ya.\, \forall z.\, y \sim ya \wedge ya \sim z \to y \sim z]$
$\Rightarrow y \sim x$
Mit Regel ($\forall$ A) aus (20):
Wir instantiieren die $\forall$-quantifizierte Variable mit ya.

(20) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall z.\, y \sim ya \wedge ya \sim z \to y \sim z]$
$\Rightarrow y \sim x$
Mit Regel ($\forall$ A) aus (21):
Wir instantiieren die $\forall$-quantifizierte Variable mit x.

(21) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$y \sim ya \wedge ya \sim x \to y \sim x]$
$\Rightarrow y \sim x$
Mit Regel (MP) aus (22) und (23):
Als „Lemma“ führen wir $y \sim ya \wedge ya \sim x$ ein.

(22) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$

$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$y \sim ya \wedge ya \sim x \to y \sim x]$
$\Rightarrow y \sim ya \wedge ya \sim x \to y \sim x$
Mit Regel (Vor)

(23) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$y \sim ya \wedge ya \sim x \to y \sim x]$
$\Rightarrow y \sim ya \wedge ya \sim x$
Mit Regel ($\wedge$ S) aus (24) und (25)

(24) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$y \sim ya \wedge ya \sim x \to y \sim x]$
$\Rightarrow y \sim ya$
Mit Regel (Vor)

(25) $[x \sim ya,$
$y \sim ya,$
$ya \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$y \sim ya \wedge ya \sim x \to y \sim x]$
$\Rightarrow ya \sim x$
Mit Regel (Vor)

(26) $[x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z,$
$x \sim ya,$
$y \sim ya,$
$y \sim z]$
$\Rightarrow y \sim z$
Mit Regel (Ant) aus (27):
Umordnen des Antezedens

(27) $[x \sim ya,$
$y \sim ya,$
$y \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x;$
$\forall x.\, \forall y.\, \forall z.\, x \sim y \wedge y \sim z \to x \sim z]$
$\Rightarrow y \sim z$
Mit Regel ($\forall$ A) aus (28):
wir instantiieren die $\forall$-quantifizierte Variable mit y.

(28) $[x \sim ya,$
$y \sim ya,$
$y \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall ya.\, \forall z.\, y \sim ya \wedge ya \sim z \to y \sim z]$
$\Rightarrow y \sim z$
Mit Regel ($\forall$ A) aus (29):
Wir instantiieren die $\forall$-quantifizierte Variable wird mit x.

(29) $[x \sim ya,$
$y \sim ya,$
$y \sim x,$
$x \sim z,$
$\forall x.\, x \sim x,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$\forall z.\, y \sim x \wedge x \sim z \to y \sim z]$
$\Rightarrow y \sim z$
Mit Regel ($\forall$ A) aus (30):
Wir instantiieren die $\forall$-quantifizierte Variable mit z.

(30) $[x \sim ya,$
$y \sim ya,$
$y \sim x,$
$x \sim z,$
$\forall x.\, \forall y.\, x \sim y \to y \sim x,$
$y \sim x \wedge x \sim z \to y \sim z,$
$\forall x.\, x \sim x]$
$\Rightarrow y \sim z$
Mit Regel (MP) aus (31) und (32):
Als „Lemma“ führen wir $y \sim x \wedge x \sim z$ ein.

(31) $[x \sim ya,$
$y \sim ya,$
$y \sim x,$

$x \sim z$,
$\forall x.\, x \sim x$,
$\forall x.\, \forall y.\, x \sim y \to y \sim x$,
$y \sim x \wedge x \sim z \to y \sim z]$
$\Rightarrow y \sim x \wedge x \sim z \to y \sim z$
Mit Regel (Vor)

(32) $[x \sim ya$,
$y \sim ya$,
$y \sim x$,
$x \sim z$,
$\forall x.\, x \sim x$,
$\forall x.\, \forall y.\, x \sim y \to y \sim x$,
$y \sim x \wedge x \sim z \to y \sim z]$
$\Rightarrow y \sim x \wedge x \sim z$
Mit Regel ($\wedge$ S) aus (33) und (34)

(33) $[x \sim ya$,
$y \sim ya$,
$y \sim x$,
$x \sim z$,
$\forall x.\, x \sim x$,
$\forall x.\, \forall y.\, x \sim y \to y \sim x$,
$y \sim x \wedge x \sim z \to y \sim z]$
$\Rightarrow y \sim x$
Mit Regel (Vor)

(34) $[x \sim ya$,
$y \sim ya$,
$y \sim x$,
$x \sim z$,
$\forall x.\, x \sim x$,
$\forall x.\, \forall y.\, x \sim y \to y \sim x$,
$y \sim x \wedge x \sim z \to y \sim z]$
$\Rightarrow x \sim z$
Mit Regel (Vor)
Fertig!

3.5 Widerspruchsfreiheit (Konsistenz)

Bisher:
Wir haben bisher den semantischen Begriff der „logische Folgerung“ $\models$ und den syntaktischen Begriff der „Ableitbarkeit“ kennen gelernt und wissen bereits:

Aus $\Phi \vdash \varphi$ folgt $\Phi \models \varphi$ (Korrektheit des Kalküls)

Jetzt:
Zum semantischen Begriff „Erfüllbarkeit“ definieren wir einen entsprechenden syntaktischen Begriff „Widerspruchsfreiheit“. Das motiviert das nachstehende

Lemma 3.5.1 (Alternative Definition der Erfüllbarkeit). *Eine Formelmenge Φ ist erfüllbar $\Leftrightarrow$ es existiert keine Formel φ mit $\Phi \models \varphi$ und $\Phi \models \neg\varphi$ (d.h. wenn „false“ also* keine *logische Folgerung von Φ ist).*

Beweis. *Es sind zwei Richtungen zu zeigen:*

„$\Rightarrow$“: Wenn Φ erfüllbar ist, dann existiert ein $\mathcal{I}$ mit $\mathcal{I} \models \Phi$. Wäre nun φ eine Formel mit $\Phi \models \varphi$ und $\Phi \models \neg\varphi$, dann wäre $\mathcal{I} \models \varphi$ und $\mathcal{I} \models \neg\varphi$, also ein Widerspruch!

„$\Leftarrow$“: Wenn Φ unerfüllbar ist, dann existiert folglich kein $\mathcal{I}$ mit $\mathcal{I} \models \Phi$. Also sind alle Formeln logische Folgerungen von Φ

□

Definition 3.5.1. *Sei $\Phi \subseteq L^S$.*

(a) Φ heißt widerspruchsfrei *(oder:* konsistent*), wenn kein $\varphi \in L^S$ existiert mit $\Phi \vdash \varphi$ und $\Phi \vdash \neg\varphi$.*

(b) Φ heißt widerspruchsvoll*, wenn Φ nicht widerspruchsfrei ist, d.h. wenn ein $\varphi \in L^S$ existiert mit $\Phi \vdash \varphi$ und $\Phi \vdash \neg\varphi$.*

Bezeichnung 3.5.1. *Falls Φ widerspruchsfrei ist, schreibt man: Wf Φ. Man schreibt: Wv Φ, falls Φ widerspruchsvoll.*

Lemma 3.5.2. *Wv $\Phi \Leftrightarrow$ es existiert eine endliche Menge $\Phi_0 \subseteq \Phi$ mit Wv Φ_0.*

Beweis. *Es sind wieder zwei Richtungen zu zeigen:*

„$\Rightarrow$“:

$$\begin{aligned} \text{Wv } \Phi &\Rightarrow \text{es ex. ein } \varphi \text{ mit } \Phi \vdash \varphi \text{ und } \Phi \vdash \neg\varphi \\ &\Rightarrow \text{es existieren } \Gamma_1, \Gamma_2 \subseteq \Phi \text{ mit } \vdash \Gamma_1\, \varphi \text{ und } \vdash \Gamma_2 \neg\varphi \end{aligned}$$

Wir wählen nun $\Phi_0 = \Gamma_1 \cup \Gamma_2$. Dann gilt per Definition der Herleitbarkeit $\Phi_0 \vdash \varphi$ und $\Phi_0 \vdash \neg\varphi$ (da $\Gamma_1 \subseteq \Phi_0$ und $\Gamma_2 \subseteq \Phi_0$).

„$\Leftarrow$“: Klar, da jedes $\Gamma \subseteq \Phi_0$ auch Teilmenge von Φ ist.

□

Lemma 3.5.3. *Wenn Φ erfüllbar ist, dann ist Φ widerspruchsfrei (d.h., wenn Φ widerspruchsvoll ist, dann ist Φ unerfüllbar).*

Beweis.

$$\begin{aligned} Wv\ \Phi &\Rightarrow \text{es ex. ein } \varphi \text{ mit } \Phi \vdash \varphi \text{ und } \Phi \vdash \neg\varphi \\ &\overset{(*)}{\Rightarrow} \text{es existiert ein } \varphi \text{ mit } \Phi \models \varphi \text{ und } \Phi \models \neg\varphi \\ &\overset{(**)}{\Rightarrow} \Phi \text{ ist unerfüllbar} \end{aligned}$$

□

Bemerkung 3.5.1. *Im obigen Beweis gilt (*) wegen der Korrektheit des Kalküls, (**) wegen Lemma 3.5.1 (S.42). Wir werden später noch beweisen, daß die Umkehrung des letzen Lemmas gilt, d.h.: Wf* $\Phi \Rightarrow \Phi$ *erfüllbar bzw.* Φ *unerfüllbar* $\Rightarrow Wv\ \Phi$*. Jetzt zeigen wir, daß daraus die Vollständigkeit des Kalküls folgt.*

Zunächst aber:
Einige Eigenschaften von „$\models$“ werden auf „$\vdash$“ übertragen. Dazu das nachstehende

Lemma 3.5.4. $Wv\ \Phi \Leftrightarrow$ *für alle* $\varphi \in L^S$ *gilt:* $\Phi \vdash \varphi$

Beweis. *Es ist wieder eine Äquivalenz zu zeigen:*

„$\Leftarrow$“*: Aus der rechten Seite folgt sogar die stärkere Behauptung:* $\Phi \vdash \varphi$ *und* $\Phi \vdash \neg\varphi$ *für alle* $\varphi \in L^S$

„$\Rightarrow$“*: Die Behauptung gilt wegen der Widerspruchsregel:*

$$\begin{aligned} Wv\ \Phi &\Rightarrow \text{es existiert ein } \psi \in L^S \text{ mit } \Phi \vdash \psi \text{ und } \Phi \vdash \neg\psi \\ &\Rightarrow \text{es existieren } \Gamma_1, \Gamma_2 \subseteq \Phi \text{ mit } \vdash \Gamma_1\ \psi \text{ und } \vdash \Gamma_2\ \neg\psi \end{aligned}$$

Man wähle $\Gamma = \Gamma_1\ \Gamma_2$*. Dann folgt jeweils mit der Regel (Ant):*

$$\vdash \Gamma\ \psi \text{ und } \vdash \Gamma\ \neg\psi$$

Daraus folgt mit (Wid'):

$$\vdash \Gamma\ \varphi \text{ für jedes } \varphi \in L^S\text{, also } \Phi \vdash \varphi \text{ für jedes } \varphi \in L^S$$

□

Lemma 3.5.5. *Sei* $\Phi \subseteq L^S$, $\varphi \in L^S$*. Dann gilt:*

(a) $\Phi \vdash \varphi \Leftrightarrow Wv\ (\Phi \cup \{\neg\varphi\})$

(b) $\Phi \vdash \neg\varphi \Leftrightarrow Wv\ (\Phi \cup \{\varphi\})$

(c) Wenn $Wf\,\Phi$*, dann ist (mindestens) eine der Mengen* $\Phi \cup \{\varphi\}$ *oder* $\Phi \cup \{\neg\varphi\}$ *widerspruchsfrei.*

Beweis.

(a) Zwei Richtungen sind zu zeigen:

„⇒“: Wenn $\Phi \vdash \varphi$*, dann gilt auch* $\Phi \cup \{\neg\varphi\} \vdash \varphi$*. Außerdem gilt* $\Phi \cup \{\neg\varphi\} \vdash \neg\varphi$ *wegen (Vor).*

„⇐“: Wenn Wv $(\Phi \cup \{\neg\varphi\})$*, dann gilt nach vorigem Lemma insbesondere* $\Phi \cup \{\neg\varphi\} \vdash \varphi$*, d.h. es existiert* $\Gamma \subseteq \Phi \cup \{\neg\varphi\}$ *mit* $\vdash \Gamma\, \varphi$*. Wegen der Regel (Ant) dürfen wir annehmen, daß* Γ *von der Form* $\Gamma_1\, \neg\varphi$ *ist mit* $\Gamma_1 \subseteq \Phi$*. Also:*

$$\vdash \Gamma_1\, \neg\varphi\, \varphi \text{ und wegen (Vor) gilt auch:}$$
$$\vdash \Gamma_1\, \varphi\, \varphi\text{. Mit Regel (FU) folgt dann daraus:}$$
$$\vdash \Gamma_1\, \varphi\text{, also } \Phi \vdash \varphi$$

(b) Analog zu (a): Man vertauscht die Rollen von φ *und* $\neg\varphi$*.*

(c) Wären $\Phi \cup \{\varphi\}$ *und* $\Phi \cup \{\neg\varphi\}$ *widerspruchsvoll, dann wäre nach (a) und (b):* $\Phi \vdash \varphi$ *und* $\Phi \vdash \neg\varphi$*, also Wv* Φ*.*

□

Lemma 3.5.6. *Zum Beweis der* Vollständigkeit des Kalküls *genügt es zu zeigen:*
Wf $\Phi \Rightarrow \Phi$ *erfüllbar.*

Beweis.

$$\begin{aligned} \Phi \models \varphi \quad &\Rightarrow \quad \Phi \cup \{\neg\varphi\} \text{ unerfüllbar} \\ &\overset{oben}{\Rightarrow} \quad Wv\ (\Phi \cup \{\neg\varphi\}) \\ &\Rightarrow \quad \Phi \vdash \varphi \end{aligned}$$

□

Bemerkung 3.5.2. *Im obigen Beweis kann die erste und letzte Implikation durch eine Äquivalenz ersetzt werden. Die erste wegen Kapitel 2, die letzte wegen vorigem Lemma.*

Kapitel 4

Die Vollständigkeit des Sequenzenkalküls

„Die Mathematik allein befriedigt den Geist durch ihre außerordentliche Gewißheit.“
JOHANNES KEPLER (1571-1630)

Zu zeigen ist: „Jede widerspruchsfreie Menge $\Phi \subseteq L^S$ besitzt ein Modell“. Nun stellt sich aber die Frage: „Wo nimmt man ein Modell für eine beliebige Menge Φ her?“
Idee: Man wählt eine Struktur, deren Trägermenge aus (Äquivalenzklassen von) Termen besteht, also aus „syntaktischen Objekten“.

4.1 Der Satz von Henkin

Sei S eine Signatur, $\Phi \subseteq L^S$. Auf der Menge T^S aller Terme über S definieren wir eine Relation $\sim_\Phi$ (hängt von Φ ab) durch:

$$t_1 \sim_\Phi t_2 :\Leftrightarrow \Phi \vdash t_1 \equiv t_2$$

Lemma 4.1.1. *(a) $\sim_\Phi$ ist eine Äquivalenzrelation*

(b) $\sim_\Phi$ ist mit Funktions- und Relationszeichen verträglich, d.h.

- *für jedes $f \in F_n$ gilt: Wenn $t_1 \sim_\Phi t'_1, \ldots, t_n \sim_\Phi t'_n$, dann gilt: $f(t_1, \ldots, t_n) \sim_\Phi f(t'_1, \ldots, t'_n)$*
- *für jedes $r \in R_n$ gilt: Wenn $t_1 \sim_\Phi t'_1, \ldots, t_n \sim_\Phi t'_n$, dann gilt: $\Phi \vdash r(t_1, \ldots, t_n) \Leftrightarrow \Phi \vdash r(t'_1, \ldots, t'_n)$*

Beweis.

(a) folgt sofort aus den Regeln (Refl), (Symm) und (Trans) des Kalküls, z.B.: Wenn $t_1 \sim_\Phi t_2$, dann gilt: $\Phi \vdash t_1 \equiv t_2$, also auch: $\Phi \vdash t_2 \equiv t_1$ wegen (Symm), d.h. $t_2 \sim_\Phi t_1$.

(b) folgt aus den Regeln (Fkt) und (Rel), z.B.: Wenn $t_1 \sim_\Phi t'_1, \ldots$, *dann gilt* $\Phi \vdash t_1 \equiv t'_1, \ldots$. *Wenn dann zusätzlich* $\Phi \vdash r(t_1, \ldots, t_n)$ *gilt, so folgt* $\Phi \vdash r(t'_1, \ldots, t'_n)$ *mit Regel (Rel), also ist damit die Richtung „⇒“ bewiesen. Wenn umgekehrt* $\Phi \vdash r(t'_1, \ldots, t'_n)$ *gilt, so folgt* $\Phi \vdash r(t_1, \ldots, t_n)$ *durch n-fache Anwendung von (Symm) und Regel (Rel).*

□

Definition 4.1.1 (Termstruktur). *Sei* $\Phi \subseteq L^S$. *Die* Termstruktur $\mathcal{T}^\Phi = (T^\Phi, \tau^\Phi)$ *ist definiert durch:*

- $T^\Phi =_{\text{def}} T^S / \sim_\Phi$ *(Menge aller* $\sim_\Phi$*-Äquivalenzklassen von Termen aus* T^S*). Schreibweise:* $\overline{t}$ *ist die Äquivalenzklasse von* t
- $C^{\mathcal{T}^\Phi} =_{\text{def}} \overline{c}$ *für jedes* $c \in C$
- *Für jedes* $f \in F_n$ *sei* $f^{\mathcal{T}^\Phi} : (T^\Phi)^n \longrightarrow T^\Phi$, $f^{\mathcal{T}^\Phi}(\overline{t_1}, \ldots, \overline{t_n}) =_{\text{def}} \overline{f(t_1, \ldots, t_n)}$
- *Für jedes* $r \in R_n$ *sei* $r^{\mathcal{T}^\Phi} \subseteq (T^\Phi)^n$ *definiert durch:* $(\overline{t_1}, \ldots, \overline{t_n}) \in r^{\mathcal{T}^\Phi} :\Leftrightarrow \Phi \vdash r(t_1, \ldots, t_n)$

Bemerkung 4.1.1. *Wegen Lemma 4.1.1b sind die Funktionen* $f^{\mathcal{T}^\Phi}$ *und die Relationen* $r^{\mathcal{T}^\Phi}$ *wohldefiniert, d.h. ihr Ergebnis ist unabhängig von der Wahl der speziellen Repräsentanten* $t_1, \ldots, t_n$.

Beispiel 4.1.1. *Sei* $S = \{0, \text{succ}\}$. *Sei* $\Phi = \{v_i \equiv 0 \mid i \in \mathbb{N}\}$. *Für die Menge der Terme über S gilt dann:* $T^S = \{\text{succ}^n(0) \mid n \in \mathbb{N}\} \cup \{\text{succ}^n(v_i) \mid n \in \mathbb{N}, i \in \mathbb{N}\}$. *Es gilt* $v_i \sim_\Phi 0$ *für alle* $i \in \mathbb{N}$, *also auch* $\text{succ}^n(v_i) \sim_\Phi \text{succ}^n(0)$ *für alle* $i \in \mathbb{N}, n \in \mathbb{N}$. *Also gilt:* $T^\Phi = \{\overline{\text{succ}^n(0)} \mid n \in \mathbb{N}\}$ *und*

$$\begin{aligned} 0^{\mathcal{T}^\Phi} &= \overline{0} \\ \text{succ}^{\mathcal{T}^\Phi} &: T^\Phi \longrightarrow T^\Phi \\ \text{succ}^{\mathcal{T}^\Phi}(\overline{\text{succ}^n(0)}) &= \overline{\text{succ}(\text{succ}^n(0))} \\ &= \overline{\text{succ}^{n+1}(0)} \end{aligned}$$

Also ist $\mathcal{T}^\Phi$ *von der Form:*

$$\overline{0} \;\rightarrow\; \overline{\text{succ}(0)} \;\rightarrow\; \overline{\text{succ}^2(0)} \;\rightarrow\; \ldots \;\rightarrow\; \overline{\text{succ}^n(0)}$$

D.h., $\mathcal{T}^\Phi$ *ist isomorph zur Struktur der natürlichen Zahlen mit Nachfolgerfunktion.*

Definition 4.1.2. *Die zu* Φ gehörige Belegung $\beta^\Phi : X \longrightarrow T^\Phi$ *sei definiert durch:*

$$\beta^\Phi(x) =_{\text{def}} \overline{x} \text{ für jedes } x \in X$$

und die zu Φ gehörige Interpretation $\mathcal{I}^\Phi$ *durch:*

$$\mathcal{I}^\Phi =_{\text{def}} (\mathcal{T}^\Phi, \beta^\Phi)$$

Beispiel 4.1.2. *Seien S und Φ wie im letzten Beispiel vorgegeben. Dann ist $\beta^\Phi(v_i) = \overline{v_i} = \overline{0}$ für alle $i \in \mathbb{N}$. In diesem Beispiel gilt also $\mathcal{I}^\Phi \models \Phi$ (weil ja $\beta^\Phi(v_i) = \overline{0} = 0^{\mathcal{T}^\Phi}$)*

Lemma 4.1.2. *(a) Für alle $t \in T^S$ gilt $\mathcal{I}^\Phi(t) = \bar{t}$.*

(b) Für alle atomaren *Formeln $\varphi \in L^S$ gilt: $\mathcal{I}^\Phi \models \varphi \Leftrightarrow \Phi \vdash \varphi$*

(c) Für alle $\varphi \in L^S$ und alle $x_1, \ldots, x_n \in X$, die paarweise verschieden sind, gilt:

(i) $\mathcal{I}^\Phi \models \exists x_1, \ldots, x_n . \varphi \Leftrightarrow$ es existieren $t_1, \ldots, t_n \in T^S$ mit $\mathcal{I}^\Phi \models \varphi[t_1, \ldots, t_n / x_1, \ldots, x_n]$

(ii) $\mathcal{I}^\Phi \models \forall x_1, \ldots, x_n . \varphi \Leftrightarrow$ für alle $t_1, \ldots, t_n \in T^S$ gilt: $\mathcal{I}^\Phi \models \varphi[t_1, \ldots, t_n / x_1, \ldots, x_n]$

Beweis.

(a) Ist klar, wegen $\mathcal{I}^\Phi(c) = \overline{c}$, $\mathcal{I}^\Phi(x) = \beta^\Phi(x) = \overline{x}$ und

$$\begin{array}{rcl} \mathcal{I}^\Phi(f(t_1, \ldots, t_n)) & \overset{Semantik}{=} & f^{\mathcal{T}^\Phi}(\mathcal{I}^\Phi(t_1), \ldots, \mathcal{I}^\Phi(t_n)) \\ & \overset{I.A.}{=} & f^{\mathcal{T}^\Phi}(\overline{t_1}, \ldots, \overline{t_n}) \\ & \overset{\mathcal{T}^\Phi}{=} & \overline{f(t_1, \ldots, t_n)} \end{array}$$

(b) Es gilt:

$$\begin{array}{rcl} \mathcal{I}^\Phi \models t_1 \equiv t_2 & \overset{Semantik}{\Leftrightarrow} & \mathcal{I}^\Phi(t_1) = \mathcal{I}^\Phi(t_2) \\ & \overset{I.A.}{\Leftrightarrow} & \overline{t_1} = \overline{t_2} \\ & \Leftrightarrow & t_1 \sim_\Phi t_2 \\ & \overset{\sim}{\Leftrightarrow}^\Phi & \Phi \vdash t_1 \equiv t_2 \end{array}$$

Ferner gilt:

$$\begin{array}{rcl} \mathcal{I}^\Phi \models r(t_1, \ldots, t_n) & \overset{Semantik}{\Leftrightarrow} & (\mathcal{I}^\Phi(t_1), \ldots, \mathcal{I}^\Phi(t_n)) \in r^{\mathcal{T}^\Phi} \\ & \overset{I.A.}{\Leftrightarrow} & (\overline{t_1}, \ldots, \overline{t_n}) \in r^{\mathcal{T}^\Phi} \\ & \overset{\mathcal{T}^\Phi}{\Leftrightarrow} & \Phi \vdash r(t_1, \ldots, t_n) \end{array}$$

(c) Es gilt:

$$\begin{array}{rcll} \mathcal{I}^\Phi \models \exists x_1, \ldots, x_n . \varphi & \overset{Semantik}{\Leftrightarrow} & \text{es ex. } \overline{t_1}, \ldots, \overline{t_n} \in \mathcal{T}^\Phi \text{ mit } \mathcal{I}[\overline{t_1}/x_1] \ldots [\overline{t_n}/x_n] \models \varphi & \\ & \Leftrightarrow & \text{es ex. } t_1, \ldots, t_n \in T^S \text{ mit } \underbrace{\underbrace{\mathcal{I}[\overline{t_1}/x_1]}_{=\mathcal{I}^\Phi(t_1)} \ldots \underbrace{[\overline{t_n}/x_n]}_{=\mathcal{I}^\Phi(t_n)} \models \varphi}_{\text{d.h. } \mathcal{I} \models \varphi[t_1, \ldots, t_n / x_1, \ldots, x_n] \text{ nach Lemma 2.5.1}} & \end{array}$$

Analog zeigt man dies für den Allquantor.

□

Bemerkung 4.1.2. *Wegen (b) gilt insbesondere $\mathcal{I}^\Phi \models \varphi$ für alle atomaren Formeln $\varphi \in \Phi$ (d.h. insbesondere gilt: jede Menge Φ, die nur aus atomaren Formeln besteht, besitzt ein Modell). Aber für nicht atomare Formeln gilt dies im Allgemeinen nicht, z.B.: Sei $S = \{r\}$, r einstelliges Relationszeichen. Sei $\Phi = \{\exists x.\, r(x)\}$. Dann gilt nach dem Lemma:*

$$\begin{aligned} \mathcal{I}^\Phi \models \exists x.\, r(x) &\overset{(c)}{\Leftrightarrow} \text{ es ex. ein } t \in T^S \text{ mit } \mathcal{I}^\Phi \models r(t) \\ &\overset{(a)}{\Leftrightarrow} \Phi \vdash r(t) \end{aligned}$$

Da S weder Konstanten noch Funktionszeichen enthält, kann der Term t folglich nur eine Variable y sein, d.h. es müßte $\Phi \vdash r(y)$ gelten, also auch $\Phi \models r(y)$ wegen der Korrektheit des Kalküls. Das gilt nicht, man wähle z.B.: $\mathcal{A} = \{\{0,1\}, r^{\mathcal{A}})$ mit $r^{\mathcal{A}} = \{0\}$ und $\beta : X \longrightarrow \{0,1\}$ mit $\beta(y) = 1$. Dann gilt nämlich: $\mathcal{A}, \beta \models \exists x.\, r(x)$, weil $0 \in r^{\mathcal{A}}$, aber $\mathcal{A}, \beta \not\models r(y)$, da $\beta(y) = 1 \notin r^{\mathcal{A}}$.

Bisher:
$\mathcal{I}^\Phi$ erfüllt alle atomaren Formeln aus Φ, aber nicht unbedingt alle Formeln.

Jetzt:
Wenn Φ „groß genug“ ist, d.h. wenn „genügend viele“ Formeln aus Φ ableitbar sind, dann gilt: $\mathcal{I}^\Phi \models \Phi$. Das motiviert die folgende

Definition 4.1.3. *Sei $\Phi \subseteq L^S$ beliebige Formelmenge.*

(a) Φ *heißt* negationstreu, *wenn für jedes $\varphi \in L^S$ gilt:*

$$\Phi \vdash \varphi \text{ oder } \Phi \vdash \neg\varphi$$

(b) Φ enthält Beispiele, *wenn für jede Formel der Form $\exists x.\, \varphi$ ein Term t existiert mit*

$$\Phi \vdash (\exists x.\, \varphi) \to \varphi[t/x]$$

Bemerkung 4.1.3. *Die Menge $\Phi = \{\exists x.\, r(x)\}$ aus unserem Beispiel war weder negationstreu noch enthielt sie Beispiele.*

Lemma 4.1.3. *Sei $\Phi \subseteq L^S$ widerspruchsfrei. Wenn Φ negationstreu ist und Beispiele enthält, dann gilt:*

(a) Entweder $\Phi \vdash \varphi$ oder $\Phi \vdash \neg\varphi$

(b) $\Phi \vdash \varphi \vee \psi \Leftrightarrow \Phi \vdash \varphi$ oder $\Phi \vdash \psi$

(c) $\Phi \vdash \exists x.\, \varphi \Leftrightarrow$ es existiert ein $t \in T^S$ mit $\Phi \vdash \varphi[t/x]$

Beweis.

(a) folgt sofort aus der Negationstreue und Widerspruchsfreiheit

(b) Zwei Richtungen sind zu zeigen:

„⇐“: gilt wegen der beiden ($\vee$ S)-Regeln

„⇒“: Es gelte $\Phi \vdash \varphi \vee \psi$. Wenn $\Phi \nvdash \varphi$, dann gilt wegen Teil (a) $\Phi \vdash \neg\varphi$, also folgt mit der Regel (MP'): $\Phi \vdash \psi$.

(c) Wieder ist eine Äquivalenz zu zeigen:

„⇐“: gilt wegen der Regel ($\exists$ S)

„⇒“: Es gelte $\Phi \vdash \exists x.\, \varphi$. Da Φ Beispiele enthält, gibt es einen Term t mit $\Phi \vdash (\exists x.\, \varphi) \to \varphi[t/x]$. Also folgt mit der Regel (MP): $\Phi \vdash \varphi[t/x]$

□

Satz 4.1.1 (Satz von Henkin). *Sei $\Phi \subseteq L^S$ widerspruchsfrei. Wenn Φ negationstreu ist und Beispiele enthält, dann gilt für alle Formeln $\varphi \in L^S$:*

$$\mathcal{I}^\Phi \models \varphi \Leftrightarrow \Phi \vdash \varphi$$

(Insbesondere gilt $\mathcal{I}^\Phi \models \varphi$ für alle $\varphi \in \Phi$, also $\mathcal{I}^\Phi \models \Phi$).

Beweis. *Induktion über die Anzahl n der Junktoren und Quantoren:*
$\underline{n = 0}$: Dann ist φ atomar, also gilt die Äquivalenz nach Lemma 4.1.2(b).
$\underline{n > 0}$: Fallunterscheidung nach der Form von φ

$\underline{\varphi = \neg\psi}$:

$$\begin{aligned} \mathcal{I}^\Phi \models \neg\psi \quad &\overset{\text{Semantik}}{\Leftrightarrow} \quad \mathcal{I}^\Phi \not\models \psi \\ &\overset{\text{I.A.}}{\Leftrightarrow} \quad \Phi \nvdash \psi \\ &\overset{\text{Lemma 4.1.3a}}{\Leftrightarrow} \quad \Phi \vdash \neg\psi \end{aligned}$$

$\underline{\varphi = \psi \vee \chi}$:

$$\begin{aligned} \mathcal{I}^\Phi \models \psi \vee \chi \quad &\overset{\text{Semantik}}{\Leftrightarrow} \quad \mathcal{I}^\Phi \models \psi \text{ oder } \mathcal{I}^\Phi \models \chi \\ &\overset{\text{I.A.}}{\Leftrightarrow} \quad \Phi \vdash \psi \text{ oder } \Phi \vdash \chi \\ &\overset{\text{Lemma 4.1.3b}}{\Leftrightarrow} \quad \Phi \vdash \psi \vee \chi \end{aligned}$$

$\underline{\varphi = \exists x.\, \psi}$:

$$\begin{aligned} \mathcal{I}^\Phi \models \exists x.\, \psi \quad &\overset{\text{Lemma 4.1.2c}}{\Leftrightarrow} \quad \text{es ex. ein } t \in T^S \text{ mit } \mathcal{I}^\Phi \models \psi[t/x] \\ &\overset{\text{I.A.}}{\Leftrightarrow} \quad \text{es ex. ein } t \in T^S \text{ mit } \Phi \vdash \psi[t/x] \\ &\overset{\text{Lemma 4.1.3c}}{\Leftrightarrow} \quad \Phi \vdash \exists x.\, \varphi \end{aligned}$$

□

Bemerkung 4.1.4. *Die Induktionsannahme im letzten Falle des Beweises ist gerechtfertigt, da $\psi[t/x]$ einen Quantor weniger enthält als $\exists x.\, \varphi$, jedoch die gleiche Anzahl von Junktoren besitzt.*

4.2 Erfüllbarkeit abzählbarer widerspruchsfreier Formelmengen

Idee: Jede widerspruchsfreie Menge Φ läßt sich zu einer Menge Φ^* vergrößern, auf die der *Satz 4.1.1 von Henkin* (S.49) anwendbar ist. $\rightsquigarrow \mathcal{I}^{\Phi^*}$ ist ein Modell von Φ^*, und damit erst recht ein Modell von Φ (wegen $\Phi \subseteq \Phi^*$).

Zunächst wird vorausgesetzt: Φ abzählbar (also endlich oder abzählbar unendlich) und frei(Φ) endlich. Dann dürfen wir annehmen, daß S abzählbar ist.

Lemma 4.2.1. *Sei S abzählbar, $\Phi \subseteq L^S$ widerspruchsfrei mit frei(Φ) endlich. Dann existiert eine widerspruchsfreie Menge $\Psi \subseteq L^S$ mit $\Phi \subseteq \Psi$ und Ψ enthält Beispiele.*

Beweis. *Idee: Da frei(Φ) endlich ist, findet man stets eine Variable, die noch nicht frei vorkommt. Diese Variable kann man als „Beispiel" benutzen.*
Genauer: Da S abzählbar, ist L^S abzählbar unendlich, also ist auch die Menge aller Formeln der Form $(\exists x.\, \varphi) \in L^S$ abzählbar unendlich:

$$\exists x_0.\, \varphi_0, \exists x_1.\, \varphi_1, \ldots$$

Durch Induktion über n definieren wir eine Formelmenge Φ_n mit frei(Φ_n) endlich wie folgt:

$$\Phi_0 =_{\text{def}} \Phi$$
$$\Phi_{n+1} =_{\text{def}} \Phi_n \cup \{(\exists x_n.\, \varphi_n) \to \varphi_n[y_n/x_n]\},$$

wobei $y_n \notin$ frei(Φ_n) $\cup$ frei($\exists x_n.\, \varphi_n$). Man beachte: da frei(Φ_0) endlich ist, und in jedem Schritt nur eine Formel hinzukommt, ist frei(Φ_n) endlich für jedes n, also ex. ein solches y_n im Induktionsschritt. Zudem gilt:

$$\Phi = \Phi_0 \subseteq \Phi_1 \subseteq \Phi_2 \subseteq \ldots$$

und wir definieren:

$$\Psi =_{\text{def}} \bigcup_{n \in \mathbb{N}} \Phi_n$$

Ψ enthält Beispiele, denn jede Formel $\exists x.\, \varphi$ kommt ja unter den $\exists x_n.\, \varphi_n$ vor, und Φ_{n+1} enthält dann ein zugehöriges Beispiel $(\exists x.\, \varphi_n) \to \varphi_n[y_n/x_n]$, also enthält auch Ψ dieses Beispiel.

Noch zu zeigen: Ψ ist widerspruchsfrei.
Angenommen, Ψ wäre widerspruchsvoll. Dann existiert bereits eine endliche Teilmenge $\Psi' \subseteq \Psi$, die widerspruchsvoll ist. Dann existiert ein $n \in \mathbb{N}$ mit $\Psi' \subseteq \Phi_n$, also ist bereits ein Φ_n widerspruchsvoll. Wir wählen n minimal mit Φ_n widerspruchsvoll ($\rightsquigarrow n \neq 0$ nach Voraussetzung), also ist Φ_{n-1} widerspruchsfrei.

$$\Phi_0 = \Phi$$

$$\Phi_{n+1} = \Phi_n \cup \{(\exists x_n.\, \varphi) \to \varphi[y_n/x_n]\},$$

wobei y_n *„neu“, d.h.* $y_n \notin$ *frei*$(\Phi_n \cup \{\exists x_n.\, \varphi_n\})$

$$\Psi = \bigcup_{n\in\mathbb{N}} \Phi_n$$

Noch zu zeigen: Wenn Φ_{n+1} *widerspruchsvoll ist, dann ist bereits* Φ_n *widerspruchsvoll. Dazu genügt es zu zeigen: jede (abgeschlossene) Formel* ψ*, die aus* Φ_{n+1} *ableitbar ist, ist bereits aus* Φ_n *ableitbar.*

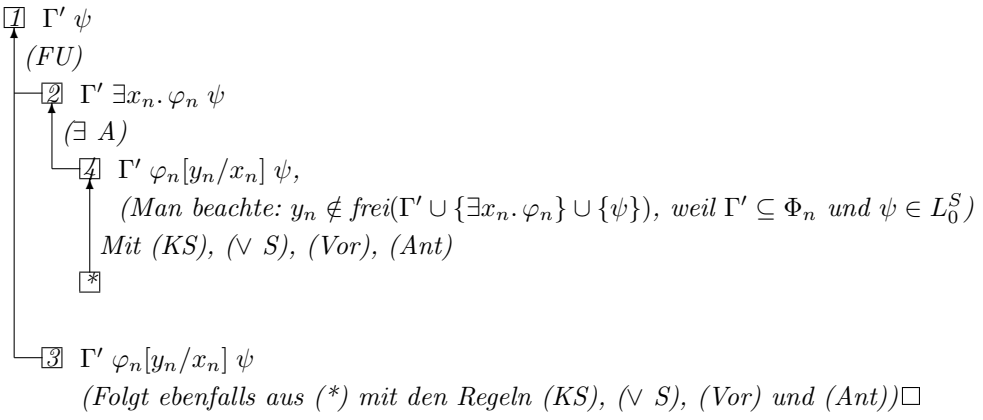
Sei also $\psi \in L_0^S$ *mit* $\Phi_{n+1} \vdash \psi$*. Dann existiert eine endliche Folge* $\Gamma \subseteq \Phi_{n+1}$ *mit* $\vdash \Gamma\psi$*. Wir dürfen annehmen (wegen der Regel (Ant)), daß* Γ *von der Form* $\Gamma'\ \neg(\exists x_n.\, \varphi_n) \vee \varphi_n[y_n/x_n]$ *ist, wobei* $\Gamma' \subseteq \Phi_n$*. Also gilt:*

$$\Gamma'\ \neg(\exists x_n.\, \varphi_n) \vee \varphi_n[y_n/x_n]\ \psi \quad (*)$$

und es genügt zu zeigen, daß hieraus $\vdash \Gamma'\psi$ *folgt.*

Intuition: Da y_n *„neu“ ist, bedeutet die Formel* $\varphi_n[y_n/x_n]$ *nur, daß ein Element* y_n *existiert, das die Eigenschaft* φ_n *hat, d.h. sie ist „gleichwertig“ zur Existenzaussage* $\exists x_n.\, \varphi_n$ *(das hieße: Tautologie* $\to$ *Antezendensregel)*

Ableitung: z.zg.:



Lemma 4.2.2. *Sei* S *abzählbar. Sei* $\Psi \subseteq L^S$ *widerspruchsfrei. Dann existiert eine widerspruchsfreie Menge* $\Theta \subseteq L^S$ *mit* $\Psi \subseteq \Theta$ *und* Θ *ist negationstreu.*

Beweis. *Sei* $\varphi_0, \varphi_1, \ldots$ *eine Abzählung aller Formeln aus* L^S*. Durch Induktion über* n *definieren wir* Θ_n *wie folgt:*

$$\Theta_0 =_{\text{def}} \Psi$$

$$\Theta_{n+1} =_{\text{def}} \begin{cases} \Theta_n \cup \{\varphi_n\}, & \textit{falls } \Theta_n \cup \{\varphi_n\} \textit{ widerspruchsfrei} \\ \Theta_n, & \textit{sonst} \end{cases}$$

$$\textit{und } \Theta =_{\text{def}} \bigcup_{n\in\mathbb{N}} \Theta_n$$

Es ist klar, daß alle Θ_n widerspruchsfrei sind (per induktiver Definition). Also ist auch Θ widerspruchsfrei. (Hinweis: die Widerspruchsfreiheit von $\Theta_n \cup \{\varphi_n\}$ in der obigen Definition ist nicht unbedingt entscheidbar; es handelt sich hier lediglich um eine mathematische Definition.)

Noch zu zeigen: Θ ist negationstreu.
Sei also $\varphi \in L^S$. Dann existiert ein n mit $\varphi = \varphi_n$. Wenn $\Theta \nvdash \neg\varphi_n$, dann gilt nach Lemma 3.5.5b (S.43): $\Theta \cup \{\varphi_n\}$ ist widerspruchsfrei, also erst recht ist $\Theta_n \cup \{\varphi_n\}$ widerspruchsfrei, also $\Theta_{n+1} = \Theta_n \cup \{\varphi_n\}$ und damit $\varphi_n \in \Theta_{n+1} \subseteq \Theta$, also $\Theta \vdash \varphi_n$ □

Korollar 4.2.1. *Sei S abzählbar, $\Phi \subseteq L^S$ widerspruchsfrei mit frei(Φ) endlich. Dann ist Φ erfüllbar (mit einer Termstruktur $\mathcal{I}^\Theta$, wobei $\Phi \subseteq \Theta \subseteq L^S$).*

Beweis. *Nach Lemma 4.2.1 (S.50) existiert ein Ψ mit $\Phi \subseteq \Psi \subseteq L^S$ und Ψ enthält Beispiele. Nach Lemma 4.2.2 existiert ein Θ mit $\Psi \subseteq \Theta \subseteq L^S$ und Θ negationstreu (Θ und Ψ widerspruchsfrei). Da Θ über der gleichen Signatur gebildet ist wie Ψ, enthält auch Θ Beispiele. Also ist der* Satz 4.1.1 von Henkin *(S.49) auf Θ anwendbar, d.h. $\mathcal{I}^\Theta$ ist ein Modell von Θ und damit auch von Φ.* □
Unser Ziel ist es jetzt, die Voraussetzung „frei(Φ) endlich“ loszuwerden. Das führt unmittelbar zu dem

Satz 4.2.1. *Sei S abzählbar und $\Phi \subseteq L^S$ widerspruchsfrei. Dann ist Φ erfüllbar (mit einer Termstruktur $\mathcal{I}^\Theta$, wobei $\Theta \subseteq L^{S'}$ für eine abzählbare Struktur $S' \supseteq S$.)*

Beweis. *Idee: Die Rolle der Variablen y_n (die im Beweis von Lemma 4.2.1) gewählt wurden), wird jetzt von neuen Konstanten c_n übernommen.*
Sei

$$S' = S \cup \{c_0, c_1, \ldots\},$$

wobei $c_0, c_1, \ldots$ abzählbar viele Konstanten sind, die nicht in S liegen. Für jedes $\varphi \in L^S$ sei $\varphi' \in L^{S'}$ die Formel, die aus φ entsteht, indem man jede freie Variable v_i durch die Konstante c_i ersetzt. Sei

$$\Phi' =_{\text{def}} \{\varphi' \mid \varphi \in \Phi\}.$$

Es ist $\Phi' \subseteq L^S$ und frei(Φ') $= \emptyset$. Wenn wir zeigen könnnen, daß Φ' widerspruchsfrei ist, dann folgt nach dem Korollar, daß Φ' ein Termmodell $\mathcal{I}^\Theta$ besitzt mit $\Phi' \subseteq \Theta \subseteq L^{S'}$. Da frei($\Phi'$) $= \emptyset$, kommt es in $\mathcal{I}^\Theta$ nicht auf die Belegung an, d.h. wir dürfen annehmen, daß

$$\mathcal{I}^\Theta(v_i) = \mathcal{I}^\Theta(c_i)$$

für alle $i \in \mathbb{N}$ gilt. Dann gilt aber nach dem Substitutionslemma $\mathcal{I}^\Theta(\varphi) = \mathcal{I}(\varphi')$, also wegen $\mathcal{I}^\Theta \models \Phi'$ auch $\mathcal{I}^\Theta \models \Phi$ (genauer: anstelle von $\mathcal{I}^\Theta$ müßte hier die

Einschränkung von $\mathcal{I}^\Theta$ auf die Signatur S stehen). Es bleibt zu zeigen: Φ' widerspruchsfrei.
Dazu genügt wieder: Jede endliche Teilmenge von Φ' ist erfüllbar (wegen Satz 3.3.1, S. 31).
Sei $\Phi'_0 = \{\varphi'_1, \ldots, \varphi'_n\}$ eine solche endliche Teilmenge. Sei $\Phi_0 = \{\varphi_1, \ldots, \varphi_n\}$ (die Menge, aus der Φ'_0 enstanden ist). Wegen $\Phi_0 \subseteq \Phi$ ist Φ_0 widerspruchsfrei, und frei(Φ_0) ist endlich. Nach dem Korollar ist Φ_0 erfüllbar, d.h. es existiert ein Modell $\mathcal{I} = (\mathcal{A}, \beta)$ von Φ_0. Wir erweitern $\mathcal{I}$ zu einer Interpretation $\mathcal{I}' = (\mathcal{A}', \beta')$ über S' durch: $\underbrace{c_i^{\mathcal{A}}}_{=\mathcal{I}(c_i)} =_{\text{def}} \underbrace{\beta(v_i)}_{=\mathcal{I}(v_i)}$.
Nach dem Substitutionslemma ist klar, daß $\mathcal{I}'(\varphi'_k) = \mathcal{I}(\varphi_k)$ für $k = 1, \ldots, m$, also ist $\mathcal{I}'$ Modell von Φ'_0. □
Wir haben bewiesen:

Satz 4.2.2 (Vollständigkeit des Sequenzenkalküls). *Sei S abzählbar, $\Phi \subseteq L^S$, $\varphi \in L^S$. Dann gilt:*

(a) $\Phi \models \varphi \Rightarrow \Phi \vdash \varphi$

(b) Φ *widerspruchsfrei* $\Rightarrow \Phi$ *erfüllbar*

Bemerkung 4.2.1. *In Teil (a) und (b) des Satzes 4.2.1 kann man die Implikation durch eine Äquivalenz ersetzen; die Rückrichtung wurde ja bereits mit der Korrektheit des Kalküls gezeigt.*

Satz 4.2.2 gilt sogar für beliebige Signaturen S, aber der Beweis ist schwieriger: anstelle von Induktion (für die abzählbar vielen Formeln $\varphi_1, \varphi_2, \ldots$) benötigt man das Zornsche *Lemma (Auswahlaxiom:* „Jede induktiv geordnete Menge besitzt maximale Elemente“*).*

Kapitel 5

Grenzen der Ausdruckskraft der Prädikatenlogik erster Stufe

„Die Grenzen meiner Sprache sind die Grenzen meiner Welt."
Ludwig (Joseph Johann) Wittgenstein (1859-1951)

Nach dem Vollständigkeitssatz (S.53) im letzten Kapitel können wir Eigenschaften der syntaktischen Begriffe „Ableitbarkeit", „Widerspruchsfreiheit" auf die semantischen Begriffe „logische Folgerung", „Erfüllbarkeit" übertragen. Das führt zum sogenannten Kompaktheitssatz.

5.1 Der Kompaktheitssatz

Satz 5.1.1 (Endlichkeitssatz oder Kompaktheitssatz). *Sei S eine Signatur, $\Phi \subseteq L^S$ und $\varphi \in L^S$. Dann gilt:*

(a) $\Phi \models \varphi \Leftrightarrow$ *es existiert eine endliche Menge* $\Phi_0 \subseteq \Phi$ *mit* $\Phi_0 \models \varphi$

(b) Φ *erfüllbar* $\Leftrightarrow$ *jede endliche Menge* $\Phi_0 \subseteq \Phi$ *ist erfüllbar*

Beweis.

(a) ist klar, weil die entsprechende Äquivalenz für „$\vdash$" gilt.

(b) ist klar, weil die entsprechende Äquivalenz für „Widerspruchsfreiheit" gilt.

□

Bemerkung 5.1.1. *Der Name „Kompaktheitssatz" verweist auf einen Zusammenhang zwischen mathematischer Logik und Topologie ($\rightsquigarrow$ Überdeckungseigenschaften), auf den wir hier nicht weiter eingehen.*

Korollar 5.1.1. *Sei $\Phi_0 \subseteq \Phi_1 \subseteq \ldots$ eine aufsteigende Folge von Mengen $\Phi_n \subseteq L^S$ und sei $\Phi = \bigcup_{n\in\mathbb{N}} \Phi_n$. Dann gilt:*

$$\Phi \text{ ist erfüllbar} \Leftrightarrow \text{jedes } \Phi_n \text{ ist erfüllbar.}$$

Beweis. *Es sind wieder zwei Richtungen zu zeigen:*

„$\Rightarrow$“: ist klar, da $\Phi_n \subseteq \Phi$

„$\Leftarrow$“: folgt aus Satz 5.1.1b (S.54), da jede endliche Teilmenge von Φ bereits in einer der Mengen Φ_n enthalten ist.

□

Satz 5.1.2. *Sei $\Phi \subseteq L^S$ eine Formelmenge, die beliebig große endliche Modelle besitzt (d.h. zu jedem $n \in \mathbb{N}$ existiert ein Modell $\mathcal{I} \models \Phi$, dessen Trägermenge mindestens n Elemente enthält). Dann besitzt Φ auch ein unendliches Modell.*

Beweis. *Sei $\Psi =_{\text{def}} \Phi \cup \{\varphi_{>n} \mid n \in \mathbb{N}\}$, wobei $\varphi_{>n}$ die (früher definierte) Formel (S.12) ist, die besagt, daß mehr als n Elemente in der Trägermenge liegen. Jede endliche Teilmenge $\Psi_0 \subseteq \Psi$ besitzt ein Modell, denn:*
Sei $m = \max\{n \in \mathbb{N} \mid \varphi_{>n} \in \Psi_0\}$ (wohldefiniert, da Ψ_0 endlich ist). Sei $\mathcal{I}$ ein Modell von Φ, das mindestens $m+1$ Elemente enthält. Dann gilt $\mathcal{I} \models \Phi$ und $\mathcal{I} \models \varphi_{>n}$ für alle $\varphi_{>n} \in \Psi_0$, also $\mathcal{I} \models \Psi_0$. Nach dem Kompaktheitssatz (Satz 5.1.1, S.54) existiert dann auch ein Modell $\mathcal{I}^* \models \Psi$, also $\mathcal{I}^* \models \Phi$ und $\mathcal{I}^* \models \varphi_{>n}$ für alle $n \in \mathbb{N}$, d.h. $\mathcal{I}^*$ ist unendliches Modell von Φ. □

Bemerkung 5.1.2. *Der Kompaktheitssatz ist nicht konstruktiv, er sichert lediglich die Existenz eines derartigen Modells.*

Korollar 5.1.2. *„Endlichkeit“ läßt sich in der Prädikatenlogik erster Stufe nicht ausdrücken, d.h. es gibt keine Formelmenge $\Phi \subseteq L^S$ mit:*

$$\mathcal{I} \models \Phi \Leftrightarrow \text{die Trägermenge von } \mathcal{I} \text{ ist endlich}$$

Beweis. *Eine Menge Φ mit dieser Eigenschaft hätte beliebig große endliche Modelle, aber kein unendliches Modell. Das widerspricht aber Satz 5.1.2 (S.55).*
□

Bemerkung 5.1.3. *„Unendlichkeit“ läßt sich durch eine Formelmenge Φ ausdrücken, nämlich $\Phi = \{\varphi_{>n} \mid n \in \mathbb{N}\}$. Eine einzige Formel reicht nicht, denn wäre $\varphi \in L^S$ eine Formel mit:*

$$\mathcal{I} \models \varphi \Leftrightarrow \text{die Trägermenge von } \mathcal{I} \text{ ist unendlich,}$$

dann würde gelten:

$$\mathcal{I} \models \neg\varphi \Leftrightarrow \text{die Trägermenge von } \mathcal{I} \text{ ist endlich.}$$

Das ist aber ein Widerspruch!

5.2 Die Sätze von Löwenheim und Skolem

Satz 5.2.1 (Satz von Löwenheim-Skolem[1] für abzählbare Signaturen). *Sei S abzählbar und sei $\Phi \subseteq L^S$. Dann gilt: Wenn Φ erfüllbar ist (also irgendein Modell besitzt), dann besitzt Φ ein abzählbares Modell.*

Beweis. *Wenn Φ erfüllbar ist, dann ist Φ widerspruchsfrei, also existiert nach Satz 4.2.1 (S.52) eine abzählbare Signatur $S' \supseteq S$ und eine Menge $\Theta \subseteq L^{S'}$ mit $\mathcal{I}^\Theta \models \Phi$. Die Trägermenge von $\mathcal{I}^\Theta$ besteht aus Äquivalenzklassen von Termen aus $T^{S'}$. Da S' abzählbar ist, ist $T^{S'}$ abzählbar, also auch die Menge der Äquivalenzklassen von Termen aus $T^{S'}$.* □

Beispiel 5.2.1. *Sei $S = S^<_{\mathrm{Ar}}$ und $\mathcal{R} = (\mathbb{R}, \ldots)$ die übliche S-Struktur der reellen Zahlen. Sei $\Phi = \{\varphi \in L_0^S \mid \mathcal{R} \models \varphi\}$. Dann gilt nach Satz 5.2.1, daß Φ (außer dem überabzählbaren Modell $\mathcal{R}$ auch ein abzählbares Modell $\mathcal{R}^*$ besitzt (Die Belegungen spielen hier keine Rolle, da Φ nur aus abgeschlossenen Formeln besteht). $\mathcal{R}^*$ ist nicht isomorph zu $\mathcal{R}$ (da es keine bijektive Abbildung geben kann). Mit anderen Worten: Wir können die reellen Zahlen durch Formeln der Prädikatenlogik erster Stufe (über $S^<_{\mathrm{Ar}}$) nicht „bis auf Isomorphie" charakterisieren.*

Intuition: Um die reellen Zahlen „bis auf Isomorphie" zu charakterisieren, benötigt man ein Axiom zweiter Stufe, z.B.: das sogenannte Vollständigkeitsaxiom *„Jede nichtleere nach oben beschränkte Teilmenge von $\mathbb{R}$ besitzt ein Supremum." Unsere Überlegungen zeigen, daß sich dies nicht in der Sprache erster Stufe ausdrücken läßt (noch nicht einmal durch unendlich viele Formeln).*

Ähnlich wie der Vollständigkeitssatz (S.53) läßt sich auch Satz 5.2.1 (S.56) auf beliebige Signaturen S verallgemeinern. Das führt zu dem

Satz 5.2.2 („Absteigender" Satz von Löwenheim-Skolem). *Sei S eine Signatur und sei $\Phi \subseteq L^S$. Dann gilt: Wenn Φ erfüllbar ist dann besitzt Φ ein Modell, dessen Trägermenge höchstens so groß wie L^S ist (d.h. dessen Trägermenge sich injektiv in L^S abbilden läßt).*

Beweis. *Hier nicht!* □

Bemerkung 5.2.1. *Satz 5.2.1 ist ein Spezialfall von Satz 5.2.2, wenn S abzählbar ist, dann ist L^S abzählbar unendlich, also besagt Satz 5.2.2 in diesem Fall, daß ein Modell mit abzählbarer Trägermenge existiert.*

Bemerkung 5.2.2. *Es gibt noch einen „aufsteigenden" Satz von Löwenheim-Skolem, der die Existenz von beliebig großen Modellen garantiert und den Satz von Löwenheim-Skolem-Tarski, der die Existenz von Modellen einer fest vorgegebenen (unendlichen) Größenordnung garantiert.*

[1] Leopold Löwenheim (1878-1957), dt. Mathematiker
Albert Thoralf Skolem (1887-1963), norw. Mathematiker und Logiker

5.3 Elementare Klassen

Fragestellung: Welche Eigenschaften von Strukturen lassen sich in der Prädikatenlogik erster Stufe ausdrücken?

Definition 5.3.1. *(a) Sei $\Phi \subseteq L_0^S$ eine Menge abgeschlossener Formeln. Dann sei*

$$Mod^S\Phi =_{\text{def}} \{\mathcal{A} \mid \mathcal{A} \text{ ist } S\text{-Struktur mit } \mathcal{A} \models \Phi\}$$

die Klasse aller Modelle *von Φ.*

(b) Sei $\varphi \in L_0^S$. Dann sei

$$Mod^S\varphi =_{\text{def}} Mod^S\{\varphi\} = \{\mathcal{A} \mid \mathcal{A} \text{ ist } S\text{-Struktur mit } \mathcal{A} \models \varphi\}$$

(Kürzer: ModΦ bzw. Modφ, wenn S bekannt ist. Oft schreibt man auch: Mod(Φ) bzw. Mod(φ) statt ModΦ und Modφ)

Definition 5.3.2. *Sei $\mathcal{K}$ eine Klasse von S-Strukturen.*

(a) $\mathcal{K}$ heißt elementar*, wenn ein $\varphi \in L_0^S$ existiert mit $\mathcal{K} = Mod^S\varphi$*

(b) $\mathcal{K}$ heißt Δ-elementar*, wenn eine Menge $\Phi \subseteq L_0^S$ existiert mit $\mathcal{K} = Mod^S\Phi$*

Beispiel 5.3.1. *Die folgenden drei Beispiele sind bereits bekannt.*

(1) Für beliebige Signaturen S gilt: Die Klasse $\mathcal{K}_{<\infty}$ aller S-Strukturen mit endlicher Trägermenge ist nicht Δ-elementar (also auch nicht elementar)

(2) Für beliebiges S ist die Klasse $\mathcal{K}_{\infty}$ aller S-Strukturen mit unendlicher Trägermenge Δ-elementar (mit $\Phi = \{\varphi_{>n} \mid n \in \mathbb{N}\}$), aber nicht elementar.

(3) Sei $S = S_{\text{Ar}}^{<}$. Dann ist die Klasse $\mathcal{K}_{\simeq\mathcal{R}} =_{\text{def}} \{\mathcal{A} \mid \mathcal{A}$ S-Struktur, $\mathcal{A} \simeq \mathcal{R}\}$ nicht Δ-elementar.

Weitere (einfache) Beispiele: *„Viele“ in der Mathematik betrachteten Klassen von Strukturen sind elementar, z.B.:*

- *die Klasse aller Mengen mit Äquivalenzrelation ($S = \{\sim\}$)*
- *die Klasse aller Gruppen ($S = \{0, +\}$)*
- *die Klasse aller Ringe ($S = \{0, 1, +, *\}$)*
- *die Klasse aller Körper ($S = \{0, 1, +, *\}$)*

denn: Jede dieser Klassen ist durch endlich viele Axiome (erster Stufe) $\varphi_1, \ldots, \varphi_n$ definiert (z.B.: $\text{refl}, \text{symm}, \text{trans}$ *für Äquivalenzrelationen), also gilt*

$$\mathcal{K} = Mod^S(\varphi_1 \wedge \ldots \wedge \varphi_n)$$

Weiteres Gegenbeispiel: *Sei $S = \{r\}$, r zweistellige Relation. Sei*

$$\Phi = \{\forall x.\, \neg r(x,x), \forall x, y.\, r(x,y) \to r(y,x)\}$$

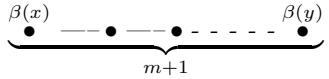
Die Klasse aller Graphen *sei definiert als*

$$\mathcal{K}_{\mathrm{Grph}} =_{\mathrm{def}} \mathit{Mod}^S \Phi$$

(also ist $\mathcal{K}_{\mathrm{Grph}}$ Δ-elementar). Wir wollen zeigen: die Klasse $\mathcal{K}$ aller zusammenhängenden Graphen[2] *ist nicht Δ-elementar.*
Beweis: Angenommen, es existiert ein $\Psi \subseteq L_0^S$ mit $\mathcal{K} = \mathit{Mod}^S \Psi$. Für jedes $n \geq 2$ sei

$$\psi_n =_{\mathrm{def}} \neg x \equiv y \wedge \neg \exists x_1, \ldots, x_n.\, (x \equiv x_1 \wedge y \equiv x_n \wedge \bigwedge_{i=1}^{n-1} r(x_i, x_{i+1}))$$

Die Formel ψ_n bedeutet: x und y sind verschieden, und es gibt keinen Pfad der Länge $n-1$ von x nach y. Sei $\Theta = \Psi \cup \{\psi_n \mid n \geq 2\}$. Jede endliche Teilmenge Θ_0 von Θ besitzt ein Modell, denn: Sei $m = max\{n \geq 2 \mid \psi_n \in \Theta_0\}$. Sei $\mathcal{I} = (\mathcal{A}, \beta)$, wobei $\mathcal{A}$ der folgende zusammenhängende Graph ist:



Dann gilt $\beta(x) \neq \beta(y)$ und es existiert kein Pfad der Länge $\leq m$ von $\beta(x)$ nach $\beta(y)$, d.h. $\mathcal{I} \models \psi_n$ für alle $\psi_n \in \Theta_0$. Da $\mathcal{A}$ ein zusammenhängender Graph ist, gilt außerdem: $\mathcal{I} \models \Psi$, also $\mathcal{I} \models \Theta_0$.

Also folgt nach dem Kompaktheitssatz: Θ hat selbst ein Modell $\mathcal{I}^* = (\mathcal{A}^*, \beta^*)$. Wegen $\mathcal{I}^* \models \Psi$ ist $\mathcal{A}^*$ ein zusammenhängender Graph. Wegen $\mathcal{I}^* \models \psi_n$ für alle $n \geq 2$, existiert zwischen $\beta^*(x)$ und $\beta^*(y)$ kein Pfad im Widerspruch zur Eigenschaft zusammenhängend! Also war die Annahme falsch, daß eine Menge $\Psi \subseteq L_0^S$ existiert mit $\mathcal{K} = \mathit{Mod}^S \Psi$. $\rightsquigarrow$ $\mathcal{K}$ ist nicht Δ-elementar.

5.4 Elementare Äquivalenz, Nichtstandardmodelle

Definition 5.4.1 (Theorie). *(a) Sei S eine Signatur, $\mathcal{K}$ eine Klasse von S-Strukturen. Dann sei*

$$\mathit{Th}(\mathcal{K}) =_{\mathrm{def}} \{\varphi \in L_0^S \mid \mathcal{A} \models \varphi \text{ für alle } \mathcal{A} \in \mathcal{K}\}$$

die Theorie *von $\mathcal{K}$.*

[2] Zu je zwei Knoten des Graphen existiert ein Pfad.

(b) Für eine einzelne S-Struktur $\mathcal{A}$ sei

$$Th(\mathcal{A}) =_{\text{def}} \{\varphi \in L_0^S \mid \mathcal{A} \models \varphi\} \ (= Th(\{\mathcal{A}\})$$

die Theorie *von $\mathcal{A}$.*

Lemma 5.4.1. *(i) $Th(\mathcal{K})$ ist abgeschlossen unter „$\models$“ (d.h. wenn $Th(\mathcal{K}) \models \varphi$ für ein $\varphi \in L_0^S$, dann gilt schon $\varphi \in Th(\mathcal{K})$)*

(ii) $\mathcal{K} \subseteq Mod(Th(\mathcal{K}))$ (insbesondere: $\mathcal{A} \in Mod(Th(\mathcal{A}))$)

(iii) Für jedes $\Phi \subseteq L_0^S$ gilt: $\Phi \subseteq Th(Mod(\Phi))$

(iv) Für jedes $\varphi \in L_0^S$ gilt: $\varphi \in Th(\mathcal{A})$ oder $\neg\varphi \in Th(\mathcal{A})$ (d.h. $Th(\mathcal{A})$ ist maximal unter den erfüllbaren Mengen)

(v) $Mod(\Phi) = Mod(Th(Mod(\Phi)))$ (d.h. wenn $\mathcal{K}$ Δ-elementar ist, dann ist $\mathcal{K} = Mod(Th(\mathcal{K}))$)

(vi) $Th(\mathcal{K}) = Th(Mod(Th(\mathcal{K})))$

Beweis.

(ii) Sei $\mathcal{A} \in \mathcal{K}$. Wegen $Th(\mathcal{K}) = \{\varphi \in L_0^S \mid \mathcal{A} \models \varphi$ für alle $\mathcal{A} \in \mathcal{K}\}$ folgt $\mathcal{A} \models \varphi$ für alle $\varphi \in Th(\mathcal{K})$ nach Definition, d.h. $\mathcal{A} \in Mod(Th(\mathcal{K}))$

(i) Sei $\varphi \in L_0^S$ mit $Th(\mathcal{K}) \models \varphi$. Dann gilt $\mathcal{A} \models \varphi$ für alle Modelle $\mathcal{A}$ von $Th(\mathcal{K})$, d.h für alle $\mathcal{A} \in Mod(Th(\mathcal{K}))$, also - wegen (ii) - erst recht für alle $\mathcal{A} \in \mathcal{K}$. Also ist $\varphi \in Th(\mathcal{K})$.

(iii) Sei $\varphi \in \Phi$. Per Definition von $Mod(\Phi)$ gilt: $\mathcal{A} \models \varphi$ für alle $\mathcal{A} \in Mod(\Phi)$. Per Definition von Th folgt dann: $\varphi \in Th(Mod(\Phi))$

(iv) Klar, denn wegen der Abgeschlossenheit von φ gilt: $\mathcal{A} \models \varphi$ oder $\mathcal{A} \models \neg\varphi$

(v) „$\supseteq$“ folgt aus (iii), denn aus $\Phi \subseteq \Psi$ folgt $Mod(\Phi) \supseteq Mod(\Psi)$ (die kleinere Formelmenge besitzt eventuell mehr Modelle). „$\subseteq$“ gilt wegen (ii) mit $\mathcal{K} = Mod(\Phi)$

(vi) „$\subseteq$“ gilt wegen (iii) mit $\Phi = Th(\mathcal{K})$ „$\supseteq$“ folgt aus (ii), denn aus $\mathcal{K} \subseteq \mathcal{K}'$ folgt $Th(\mathcal{K}) \supseteq Th(\mathcal{K}')$ (in der größeren Klasse von Strukturen gelten eventuell weniger Formeln).

□

Bemerkung 5.4.1. *Ein Paar von Operatoren wie Mod und Th, die beide die Teilmengenbeziehung „$\subseteq$“ umkehren und außerdem (ii) und (iii) erfüllen bezeichnet man als* Galoissche[3] Korrespondenz *(weil in der* Galois-Theorie *ein solches Paar von Operatoren vorkommt). (v) und (vi) ergeben sich dann als Folgerungen.*

[3] Evariste Galois (1811-1832), frz. Mathematiker, begründete unter anderem die Gruppentheorie

Definition 5.4.2 (Elementare Äquivalenz). *Seien $\mathcal{A}$ und $\mathcal{B}$ zwei S-Strukturen. $\mathcal{A}$ und $\mathcal{B}$ heißen* elementar äquivalent*, wenn $Th(\mathcal{A}) = Th(\mathcal{B})$.*

Bezeichnung 5.4.1. *Sind $\mathcal{A}$ und $\mathcal{B}$ elementar äquivalent, so schreibt man auch kurz $\mathcal{A} \equiv \mathcal{B}$.*

Wir wissen schon: Aus $\mathcal{A} \simeq \mathcal{B}$ folgt stets $\mathcal{A} \equiv \mathcal{B}$. Wir wissen auch, daß die Umkehrung im allgemeinen nicht gilt, z.B.: Sei $S = S^{<}_{\mathrm{Ar}}$ und $\mathcal{R}$ die S-Struktur der reellen Zahlen. Dann besitzt $\mathrm{Th}(\mathcal{R})$ ein abzählbares Modell $\mathcal{R}^*$, das nicht isomorph zu $\mathcal{R}$ ist. Also gilt $\mathrm{Th}(\mathcal{R}) \subseteq \mathrm{Th}(\mathcal{R}^*)$ und damit $\mathrm{Th}(\mathcal{R}) = Th(\mathcal{R}^*)$.
$\rightsquigarrow$ *Isomorphie* ist also stärker als *elementare Äquivalenz*.

Bemerkung 5.4.2. *Um zu zeigen, daß $\mathcal{A} \equiv \mathcal{B}$ gilt, genügt es zu zeigen, daß $\mathcal{A} \models Th(\mathcal{B})$ (oder $\mathcal{B} \models Th(\mathcal{A})$) gilt.*

Beweis: Wenn $\mathcal{A} \models Th(\mathcal{B})$, dann gilt $Th(\mathcal{B}) \subseteq Th(\mathcal{A})$. Wegen Teil (iv) des Lemmas ist $Th(\mathcal{B})$ maximal unter allen erfüllbaren Mengen abgeschlossener Formeln, also gilt sogar die Gleichheit: $Th(\mathcal{B}) = Th(\mathcal{A})$.

Satz 5.4.1. *Sei S eine Signatur.*

(a) Sei $\mathcal{A}$ eine unendliche S-Struktur. Dann ist die Isomorphieklasse *von $\mathcal{A}$, d.h. die Klasse*

$$\mathcal{K}_{\simeq\mathcal{A}} =_{\mathrm{def}} \{\mathcal{B} \mid \mathcal{B} \text{ ist } S\text{-Struktur und } \mathcal{B} \simeq \mathcal{A}\}$$

nicht Δ-elementar (d.h. keine unendliche Struktur ist „bis auf Isomorphie“ durch Formeln erster Stufe charakterisierbar.)

(b) Sei $\mathcal{A}$ eine beliebige S-Struktur. Dann ist die „elementare Äquivalenzklasse“ *von $\mathcal{A}$, d.h. die Klasse*

$$\mathcal{K}_{\equiv\mathcal{A}} =_{\mathrm{def}} \{\mathcal{B} \mid \mathcal{B} \text{ ist } S\text{-Struktur und } \mathcal{B} \equiv \mathcal{A}\}$$

Δ-elementar.

Genauer: $\mathcal{K}_{\equiv\mathcal{A}} = Mod(Th(\mathcal{A}))$ und $\mathcal{K}_{\equiv\mathcal{A}}$ ist die kleinste Δ-elementare Klasse, die $\mathcal{A}$ enthält.

(c) Für unendliche Strukturen $\mathcal{A}$ gilt also: $\mathcal{K}_{\simeq\mathcal{A}} \subset \mathcal{K}_{\equiv\mathcal{A}}$

Beweis.

(a) folgt aus dem „aufsteigenden Satz von Löwenheim-Skolem“: Angenommen, $\mathcal{K}_{\simeq\mathcal{A}} = Mod(\Phi)$ für ein $\Phi \subseteq L^S_0$. Wenn A die Trägermenge von $\mathcal{A}$ ist, dann existiert nach diesem Satz ein Modell $\mathcal{A}^*$ von Φ, dessen Trägermenge mindestens so groß wie die Potenzmenge von A ist. Also ist $\mathcal{A}^*$ nicht isomorph zu $\mathcal{A}$. Also gilt $\mathcal{A}^* \in Mod(\Phi)$, $\mathcal{A}^* \not\simeq \mathcal{A}$ Widerspruch!

(b) Wir wissen schon:

$$\begin{aligned} \mathcal{B} \equiv \mathcal{A} &\Leftrightarrow \mathcal{B} \models \mathit{Th}(\mathcal{A}) \\ &\Leftrightarrow \mathcal{B} \in \mathit{Mod}(\mathit{Th}(\mathcal{A})) \end{aligned}$$

Also ist $\mathcal{K}_{\equiv\mathcal{A}} = \mathit{Mod}(\mathit{Th}(\mathcal{A}))$ eine Δ-elementare Klasse. Noch zu zeigen: $\mathcal{K}_{\equiv\mathcal{A}}$ ist die kleinste Δ-elementare Klasse, die $\mathcal{A}$ enthält, d.h. für jede Δ-elementare Klasse $\mathcal{K}$, die $\mathcal{A}$ enthält, gilt:

$$\mathcal{K}_{\equiv\mathcal{A}} \subseteq \mathcal{K}$$

Sei also $\mathcal{K}$ Δ-elementar mit $\mathcal{A} \in \mathcal{K}$, d.h. es existiert ein $\Phi \subseteq L_0^S$ mit $\mathcal{K} = \mathit{Mod}(\Phi)$. Dann gilt für jede Struktur $\mathcal{B} \in \mathcal{K}_{\equiv\mathcal{A}}$: $\mathcal{B} \models \Phi$ (weil $\mathcal{A} \models \Phi$) und damit $\mathcal{B} \in \mathcal{K}$. Damit ist $\mathcal{K}_{\equiv\mathcal{A}} \subseteq \mathcal{K}$ gezeigt.

(c) klar wegen (a) und (b)

□

Satz 5.4.2 (Skolem). *Sei $S = S_{\mathrm{Ar}} = \{0, 1, +, *\}$. Es gibt ein abzählbares* Nichtstandardmodell der Arithmetik, *d.h. eine S_{Ar}-Struktur $\mathcal{N}^*$ mit $\mathcal{N}^* \equiv \mathcal{N}$ und $\mathcal{N}^* \not\cong \mathcal{N}$.*

Beweis. *Idee: Man sucht ein Modell $\mathcal{N}^*$, in dem nicht jede Zahl von der Form $1 + \ldots + 1$ ist. Dazu: Kompaktheitssatz*

Sei $\Psi =_{\mathrm{def}} \mathit{Th}(\mathcal{N}) \cup \{\psi_n \mid n \in \mathbb{N}\}$ wobei

$$\psi_n =_{\mathrm{def}} \neg x \equiv \underbrace{1 + \ldots + 1}_{n}$$

Jede endliche Teilmenge $\Psi_0 \subseteq \Psi$ besitzt ein Modell, denn: Sei

$$m = \max\{n \mid \psi_n \in \Psi_0\}$$

Dann ist $(\mathcal{N}, \beta)$ mit $\beta(x) = m + 1$ ein Modell von Ψ_0. Also besitzt nach dem Kompaktheitssatz auch Ψ ein Modell $(\mathcal{N}^*, \beta^*)$, d.h. $\underbrace{\mathcal{N}^* \models \mathit{Th}(\mathcal{N})}_{\mathcal{N}^* \equiv \mathcal{N}}$ und $(\mathcal{N}^*, \beta^*)$ erfüllt alle ψ_n: $\underbrace{(\mathcal{N}^*, \beta^*) \models \psi_n \text{ für alle } n \in \mathbb{N}}$

$$\text{d.h. } \beta^*(x) \neq \underbrace{1 + \ldots + 1}_{n} \text{ für alle } n$$

Noch zu zeigen: $\mathcal{N} \not\cong \mathcal{N}^*$

Angenommen, $\pi : \mathcal{N} \longrightarrow \mathcal{N}^*$ ist ein Isomorphismus. Dann gilt für jedes $n \in \mathbb{N}$:

$$\begin{aligned} \pi(n) &= \pi(1^{\mathcal{N}} +^{\mathcal{N}} \ldots +^{\mathcal{N}} 1^{\mathcal{N}}) \\ &= 1^{\mathcal{N}^*} +^{\mathcal{N}^*} \ldots +^{\mathcal{N}^*} 1^{\mathcal{N}^*} \end{aligned}$$

Also würde aus der Surjektivität von π folgen, daß auch jedes Element von $\mathcal{N}^*$ endliche Summe von Einsen ist. Widerspruch! □

Kapitel 6

Grenzen der formalen Beweismethode

„Logik und Vernunft sind die Hosenträger beim Denken.“
Werner Mitsch (*1936)

Wir wissen: Die Begriffe „logische Folgerung“ und „Ableitbarkeit“ stimmen überein. $\rightsquigarrow$ Wir erhalten z.B. alle allgemeingültigen Formeln mit Hilfe eines „mechanischen Verfahrens“.

6.1 Begriffe aus der Berechenbarkeitstheorie

Einige wesentliche Begriffe aus der Berechnenbarkeitstheorie müssen erklärt werden, dazu die folgende

Definition 6.1.1. *Sei Z ein endlicher Zeichenvorrat. Eine Menge $M \subseteq Z^*$ heißt*

(a) entscheidbar, *wenn ein Algorithmus existiert, der bei Eingabe eines beliebigen Wortes $w \in Z^*$*

- *mit der Ausgabe* 1 *(oder „true“) hält, falls $w \in M$*
- *mit der Ausgabe* 0 *(oder „false“) hält, falls $w \notin M$*

(b) semi-entscheidbar *oder* akzeptierbar, *wenn es einen Algorithmus gibt, der bei Eingabe eines Wortes $w \in Z^*$*

- *mit Ausgabe* 1 *(„true“) halt, falls $w \in M$*
- *nicht hält, falls $w \notin M$*

(c) rekursiv aufzählbar, *wenn es einen Algorithmus (Aufzählungsalgorithmus) gibt, der (ohne Eingabe) nach und nach „alle“ Worte $w \in M$ (eventuell auch mit Wiederholungen) ausgibt, d.h.*

- *wenn $w \in M$, dann wird w irgendwann ausgegeben (aber wir wissen nicht wann)*
- *wenn $w \notin M$, dann wird w nie ausgegeben*

Bemerkung 6.1.1. *Der Begriff „rekursiv“ ist historisch bedingt und ist ein Synonym für den Begriff „berechenbar“. Er hat im Grunde genommen nichts mit der heutigen Vorstellung von „Rekursion“ zu tun.*

Zusammenhänge:

- $\emptyset$ ist entscheidbar (durch den Algorithmus, der immer 0 liefert)
- Z^* ist entscheidbar (durch den Algorithmus, der immer 1 liefert)
- M entscheidbar $\Rightarrow$ M akzeptierbar
- M entscheidbar $\Leftrightarrow$ $Z^* \backslash M$ entscheidbar
- M entscheidbar $\Leftrightarrow$ M und $Z^* \backslash M$ akzeptierbar
- M akzeptierbar $\Leftrightarrow$ M rekursiv aufzählbar

Bemerkung 6.1.2. *(a) Anstelle von Mengen $M \subseteq Z^*$ (Z endlicher Zeichenvorrat) können wir auch Mengen $M \subseteq \mathbb{N}$ betrachten, (indem wir natürliche Zahlen als Zeichenreihen, z.B. über $Z = \{0, 1\}$ betrachten)*

(b) Anstelle eines endlichen Zeichenvorrats können wir einen abzählbaren Zeichenvorrat zulassen, denn abzählbar viele Zeichen $z_0, z_1, \ldots$ lassen sich zum Beispiel über $\{z, 0, \ldots, 9\}$ kodieren durch $z0, z1, \ldots$.

(c) Außerdem können wir Mengen $M \subseteq (Z^*)^k$ oder $M \subseteq \mathbb{N}^k$ ($k \geq 2$) betrachten, indem wir ein Tupel $(w_1, \ldots, w_k) \in (Z^*)^k$ als Wort $w_1 \# w_2 \ldots \# w_k \in (Z \cup \{\#\})^*$ schreiben, wobei $\#$ ein neues Zeichen ist.

Wir setzen in diesem Kapitel voraus: Die Signatur S ist abzählbar $\rightsquigarrow$ Das Alphabet für Formeln, Terme,... ist abzählbar (unendlich): $S \cup X \cup \{\neg, \wedge, \vee, \ldots\}$. In diesem Sinne gilt dann: Die Mengen T^S, L^S, L_0^S, L_n^S ($n \in \mathbb{N}$) sind entscheidbar (der Entscheidungsalgorithmus ist durch die *kontextfreie Grammatik*, d.h. durch den Parser gegeben).

Fragestellung:
Welche „semantisch definierten“ Formelmengen sind entscheidbar bzw. akzeptierbar?

Satz 6.1.1. *Sei S eine abzählbare Signatur. Dann gilt:*

(a) Die Menge aller allgemeingültigen Formeln in L^S (oder L_0^S) ist akzeptierbar.

(b) Wenn $\Phi \subseteq L^S$ entscheidbar ist, dann ist die Menge $\Phi^{\models}$ aller logischen Folgerungen von Φ akzeptierbar.

Beweis.

(a) ist ein Spezialfall von (b), indem man $\Phi = \emptyset$ wählt.

(b) Einen Aufzählungsalgorithmus für $\Phi^{\models}$ erhält man so: Da L^S entscheidbar ist, ist auch

- *die Menge $(L^S)^+$ aller Sequenzen (= endliche Folgen von Formeln) entscheidbar,*
- *die Menge $((L^S)^+)^+$ aller endlichen Folgen von Sequenzen entscheidbar.*

Also sind beide auch rekursiv aufzählbar. Also können wir nach und nach alle endlichen Folgen von Sequenzen aufzählen und jeweils testen, ob eine solche Folge „zufällig" eine Ableitung (in unserem Sequenzenkalkül) einer Formel φ aus der Menge Φ ist oder nicht. Wenn ja, so geben wir φ aus, ansonsten verwerfen wir die Auswahl. Dieses „Testen" ist möglich, denn:

- *wir können für jede Sequenz in der Folge überprüfen*
  - *ob sie ein Axiom ist*
  - *oder mit einer Ableitungsregel aus vorhergehenden Sequenzen folgt.*
- *wir können überprüfen, ob die letzte Sequenz in der Folge von der Form $\varphi_0 \dots \varphi_n\ \varphi$ mit $\varphi_0, \dots, \varphi_n \in \Phi$ ist (das ist möglich, weil Φ entscheidbar ist).*

□

Spezialfälle von Satz 6.1.1:
Da jede endliche Menge $\Phi \subseteq L^S$ entscheidbar ist, ist die Menge $\Phi^{\models}$ aller logischen Folgerungen einer endlichen Menge rekursiv aufzählbar, z.B.:

- die *Theorie der Äquivalenzrelationen* ($\Phi = \{\text{refl}, \text{symm}, \text{trans}\}$)
- die *Theorie der partiellen Ordnungen (Halbordnungen)*
- die *Theorie der Gruppen* ($\Phi =$ Gruppenaxiome)
- die *Theorie der Ringe*
  ⋮
- die *Theorie Th($\mathcal{K}_\infty$) aller unendlichen Strukturen*, denn $\Phi = \{\varphi_{>n} \mid n \in \mathbb{N}\}$ ist entscheidbar (weil man überprüfen kann, ob eine Formel von der Form $\varphi_{>n}$ ist)

6.2 Theorien und Axiomatisierbarkeit

Definition 6.2.1. *Sei S eine Signatur.*

(a) Eine Theorie *Th (über S) ist eine erfüllbare Menge $Th \subseteq L_0^S$, die abgeschlossen ist unter „$\models$“ (d.h., wenn $\varphi \in L_0^S$ mit $Th \models \varphi$, dann $\varphi \in Th$)*

(b) Eine Theorie heißt axiomatisierbar*, wenn es eine entscheidbare Menge $\Phi \subseteq Th$ gibt mit $Th = \Phi^{\models}$ (auch $\Phi = \emptyset$ denkbar). Die Formeln aus Φ nennt man dann* Axiome*.*

(c) Eine Theorie heißt endlich axiomatisierbar*, wenn man in (b) eine endliche Menge Φ findet.*

Neue Formulierung von Satz 6.1.1:
Jede axiomatisierbare Theorie ist akzeptierbar.

Neue Formulierung der Beispiele:

- die *Theorie der Äquivalenzrelationen*,
- die *Theorie der partiellen Ordnungen (Halbordnungen)*,
- die *Theorie der Gruppen*,
- und die *Theorie der Ringe*

  ⋮

sind endlich axiomatisierbar.

- die *Theorie $Th(\mathcal{K}_\infty)$ aller unendlichen Strukturen* ist axiomatisierbar.

Wir wissen bereits:

(1) Für jede S-Struktur $\mathcal{A}$ ist $\mathrm{Th}(\mathcal{A}) = \{\varphi \in L_0^S \mid \mathcal{A} \models \varphi\}$ eine Theorie, denn $\mathrm{Th}(\mathcal{A})$ ist erfüllbar mit $\mathcal{A} \models \mathrm{Th}(\mathcal{A})$ und $\mathrm{Th}(\mathcal{A})$ ist abgeschlossen unter logischer Folgerung „$\models$“.

(2) Für jede Klasse $\mathcal{K} \neq \emptyset$ von S-Strukturen ist $\mathrm{Th}(\mathcal{K}) = \{\varphi \in L_0^S \mid \mathcal{A} \models \varphi \text{ für alle } \mathcal{A} \in \mathcal{K}\}$ eine Theorie, denn $\mathcal{A} \models \mathrm{Th}(\mathcal{K})$ für alle $\mathcal{A} \in \mathcal{K}$, d.h. $Th(\mathcal{K})$ ist erfüllbar, und $Th(\mathcal{K})$ ist abgeschlossen unter „$\models$“.

(3) Für jede erfüllbare Menge $\Phi \subseteq L_0^S$ ist $\Phi^{\models} =_{\mathrm{def}} \{\varphi \in L_0^S \mid \Phi \models \varphi\}$ eine Theorie, denn jedes Modell von Φ ist auch Modell von $\Phi^{\models}$, und $\Phi^{\models}$ ist abgeschlossen unter „$\models$“.

Bemerkung 6.2.1. *In (2) ist $\mathcal{K} \neq \emptyset$ eine notwendige Voraussetzung, denn $Th(\emptyset) = L_0^S$ ist unerfüllbar und deshalb* keine *Theorie.*

Definition 6.2.2. *Eine Theorie $Th \subseteq L_0^S$ heißt* vollständig*, wenn für jedes $\varphi \in L_0^S$ gilt: $\varphi \in Th$ oder $\neg\varphi \in Th$.*

Wir wissen bereits, daß für jede S-Struktur $\mathcal{A}$ $\mathrm{Th}(\mathcal{A})$ eine vollständige Theorie ist.

Lemma 6.2.1. *Sei $Th \subseteq L_0^S$ eine Theorie. Dann sind folgende Aussagen äquivalent:*

(a) Th ist vollständig

(b) Th ist maximal unter allen erfüllbaren Teilmengen von L_0^S

(c) Th ist maximal unter allen Theorien über der Signatur S

(d) Für jedes Modell $\mathcal{A}$ von Th gilt: $Th = Th(\mathcal{A})$

(e) Es existiert eine S-Struktur $\mathcal{A}$ mit $Th = Th(\mathcal{A})$

(f) Für alle Modelle $\mathcal{A}$, $\mathcal{B}$ von Th gilt: $Th(\mathcal{A}) = Th(\mathcal{B})$ (d.h. alle Modelle von Th sind elementar äquivalent)

Beweis. *Wir führen einen Ringschlußbeweis:*

- *„(a)⇒(b)“: Angenommen, es existiert ein $\Phi \subseteq L_0^S$, Φ erfüllbar und $Th \subset \Phi$. Dann existiert ein $\varphi \in \Phi$ mit $\varphi \notin Th$. Dann folgt wegen (a) $\neg\varphi \in Th \subseteq \Phi$, also ist Φ unerfüllbar. Widerspruch!*
- *„(b)⇒(c)“: Klar!*
- *„(c)⇒(d)“: Wenn $\mathcal{A} \models Th$, dann gilt $Th \subseteq Th(\mathcal{A})$. Also folgt $Th = Th(\mathcal{A})$, weil Th maximal ist unter allen Theorien.*
- *„(d)⇒(e)“: Klar, da jede Theorie Th nach Definition mindestens ein Modell besitzt.*
- *„(d)⇒(f)“: Klar!*
- *„(e)⇒(a)“: Wissen wir schon!*
- *„(f)⇒(a)“: Angenommen, es existiert ein $\varphi \in L_0^S$ mit $\varphi \notin Th$ und $\neg\varphi \notin Th$. Da Th abgeschlossen unter „$\models$“ folgt: $Th \not\models \varphi$ und $Th \not\models \neg\varphi$. Also existieren Modelle $\mathcal{A}$ und $\mathcal{B}$ von Th mit $\mathcal{A} \not\models \varphi$ und $\mathcal{B} \not\models \neg\varphi$, also $\mathcal{B} \models \underbrace{\neg(\neg\varphi)}_{\varphi}$ (weil φ abgeschlossen). Also gilt: $Th(\mathcal{A}) \neq Th(\mathcal{B})$ ($\varphi \notin Th(\mathcal{A})$, $\varphi \in Th(\mathcal{B})$).*

□

Satz 6.2.1. *(a) Jede vollständige axiomatisierbare Theorie ist entscheidbar.*

(b) Jede rekursiv aufzählbare vollständige Theorie ist entscheidbar.

Beweis.

(a) *folgt sofort aus (b), weil jede axiomatisierbare Theorie rekursiv aufzählbar ist.*

(b) *Um zu entscheiden, ob φ in der Theorie liegt, startet man den Aufzählungsalgorithmus und wartet bis φ oder sein Negat $\neg\varphi$ in der Aufzählung auftaucht (Wegen der Vollständigkeit muß eines von beiden irgendwann auftauchen). Wenn φ auftaucht $\rightsquigarrow$ Antwort 1, wenn $\neg\varphi$ auftaucht $\rightsquigarrow$ Antwort 0.*

□

6.3 Die Unentscheidbarkeit der Arithmetik

Sei $S = S_{\mathrm{Ar}} = \{0, 1, +, *\}$ und sei $\mathcal{N} = (\mathbb{N}, \ldots)$ die übliche S-Struktur der natürlichen Zahlen (*Standardmodell der Arithmetik*).

Wir wollen zeigen: $\mathrm{Th}(\mathcal{N})$ ist unentscheidbar
Da $\mathrm{Th}(\mathcal{N})$ vollständig ist folgt dann mit Satz 6.2.1: *$Th(\mathcal{N})$ ist nicht axiomatisierbar.*

Aus der Berechenbarkeitstheorie wissen wir: *Das* Halteproblem für Turingmaschinen *(oder für irgendeine Turingmächtige Programmiersprache bzw. Turingmächtiges Berechnungsmodell) ist unentscheidbar, d.h. die Menge*

$$\mathcal{H} =_{\mathrm{def}} \{(\pi, n) \mid \pi \textit{ Programm, } n \in \mathbb{N} \textit{ und } \pi \textit{ hält bei Eingabe } n\}$$

ist nicht entscheidbar.

Hier: Wir betrachten die Menge $\mathbb{WH}$ aller `WHILE`-Programme π, definiert durch die folgende kontextfreie Grammatik:

$$\begin{array}{rcll} \pi & ::= & x := t & (x \in X,\, t \in T^S) \\ & | & \pi_1;\, \pi_2 & \\ & | & \underline{\text{if}}\ b\ \underline{\text{then}}\ \pi_1\ \underline{\text{else}}\ \pi_2 & (b \in L^S \text{ quantorenfrei}) \\ & | & \underline{\text{while}}\ b\ \underline{\text{do}}\ \pi_1 & (b \in L^S \text{ quantorenfrei}) \end{array}$$

Der Einfachheit halber nehmen wir an, daß unsere `WHILE`-Programme nur eine Variable x enthalten (bei mehreren Variablen bleibt die Idee die gleiche, aber großer Schreibaufwand!)

Ziel: Wir zeigen, daß für jedes `WHILE`-Programm π sich eine Formel φ_π konstruieren läßt, die das Ein-/Ausgabeverhalten von π (*Denotationelle Semantik*) beschreibt.

Zunächst: eine formale Definition des Ein-/Ausgabeverhaltens. Jedem `WHILE`-Programm π (mit einer einzigen Variablen x) ordnen wir eine Relation $[\![\pi]\!] \subseteq \mathbb{N}^2$ zu, für die gilt:

$$[\![\pi]\!] = \{(m, n) \in \mathbb{N}^2 \mid \pi \text{ hält bei Eingabe } m \text{ mit Ausgabe } n\}$$

(da WHILE-Programme deterministisch sind, ist $[\![\pi]\!]$ sogar funktional, d.h. $[\![\pi]\!]$ ist eine partielle Funktion). $[\![\pi]\!]$ wird durch die Induktion über die Größe von π definiert:

(i) $[\![x := t]\!] = \{(m, \mathcal{I}[m/x](t)) \mid m \in \mathbb{N}\}$

(ii) $[\![\pi_1;\ \pi_2]\!] = \{(m,n) \mid$ es ex. ein $k \in \mathbb{N}$ mit $(m,k) \in [\![\pi_1]\!]$ und $(k,n) \in [\![\pi_2]\!]\}$

(iii) $[\![\underline{\text{if}}\ b\ \underline{\text{then}}\ \pi_1\ \underline{\text{else}}\ \pi_2]\!] = \{(m,n) \in \mathbb{N}^2 \mid (\mathcal{I}[m/x](b) =$ true und $(m,n) \in [\![\pi_1]\!])$ oder $(\mathcal{I}[m/x](b) =$ false und $(m,n) \in [\![\pi_2]\!])\}$

(iv) $[\![\underline{\text{while}}\ b\ \underline{\text{do}}\ \pi_1]\!] = \{(m,n) \in \mathbb{N}^2 \mid$ es ex. $k \in \mathbb{N}$, $a_0, \ldots, a_k \in \mathbb{N}$ mit $m = a_0$ und $n = a_k$ und $\mathcal{I}[n/x](b) =$false und f.a. $i \in \mathbb{N}$ mit $i < k$ gilt: $\mathcal{I}[a_i/x](b) =$true und $(a_i, a_{i+1}) \in [\![\pi_1]\!]\}$

Wir wollen jetzt zeigen:
Für jedes WHILE-Programm π läßt sich eine Formel φ_π konstruieren, die die Relation $[\![\pi]\!]$ in $\mathcal{N}$ definiert. Zur Erinnerung: $\varphi \in L_k^S$ definiert die Relation $R \subseteq A^k$ in der Struktur $\mathcal{A} = (A, \beta)$, wenn:

$$R = \{(\beta(v_0), \ldots, \beta(v_{k-1})) \mid (\mathcal{A}, \beta) \models \varphi\}$$

Z.B „<“ wird in $\mathcal{N}$ definiert durch die Formel:

$$\exists v_2.\, \neg v_2 \equiv 0 \wedge v_0 + v_2 \equiv v_1$$

Alternative Formulierung (wg. Koinzidenzlemma, S.14): $\varphi \in L_k^S$ definiert $R \subseteq A^k$, wenn gilt:

$$R = \{(a_0, \ldots, a_{k-1}) \mid \mathcal{I}[a_0/v_0] \ldots [a_{k-1}/v_{k-1}] \models \varphi\},$$

wobei $\mathcal{I} = (\mathcal{A}, \beta)$ mit beliebiger Belegung $\beta : X \longrightarrow A$. Wenn wir bewiesen haben, daß sich diese Formeln φ_π konstruieren lassen, dann gilt der folgende

Satz 6.3.1 (Unentscheidbarkeit der Arithmetik). *Die Theorie Th($\mathcal{N}$) der natürlichen Zahlen (über der Signatur $S_{\text{Ar}} = \{0, 1, +, *\}$) ist unentscheidbar (also auch nicht rekursiv aufzählbar und nicht axiomatisierbar).*

Beweis. *Angenommen, Th($\mathcal{N}$) wäre entscheidbar. Dann könnten wir das Halteproblem für WHILE-Programme wie folgt lösen: Für die Eingabe $(\pi, n) \in \mathbb{WH} \times \mathbb{N}$ konstruieren wir zunächst die Formel φ_π. Dann gilt:*

$$\begin{aligned} (m,n) \in [\![\pi]\!] \quad &\Leftrightarrow \quad \mathcal{I}[m/v_0][n/v_1] \models \varphi_\pi \\ &\overset{\text{Lemma 2.5.1}}{\Leftrightarrow} \quad \mathcal{I}[n/v_1] \models \varphi_\pi[\underbrace{1 + \ldots + 1}_{m}/v_0] \end{aligned}$$

Also π hält für die Eingabe m gdw. es existiert ein $n \in \mathbb{N}$ mit

$$\begin{aligned} \mathcal{I}[n/v_1] \models \varphi_\pi[\underbrace{1+\ldots+1}_{m}/v_0] \quad &\Leftrightarrow \quad \mathcal{I} \models \exists v_1.\, \varphi_\pi[\underbrace{1+\ldots+1}_{m}/v_0] \\ &\overset{Abgeschl.}{\Leftrightarrow} \quad \mathcal{N} \models \exists v_1.\, \varphi_\pi[\underbrace{1+\ldots+1}_{m}/v_0] \\ &\Leftrightarrow \quad (\exists v_1.\, \varphi_\pi[\underbrace{1+\ldots+1}_{m}/v_0]) \in Th(\mathcal{N}) \end{aligned}$$

D.h., um zu überprüfen, ob π für m hält, braucht man nur diese Formel zu konstruieren und testen, ob sie in $Th(\mathcal{N})$ liegt $\rightsquigarrow$ Widerspruch zur Unentscheidbarkeit von $\mathcal{H}$.

Noch zu zeigen: Konstruktion von φ_π
φ_π wird durch Induktion über die Größe von π definiert:

(i) $\pi = x := t$
$\varphi_\pi =_{\text{def}} v_1 \equiv t[v_0/x]$*: Der Ausgabewert v_1 ergibt sich, in dem man den Eingabewert v_0 in den Term t einsetzt*

(ii) $\pi = \pi_1;\ \pi_2$
$\varphi_\pi =_{\text{def}} \exists v_2.\, \varphi_{\pi_1}[v_2/v_1] \wedge \varphi_{\pi_2}[v_2/v_0]$*: Es gibt einen Wert v_2, der Ausgabewert von π_1 und Eingabewert von π_2 ist*

(iii) $\pi = \underline{if}\ b\ \underline{then}\ \pi\ \underline{else}\ \pi_2$
$\varphi_\pi =_{\text{def}} (b[v_0/x] \wedge \varphi_{\pi_1}) \vee (\neg b[v_0/x] \wedge \varphi_{\pi_2})$*: Entweder b gilt für die Eingabe v_0 und der Ausgabewert v_1 ergibt sich aus v_0 mit π_1 oder b gilt nicht für die Eingabe v_0 und der Ausgabewert v_1 ergibt sich aus v_0 mit π_2*

(iv) ???

□

In Punkt (iv) haben wir ein Problem: Für $\pi = \underline{\text{while}}\ b\ \underline{\text{do}}\ \pi_1$ haben wir in der Definition von $[\![\pi]\!]$ die Schreibweise „es existiert ein $k \in \mathbb{N}$, $a_0, \ldots, a_k \in \mathbb{N}$ mit…“. Das läßt sich nicht „direkt“ in Prädiaktenlogik erster Stufe umsetzen, weil die Anzahl der Werte $a_0, \ldots a_k$ vom $\exists$-quantifizierten k abhängt.

Idee: Jede endliche Folge $(a_0, \ldots, a_k)$ (beliebiger Länge k) von natürlichen Zahlen läßt sich als ein Paar $(c, d) \in \mathbb{N}^2$ kodieren, und zwar so, daß die Aussage „a ist i-tes Element der durch (c, d) kodierten Folge“ in $\mathcal{N}$ definierbar ist. Zur Kodierung benutzen wir den aus der Zahlentheorie bekannten

Satz 6.3.2 (Chinesischer Restsatz). *Seien $m_0, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd und seien $a_0, \ldots, a_k \in \mathbb{N}$ mit $a_i < m_i$ (d.h. a_i kommt als Rest* $\mod (m_i)$ *in Frage). Dann existiert eine Zahl $a \in \mathbb{N}$ mit*

$$a \equiv a_i \mod m_i$$

für $0 \leq i \leq k$.

Beweis. *Hier nicht!* □

Idee: Eine Zahlenfolge $a_0, \ldots, a_k$ wollen wir als die Zahl a kodieren, aber dazu müssen wir noch passende Module $m_0, \ldots, m_k$ finden $\rightsquigarrow$ diese $m_0, \ldots, m_k$ können wir durch die zweite Zahl angeben. Zunächst aber die

Definition 6.3.1 (Gödelsche β-Funktion). *(a) Die* Gödelsche[1] β-Funktion $\beta : \mathbb{N}^3 \longrightarrow \mathbb{N}$ *ist definiert durch:*

$$\beta(c, d, i) =_{\text{def}} c \mod (1 + (1 + i)d)$$

(b) Das Gödelsche β-Prädikat $R_\beta \subseteq \mathbb{N}^4$ *ist definiert als der Graph von β, also*

$$R_\beta =_{\text{def}} \{(c, d, i, r) \mid r = \beta(c, d, i)\}$$

Lemma 6.3.1. *(a) Zu jeder Folge $a_0, \ldots, a_k \in \mathbb{N}$ existieren $c, d \in \mathbb{N}$ mit $\beta(c, d, i) = a_i$ für $0 \leq i \leq k$.*

(b) R_β ist in $\mathcal{N}$ definierbar durch die Formel $\varphi_\beta \in L_4^{S_{\text{Ar}}}$.

Beweis.

(a) Gesucht: Zahl d, so daß die Zahlen $1 + (1 + i)d$ paarweise teilerfremd sind und $a_i < 1 + (1 + i)d$. Wenn wir ein solches d finden, dann existiert nach dem Chinesischen Restsatz ein c mit

$$\beta(c, d, i) = a_i$$

für $0 \leq i \leq k$. Wir wählen $d = s!$ mit $s = \max\{k, a_0, \ldots, a_k\}$. Dann gilt:

$$a_i \leq s < 1 + (1 + i)s!$$

Noch zu zeigen: Paarweise Teilerfremdheit
Angenommen, $i < j$ und $1+(1+i)s!$ und $1+(1+j)s!$ besitzen gemeinsame Teiler $\rightsquigarrow$ es existiert eine Primzahl p, die beide teilt, also teilt p auch $(j - i)s!$. Wegen $j - i < k \leq s$, muß p dann eine Zahl $s' \leq s$ teilen, also $p \mid s!$. Weil p auch $1 + (1 + i)s!$ teilt, müßte $p \mid 1$ gelten. Widerspruch!

(b) Es gilt:

$$\begin{aligned}
(c, d, i, r) \in R_\beta \quad &\Leftrightarrow \quad r = \beta(c, d, i) \\
&\Leftrightarrow \quad r = c \mod (1 + (1 + i)d) \\
&\Leftrightarrow \quad r < 1 + (1 + i)d \\
&\qquad \text{und es ex. ein } q \in \mathbb{N} \text{ mit } c = q(1 + (1 + i)d) + r
\end{aligned}$$

□

[1] Kurt Gödel (1906-1978), österreichischer Mathematiker

Mit Hilfe der Gödelschen β-Funktion können wir die Definition von $[\![\underline{\text{while}}\ b\ \underline{\text{do}}\ \pi]\!]$ umformulieren.

$$\begin{aligned}[\![\underline{\text{while}}\ b\ \underline{\text{do}}\ \pi_1]\!] = \{(m,n) \in \mathbb{N}^2 \mid &\text{ es ex. } k \in \mathbb{N},\ a_0, \ldots, a_k \in \mathbb{N} \text{ mit } m = a_0 \\ &\text{und } n = a_k \text{ und } \mathcal{I}[n/x](b) = \text{false und f.a. } i \in \mathbb{N} \text{ mit } i < k \text{ gilt:} \\ &\mathcal{I}[a_i/x](b) = \text{true und } (a_i, a_{i+1}) \in [\![\pi_1]\!]\}\end{aligned}$$

$$\begin{aligned}= \{(m,n) \in \mathbb{N}^2 \mid &\text{ es ex. } k \in \mathbb{N},\ c,d \in \mathbb{N} \text{ mit } m = \beta(c,d,0) \\ &\text{und } n = \beta(c,d,k),\ \mathcal{I}[n/x](b) = \text{false und f.a. } i \in \mathbb{N} \text{ gilt:} \\ &\text{wenn } i < k \text{ dann } \mathcal{I}[\beta(c,d,i)/x](b) = \text{true und} \\ &(\beta(c,d,i), \beta(c,d,i+1)) \in [\![\pi]\!]\}\end{aligned}$$

$$\begin{aligned}= \{(m,n) \in \mathbb{N}^2 \mid &\text{ es ex. } k \in \mathbb{N},\ c,d \in \mathbb{N} \text{ mit } R_\beta(c,d,0,m) \\ &\text{und } R_\beta(c,d,k,n),\ \mathcal{I}[n/x](\neg b) = \text{true und f.a. } i,u,v \in \mathbb{N} \text{ gilt:} \\ &\text{wenn } i < k,\ R_\beta(c,d,i,u),\ R_\beta(c,d,i+1,v), \text{ dann} \\ &\mathcal{I}[u/x](b) = \text{true und } (u,v) \in [\![\pi]\!]\}\end{aligned}$$

Also ist $[\![\underline{\text{while}}\ b\ \underline{\text{do}}\ \pi]\!]$ definierbar durch die Formel:

$$\begin{aligned}&\exists k, c, d.\ \varphi_\beta[c/v_0][d/v_1][0/v_2][v_0/v_3] \\ &\wedge \varphi_\beta[c/v_0][d/v_1][k/v_2][v_1/v_3] \wedge \neg b[v_0/x] \\ &\wedge \forall i, u, v.\ i < k \wedge \varphi_\beta[c/v_0][d/v_1][i/v_2][u/v_3] \\ &\wedge \varphi_\beta[c/v_0][d/v_1][i+1/v_2][v/v_3] \\ &\rightarrow b[u/x] \wedge \varphi_\pi[u/v_0][v/v_1]\end{aligned}$$

Damit ist der Beweis der Unvollständigkeit der Arithmetik abgeschlossen. Eigentlich hätte man im obigen Beweis noch die Relation $i < k$ geeignet ersetzen müssen, da $< \notin S_{\text{Ar}}$; der Übersicht halber wurde dies aber nicht gemacht. Wir haben „nebenbei“ bewiesen:

Satz 6.3.3. *(a) Jede partielle berechenbare Funktion $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ ist definierbar in der Struktur $\mathcal{N}$.*

(b) Jede rekursiv aufzählbare Menge $M \subseteq \mathbb{N}^k$ ist definierbar in $\mathcal{N}$.

Bemerkung 6.3.1. *Zur Erinnerung: eine (partielle) Funktion $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ heißt (partiell) berechenbar, wenn es eine Turingmaschine (oder ein Turingmächtiges Berechnungsmodell) $\mathcal{M}$ gibt, so daß*

- *$(x_1, \ldots, x_k) \in Def(f)$, dann liefert $\mathcal{M}$ bei Eingabe $x_1, \ldots, x_k$ die Ausgabe $f(x_1, \ldots, x_n)$,*
- *$(x_1, \ldots, x_k) \notin Def(f)$, dann liefert $\mathcal{M}$ bei Eingabe von $x_1, \ldots, x_k$ keine Ausgabe (hält also nicht)*

Ist f zusätzlich total, so sagt man, f ist total berechenbar.

Beweis.

(a) *Da f berechenbar ist, existiert ein* `WHILE`*-Programm π (mit k Variablen), das die Funktion f berechnet (wobei das Ergebnis in der ersten Variablen stehen soll). Da $[\![\pi]\!]$ durch eine Formel $\varphi_\pi \in L^S_{2k}$ definierbar ist, ist f durch*

$$(\exists v_{k+1}, \ldots, v_{2k-1}.\, \varphi_\pi) \in L^S_{k+1}$$

definierbar.

(b) *Da M rekursiv aufzählbar ist, ist M auch akzeptierbar, d.h. es existiert ein* `WHILE`*-Programm π (mit k Variablen), das genau für die Elemente aus M hält. Da $[\![\pi]\!]$ durch φ_π definierbar ist, ist M durch*

$$(\exists v_{k+1}, \ldots, v_{2k-1}.\, \varphi_\pi) \in L^S_k$$

definierbar.

□

Bemerkung 6.3.2. *Es gibt sogar noch „viel mehr“ Mengen, die in $\mathcal{N}$ definierbar sind, z.B.: Jede Menge, deren Komplement rekursiv aufzählbar ist (man nennt diese Mengen auch* co-rekursiv aufzählbar*), ist definierbar (durch die Formel $\neg\varphi$, falls φ das Komplement definiert). Man beachte: im allgemeinen ist das Komplement einer rekursiv aufzählbaren Menge nicht rekursiv aufzählbar (denn es gilt ja: M entscheidbar $\Leftrightarrow$ M und das Komplement $\overline{M}$ sind rekursiv aufzählbar).*

Frage: Sind alle Teilmengen $M \subseteq \mathbb{N}^k$ in der Struktur $\mathcal{N}$ definierbar?

Antwort: Nein, denn es gibt überabzählbar viele Teilmengen von $\mathbb{N}^k$ ($\wp(\mathbb{N})$ ist bereits überabzählbar), aber nur abzählbar viele Formeln in $L^{S_{\mathrm{Ar}}}_k$

Frage: Läßt sich eine konkrete Menge angeben, die nicht definierbar ist?

Dazu: In Analogie zur Berechenbarkeitstheorie. Zum Beweis der Unentscheidbarkeit des Halteproblems betrachtet man die Menge aller Programme (Turingmaschinen), die „nicht auf sich selbst halten“ und zeigt dann, daß diese Menge nicht rekursiv aufzählbar sein kann.

Hier: Man betrachtet die Menge aller Formeln, die „nicht für sich selbst gelten“, und zeigt, daß diese Menge nicht definierbar sein kann.

Genauer: Wir betrachten eine Aufzählung $\varphi_0, \varphi_1, \ldots$ aller Formeln in L^S. Die Zahl n mit $\varphi = \varphi_n$ bezeichnet man als *Gödelnummer* oder *Gödelnumerierung* von φ. Schreibweise: $\#\varphi$, weitere Schreibweise: $\underline{n}$ steht abkürzend für $\underbrace{1 + \ldots + 1}_{n}$

Satz 6.3.4. *(a) Die Menge* $D = \{\#\varphi \mid \varphi \in L_1^S \text{ und } \mathcal{N} \not\models \varphi[\underline{\#\varphi}/v_0]\}$ *(die Menge aller Formeln, die „nicht für sich selbst gelten“) ist nicht definierbar in* $\mathcal{N}$*.*

(b) Die Menge $\#Th(\mathcal{N}) = \{\#\varphi \mid \varphi \in Th(\mathcal{N})\}$ *ist nicht definierbar in* $\mathcal{N}$*.*

Beweis.

(a) Angenommen, es existiert eine Formel $\varphi_D \in L_1^S$*, die* D *definiert. Dann betrachtet man die Formel*

$$\varphi_D[\underline{\#\varphi_D}/v_0]$$

Es gilt dann:

$$\begin{aligned} \mathcal{N} \models \varphi_D[\underline{\#\varphi_D}/v_0] &\overset{\text{Def. von } \varphi_D}{\Leftrightarrow} \#\varphi_D \in D \\ &\overset{\text{Def. von } D}{\Leftrightarrow} \mathcal{N} \not\models \varphi_D[\underline{\#\varphi_D}/v_0] \end{aligned}$$

*Widerspruch (*Liar's paradox, Lügnerparadoxon*)*

(b) Angenommen, $\#Th(\mathcal{N})$ *wäre definierbar in* $\mathcal{N}$ *durch eine Formel* φ_{Th}*. Dann definieren wir* $f : \mathbb{N} \rightharpoonup \mathbb{N}$ *mit*

$$f(n) = \begin{cases} \#(\neg\varphi_n[\underline{\#\varphi_n}/v_0]), & \text{falls } \varphi_n \in L_1^S \\ \text{undefiniert}, & \text{sonst} \end{cases}$$

f *ist eine partielle berechenbare Funktion und es gilt:*

$$f^{-1}(\#Th(\mathcal{N})) = D, \text{ denn:}$$

$$\begin{aligned} n \in f^{-1}(\#Th(\mathcal{N})) &\Leftrightarrow f(n) \in \#Th(\mathcal{N}) \\ &\Leftrightarrow \#(\neg\varphi_n[\underline{\#\varphi_n}/v_0]) \in \#Th(\mathcal{N}) \\ &\overset{\#\text{ injektiv}}{\Leftrightarrow} \neg\varphi_n[\underline{\#\varphi_n}/v_0] \in Th(\mathcal{N}) \\ &\Leftrightarrow \mathcal{N} \models \neg\varphi_n[\underline{\#\varphi_n}/v_0] \\ &\overset{\text{Abgeschl.}}{\Leftrightarrow} \mathcal{N} \not\models \varphi_n[\underline{\#\varphi_n}/v_0] \\ &\Leftrightarrow \#\varphi_n \in D \\ &\Leftrightarrow n \in D \end{aligned}$$

Da f *als berechenbare Funktion durch eine Formel* $\varphi_f \in L_2^S$ *definierbar ist, folgt:* D *ist definierbar durch die Formel*

$$\exists v_1 . \varphi_f \wedge \varphi_{\mathrm{Th}}[v_1/v_0]$$

im Widerspruch zu (a).

□

6.3.1 Weitere Resultate über (un-)entscheidbare Theorien

Satz 6.3.5. *(a) Die Theorie $Th(\mathcal{N}^<)$ der natürlichen Zahlen über der Signatur $S^<_{\mathrm{Ar}}$ ist unentscheidbar (Gleiches gilt, wenn man andere Zeichen zu S_{Ar} hinzunimmt).*

(b) Die Theorie $Th(\mathcal{Z}^<)$ der ganzen Zahlen über der Signatur $S^<_{\mathrm{Ar}}$ ist unentscheidbar.

(c) Die Theorie $Th(\mathcal{Z})$ der ganzen Zahlen über der Signatur S_{Ar} ist unentscheidbar.

(d) Die Theorie $Th(\mathcal{Q}^<)$ der rationalen Zahlen über der Signatur $S^<_{\mathrm{Ar}}$ ist unentscheidbar.

(e) Die Theorie $Th(\mathcal{Q})$ der rationalen Zahlen über der Signatur S_{Ar} ist unentscheidbar.

Beweis.

(a) Es gilt $Th(\mathcal{N}) = Th(\mathcal{N}^<) \cap L_0^{S_{\mathrm{Ar}}}$. Wäre $Th(\mathcal{N}^<)$ entscheidbar, dann wäre auch $Th(\mathcal{N})$ entscheidbar (weil $L_0^{S_{\mathrm{Ar}}}$ entscheidbar ist, und weil der Durchschnitt zweier entscheidbarer Mengen wieder entscheidbar ist). Widerspruch!

(b),(c) Übung!

(d),(e) Nach dem gleichen Prinzip wie (b) und (c)

□

Ein interessantes und bemerkenswertes Ergebnis liefert der folgende

Satz 6.3.6. *(a) Die Theorie $Th(\mathcal{R})$ der reellen Zahlen über S_{Ar} ist entscheidbar.*

(b) Die Theorie $Th(\mathcal{R}^<)$ der reellen Zahlen über $S^<_{\mathrm{Ar}}$ ist entscheidbar.

(c) Die Theorie $Th(\mathcal{C})$ der komplexen Zahlen über S_{Ar} ist entscheidbar.

Beweis. *Hier nicht!* □

Satz 6.3.7 (Entscheidbarkeit der Presburger Arithmetik). *Die Theorie $Th(\mathcal{R})$ der natürlichen Zahlen über $S_{\mathrm{Pb}} = \{0, 1, +\}$ (oder über $S^<_{\mathrm{Pb}} = \{0, 1, +, <\}$) ist entscheidbar. Ebenso $Th(\mathcal{N}^\sigma)$ der natürlichen Zahlen über $\{0, 1, \sigma\}$ oder $\{0, 1, \sigma, <\}$, wobei σ die Nachfolgerfunktion ist.*

Beweis. *Idee: Man beweist dies durch die Angabe eines konkreten Entscheidungsalgorithmus (sehr ineffizient und kompliziert).*

□

Satz 6.3.8. *Die Theorie $Th(\mathcal{K}^S)$ aller allgemeingültigen Formeln aus L_0^S ist im algemeinen unentscheidbar („im allgemeinen“ heißt: wenn die Signatur nicht zu einfach ist).*

Beweis. *Hier nicht!* □

Kapitel 7

Prädikatenlogik zweiter Stufe

„Gott hat alle Sprachen zu seinem Lob und zu seiner Ehre geschaffen.“
Johannes XXIII. (1881-1963)

7.1 Vor- und Nachteile der Prädikatenlogik erster Stufe

Vorteil:
Existenz eines korrekten und vollständigen Kalküls (z.B. Sequenzenkalkül), d.h. der semantische Begriff der logischen Folgerung „$\models$“ läßt sich auf den syntaktischen Begriff der Ableitbarkeit „$\vdash$“ zurückführen ($\rightsquigarrow$ Rechnerunterstützung für Beweise: *theorem proving*).

Nachteile:

(a) Die Sprache ist nicht sehr ausdrucksstark, weil man nur über Elemente quantifizieren kann. Das führt dazu, daß sich „wichtige“ Eigenschaften von Strukturen nicht zum Ausdruck bringen lassen, wie z.B.

- Endlichkeit, Abzählbarkeit der Struktur
- Induktionsprinzip für natürliche Zahlen
- Vollständigkeit der reellen Zahlen („Jede nichtleere nach oben beschränkte Teilmenge besitzt ein Supremum“)

(b) Trotz des vollständigen Kalküls hat auch die formale Beweisbarkeit ihre Grenzen, da viele „wichtige“ Theorien nicht axiomatisierbar (da nicht entscheidbar) sind, z.B. $\mathrm{Th}(\mathcal{N})$

(a) ist auch in der „Praxis“ (Formalisierung mathematischer Sätze, Programmverifikation) hinderlich, weil man dort über Mengen, Folgen, Funktionen, etc. sprechen (und auch darüber quantifizieren) will.

Deshalb: Ausdrucksstärkere Logiken, z.B. Prädikatenlogik zweiter Stufe. Der Nachteil (a) wird dadurch weitgehend behoben, aber der Vorteil geht verloren, d.h. wir haben keinen vollständigen Kalkül mehr.

7.2 Formale Definition der Prädikatenlogik zweiter Stufe

Wir werden keine vollständige induktive Definition angeben, sondern lediglich die Erweiterungen angeben.

7.2.1 Die Syntax der Prädikatenlogik zweiter Stufe

Neben der Menge $X = \{v_0, v_1, \ldots\}$ der (Individuen-)Variablen werden weitere Variablenmengen vorgegeben, nämlich:

- für jedes $n \geq 1$ eine abzählbar unendliche Menge $\mathcal{F}^n = \{F_0^n, F_1^n, \ldots\}$ von *Funktionsvariablen* der Stelligkeit n
- für jedes $n \geq 1$ eine abzählbar unendliche Menge $\mathcal{P}^n = \{P_0^n, P_1^n, \ldots\}$ von *Prädikatvariablen* (oder *Relationsvariablen*) der Stelligkeit n

Die Signatur S ist wie früher definiert. In der induktiven Definition von Termen nehmen wir hinzu:

- Wenn $t_1, \ldots, t_n$ Terme sind und $F \in \mathcal{F}^n$, dann ist $F(t_1, \ldots, t_n)$ ein Term

In der induktiven Definition von Formeln nehmen wir hinzu:

- Wenn $t_1, \ldots, t_n$ Terme sind und $P \in \mathcal{P}^n$, dann ist $P(t_1, \ldots, t_n)$ eine (atomare) Formel
- Wenn φ eine Formel ist, dann sind auch $\exists F.\, \varphi$, $\forall F.\, \varphi$, $\exists P.\, \varphi$ und $\forall P.\, \varphi$ Formeln (für alle Funktionsvariablen F und Prädikatvariablen P)

Bezeichnungen: T_{II}^S und L_{II}^S für die Menge aller Terme bzw. Formeln zweiter Stufe über der Signatur S.
Die Menge frei(φ) ist wie bisher definiert unter Berücksichtigung der neuen Variablen.

7.2.2 Die Semantik der Prädikatenlogik zweiter Stufe

Da Signaturen S wie bisher definiert sind, werden auch S-Strukturen $\mathcal{A}$ wie bisher definiert. Belegungen β müssen jedoch neu definiert werden (da es neue Variablen gibt): Sei $\mathcal{A} = (A, \alpha)$ eine S-Struktur. Eine zu $\mathcal{A}$ passende Belegung β ist eine Abbildung für die gilt:

- $\beta(x) \in A$ für jedes $x \in X$
- $\beta(F) : A^n \longrightarrow A$ für jedes $F \in \mathcal{F}^n$
- $\beta(P) \subseteq A^n$ für jedes $P \in \mathcal{P}^n$

Eine Interpretation $\mathcal{I}$ ist wieder ein Paar $\mathcal{I} = (\mathcal{A}, \beta)$. Die Schreibweisen $\beta[a/x]$ und $\mathcal{I}[a/x]$ werden auf Funktions- und Prädikatvariablen verallgemeinert, z.B. $\beta[g/F]$, falls $F \in \mathcal{F}^n$ und $g : A^n \longrightarrow A$ bzw. $\beta[Q/P]$, falls $P \in \mathcal{P}^n$ und $Q \subseteq A^n$.

Die Semantik von Termen und Formeln wird wie früher definiert, aber mit den folgenden zusätzlichen Fällen: Sei $\mathcal{I} = (\mathcal{A}, \beta)$, dann sei:

- $\mathcal{I}(F(t_1, \ldots, t_n)) = \beta(F)(\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n))$
- $\mathcal{I}(P(t_1, \ldots, t_n)) = \text{true} \Leftrightarrow (\mathcal{I}(t_1), \ldots, \mathcal{I}(t_n)) \in \beta(P)$
- $\mathcal{I}(\exists F.\, \varphi) = \text{true} \Leftrightarrow$ es existiert ein $g : A^n \longrightarrow A$ mit $\mathcal{I}[g/F](\varphi) = \text{true}$, falls $F \in \mathcal{F}^n$
- $\mathcal{I}(\exists P.\, \varphi) = \text{true} \Leftrightarrow$ es existiert ein $C \subseteq A^n$ mit $\mathcal{I}[C/P](\varphi) = \text{true}$, falls $P \in \mathcal{P}^n$

Analog definiert man dies für den Allquantor (oder „$\forall$“ wird wie üblich als syntaktischer Zucker aufgefaßt).
Die meisten semantischen Begriffe werden von der Prädikatenlogik erster Stufe in die zweite Stufe übernommen. Ebenfalls auch die üblichen Schreibweisen, z.B.:

- *Gültigkeit in einer Struktur $\mathcal{A}$:* $\mathcal{A} \models \varphi$
- *Allgemeingültigkeit:* $\models \varphi$
- *Logische Folgerung:* $\Phi \models \varphi$, $\Phi^{\models}$
- *Theorien:* $\text{Th}(\mathcal{K})$, $\text{Th}(\mathcal{A})$
- *Modellklassen:* $\text{Mod}(\varphi)$, $\text{Mod}(\Phi)$
- *(Endliche) Axiomatisierbarkeit*

Warnung: Die Begriffe „elementar“, „Δ-elementar“ und „elementare Äquivalenz“ beziehen sich immer auf die Prädikatenlogik erster Stufe.

Weiterhin gilt auch das Koinzidenzlemma (S.14), d.h. $\mathcal{I}(\varphi)$ hängt nur von den Belegungen $\beta(x)$, $\beta(F)$ und $\beta(P)$ ab, wobei x, F, P frei in φ vorkommen, insbesondere ist $\mathcal{I}(\varphi)$ unabhängig von β, falls φ abgeschlossen.

Beispiel 7.2.1. *(1) Die* Endlichkeit der Trägermenge *läßt sich in zweiter Stufe formulieren. Man beachte: Eine Menge $A \neq \emptyset$ ist genau dann endlich, wenn jede injektive Funktion $g : A \longrightarrow A$ auch surjektiv ist. Das können wir in zweiter Stufe formulieren:*

$$\varphi =_{\text{def}} \forall F.\ \underbrace{(\forall x, y.\, F(x) \equiv F(y) \rightarrow x \equiv y)}_{F \text{ injektiv}} \rightarrow \underbrace{(\forall y.\, \exists x.\, F(x) \equiv y)}_{F \text{ surjektiv}}$$

Also gilt: Mod(φ) = $\{\mathcal{A} \mid \mathcal{A}$ besitzt eine endl. Trägermenge$\}$. Dies ist völlig unabhängig von der Signatur S (die leere Signatur S wäre hier auch denkbar).

(2) Sei S beliebig. Dann sei φ definiert durch:

$$\varphi =_{\text{def}} \forall x, y.\, x \equiv y \leftrightarrow \forall P.\, P(x) \leftrightarrow P(y)$$

*In Worten: Zwei Elemente x und y sind gleich, wenn sie sich nicht (durch eine Eigenschaft P) unterscheiden lassen (*Leibniz*). φ ist allgemeingültig, denn: Die Richtung „$\rightarrow$“ ist klar und „$\leftarrow$:“ Man wähle eine einelementige Menge für P.*

Folgerung: Die Gleichheit $t_1 \equiv t_2$ kann als Abkürzung aufgefaßt werden für

$$\forall P.\, P(t_1) \leftrightarrow P(t_2)$$

(3) Sei $S = \{0, \sigma\}$, $\mathcal{N}^\sigma$ die S-Struktur der natürlichen Zahlen (σ steht für die Nachfolgerfunktion). Dann läßt sich $\mathcal{N}^\sigma$ bis auf Isomorphie charakterisieren durch die Axiome (diese wurden erstmals von Peano *aufgestellt, vgl. Übung):*

(P1) $\forall x.\, \neg\sigma(x) \equiv 0$

(P2) $\forall x, y.\, \sigma(x) \equiv \sigma(y) \rightarrow x \equiv y$

(P3) $\forall P.\, P(0) \wedge (\forall x.\, P(x) \rightarrow P(\sigma(x))) \rightarrow \forall x.\, P(x)$

(P1) besagt: „0 ist kein Nachfolger einer natürlichen Zahl.“, (P2) besagt: „Die Nachfolgerfunktion ist injektiv.“ und (P3) beschreibt das Induktionsprinzip.

Folgerung: In der Prädikatenlogik zweiter Stufe ist Th($\mathcal{N}^\sigma$) endlich axiomatisierbar mit den Axiomen (P1) bis (P3), denn: Wenn $\mathcal{A}$ Modell von (P1)-(P3) ist, dann ist

$$\mathcal{A} \simeq \mathcal{N}^\sigma,$$

also $\mathcal{A} \models$ Th($\mathcal{N}^\sigma$), d.h. alle Formeln aus Th($\mathcal{N}^\sigma$) sind logische Folgerungen von (P1)-(P3).

(4) Die Überlegungen aus (3) lassen sich auf $S_{\text{Pb}} = \{0, 1, +\}$ und $S_{\text{Ar}} = \{0, 1, +, *\}$ übertragen: Die Struktur $\mathcal{N}^{\text{Pb}}$ der natürlichen Zahlen über S_{Pb} läßt sich durch endlich viele Axiome bis auf Isomorphie charakterisieren. Dazu sind folgende Modifikationen durchzuführen:

- *in (P1) bis (P3) ersetzt man* $\sigma(\ldots)$ *durch* $\ldots + 1$
- *man nimmt zwei Axiome für die Addition* $+$ *hinzu, nämlich*

(A1) $\forall x.\, x + 0 \equiv x$

(A2) $\forall x, y.\, x + (y + 1) \equiv (x + y) + 1$

Analog läßt sich $\mathcal{N}$ *über* S_{Ar} *bis auf Isomorphie charakterisieren, indem man noch zwei Axiome für die Multiplikation* $*$ *hinzunimmt:*

(M1) $\forall x.\, x * 0 \equiv 0$

(M2) $\forall x, y.\, x * (y + 1) \equiv x * y + x$

Also sind auch $Th(\mathcal{N}^{\mathrm{Pb}})$ *und* $Th(\mathcal{N})$ *in der zweiten Stufe endlich axiomatisierbar.*

Folgerung: In der Prädikatenlogik zweiter Stufe gilt nicht mehr: Jede (endlich) axiomatisierbare Theorie ist rekursiv aufzählbar, denn: Wäre die Theorie zweiter Stufe von $\mathcal{N}$ *rekursiv aufzählbar, dann wäre auch die Theorie erster Stufe von* $\mathcal{N}$ *rekursiv aufzählbar, weil sie ja gerade aus den Formeln besteht, die keine Funktions- und Prädikatvariablen enthalten.*

Weitere Folgerung: Es gibt keinen korrekten und vollständigen Kalkül für die Prädikatenlogik zweiter Stufe.

Bemerkung: Dazu muß man den Begriff „Kalkül" präzise definieren: Ein Kalkül *besteht*

- *aus einer Menge* $\mathbb{SO}$ *von* „syntaktischen Objekten" *(z.B. Sequenzen)*
- *einer endlichen Menge von* Axiomen*, jedes Axiom ist eine entscheidbare Teilmenge von* $\mathbb{SO}$
- *einer endlichen Menge von* Regeln*, jede Regel mit* n *Prämissen ist eine entscheidbare Teilmenge von* $\mathbb{SO}^{n+1}$

Wenn man dann Ableitbarkeit *wie üblich definiert, so erhält man wie früher beim Sequenzenkalkül: Die aus einer entscheidbaren Menge* Φ *ableitbaren Formeln lassen sich rekursiv aufzählen. Wenn der Kalkül zudem korrekt und vollständig ist, d.h. wenn „*$\vdash$*" und „*$\models$*" übereinstimmen, so folgt: Für jede entscheidbare Menge* Φ *ist* $\Phi^{\models}$ *rekursiv aufzählbar, also müßte* $Th(\mathcal{N})$ *in der zweiten Stufe rekursiv aufzählbar sein, Widerspruch!*

(5) Sei $S = S_{\mathrm{Ar}}$ *und* $\mathcal{R}^{<}$ *die übliche Struktur der reellen Zahlen.* $\mathcal{R}^{<}$ *ist (bis auf Isomorphie) der einzige vollständig geordnete Körper, d.h* $\mathcal{R}^{<}$ *ist durch die folgenden Axiome bis auf Isomorphie eindeutig festgelegt:*

- *Körperaxiome:*

(K1) $\forall x, y.\, x + y \equiv y + x$
$\forall x, y.\, x * y \equiv y * x$

(K2) $\forall x, y, z.\, (x + y) + z \equiv x + (y + z)$
$\forall x, y, z.\, (x * y) * z \equiv x * (y * z)$

(K3) $\forall x, y.\, \exists x'.\, x + x' \equiv y$
$\forall x, y.\, \neg x \equiv 0 \rightarrow \exists x'.\, x * x' \equiv y$

(K4) $\forall x, y, z.\, x * (y + z) \equiv x * y + x * z$

- *Axiome für totale Ordnungen:*

  (O1) $\forall x.\, \neg x < x$

  (O2) $\forall x, y, z.\, x < y \wedge y < z \rightarrow x < z$

  (O3) $\forall x, y.\, x < y \vee x \equiv y \vee y < x$

- *Das „Vollständigkeitsaxiom“:* Jede nichtleere nach oben beschränkte Teilmenge M von $\mathbb{R}$ besitzt ein Supremum.

  (V) $\forall P.\, (\exists x.\, P(x)) \wedge (\exists y.\, \forall x.\, P(x) \rightarrow x < y) \rightarrow \exists y.\, (\forall z.\, (\forall x.\, P(x) \rightarrow (x < z) \vee x \equiv z)) \leftrightarrow (y < z \vee y \equiv z)$

- *Axiome über die „Verträglichkeit“ von $+$ und $*$ mit $<$:*

  – $\forall x, y, z.\, x < y \rightarrow x + z < y + z$

  – $\forall x, y, z.\, x < y \wedge 0 < z \rightarrow x * z < y * z$

(6) Abzählbarkeit der Trägermenge läßt sich in Prädikatenlogik zweiter Stufe ausdrücken.
Idee: Eine Menge ist genau dann abzählbar, wenn auf ihr eine totale Ordnung existiert, derart, daß zu jedem Element nur endlich viele kleinere Elemente existieren. (Beweis: „⇒:“ Wenn A abzählbar ist, d.h. $A = \{a_0, a_1, \ldots\}$, dann definiert man die totale Ordnung $<$ über die Indizes durch: $a_i < a_j \Leftrightarrow i < j$. „⇐:“ Wenn zu jedem $a \in A$ nur endlich viele kleinere existieren, dann definiert man die Abbildung $f : A \longrightarrow \mathbb{N}$ durch $a \mapsto |\{a' \in A \mid a' \leq a\}|$. f ist offensichtlich injektiv (das folgt unmittelbar aus der strikten Monotonie von f), denn für $a < b$ ist $f(a) < f(b)$. Also lassen sich die Elemente $a \in A$ nach ihren Funktionswerten $f(a)$ aufsteigend sortieren.)

Also läßt sich Abzählbarkeit durch die nachstehende Formel formulieren, wobei $P \in \mathcal{P}^1$, $Q \in \mathcal{P}^2$:

$$\begin{aligned} &\exists Q.\, Q \text{ ist totale Ordnung} \\ \wedge \forall x.\, \exists P.\, (&P \text{ ist endlich } \wedge \forall y.\, y < x \leftrightarrow P(y)) \end{aligned}$$

„Q ist totale Ordnung“ läßt sich ausdrücken durch:

$$\begin{aligned} &(\forall x.\, \neg Q(x, x)) \\ \wedge &(\forall x, y, z.\, Q(x, y) \wedge Q(y, z) \rightarrow Q(x, z)) \\ \wedge &(\forall x, y. Q(x, y) \vee x \equiv y \vee Q(y, x)) \end{aligned}$$

„P ist endlich“ läßt sich ausdrücken durch:

$$\begin{aligned} &\forall F.\,(\forall x.\,P(x) \to P(F(x))) \\ \wedge&(\forall x, y.\,P(x) \wedge P(y) \wedge F(x) \equiv F(y) \to x \equiv y) \\ &\to (\forall x.\,P(x) \to \exists y.\,P(y) \wedge x \equiv F(y)) \end{aligned}$$

Also haben wir eine Formel zweiter Stufe (über beliebiger Signatur S, daher auch etwas umständlicher) gefunden, deren Modelle genau die abzählbaren S-Strukturen sind.

(7) Die Negation der Formel aus Beispiel (6) charakterisiert genau die überabzählbaren S-Strukturen.

Folgerung: Der Satz von Löwenheim-Skolem (für abzählbare Signaturen) gilt in der Prädikatenlogik zweiter Stufe nicht! Auch der Kompaktheitssatz gilt nicht mehr in der zweiten Stufe, denn: Sei $\varphi_{<\infty}$ die in Beispiel (1) definierte Formel (zweiter Stufe), die genau die endlichen S-Strukturen als Modelle hat, und seien ferner $\varphi_{\geq n}$ ($n \in \mathbb{N}$) die früher definierten Formeln (erster Stufe), die genau die S-Strukturen mit mindestens n Elementen als Modelle besitzt. Betrachte

$$\Phi =_{\text{def}} \{\varphi_{<\infty}\} \cup \{\varphi_{\geq n} \mid n \in \mathbb{N}\}$$

Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ besitzt ein Modell: man nehme eine hinreichend große endliche Struktur. Φ selbst besitzt kein Modell, also gilt der Kompaktheitssatz nicht!

(8) Sei $S = \{<\}$. Dann lassen sich die Noetherschen partiellen Ordnungen in Prädikatenlogik zweiter Stufe charakterisieren (im Gegensatz zur erster Stufe, vgl. Übung).

Zur Erinnerung: Eine partielle Ordnung heißt Noethersch[1] *oder* wohlfundiert*, wenn es in ihr keine unendlich absteigenden Folgen $a_0 > a_1 > \ldots$ gibt (z.B. ist $(\mathbb{N}, <)$ wohlfundiert, aber $(\mathbb{Z}, <)$ nicht).*

Äquivalent dazu ist: Jede nichtleere Teilmenge von A besitzt (mindestens) ein minimales Element. *(Beweis: „$\Rightarrow$:“ Sei A Noethersch und $B \subseteq A$ mit $B \neq \emptyset$. Angenommen, B besitzt kein minimales Element, d.h. zu jedem Element existiert ein kleineres. Dann wählt man irgendein $b_0 \in B$ (ist möglich, da $B \neq \emptyset$) und erhält (durch Induktion) $b_1 \in B$ mit*

$$b_1 < b_0, b_2 \in B \text{ mit } b_2 < b_1, \ldots,$$

also eine absteigende Folge. „$\Leftarrow$:“ Trivial: Wenn A nicht Noethersch ist, d.h. es existiert eine absteigende Folge $a_0 > a_1 > \ldots$, dann besitzt die Menge

$$B = \{a_n \mid n \in \mathbb{N}\}$$

[1] Amalie Emmy Noether (1882-1935), dt. Mathematikerin

kein minimales Element.) Wir betrachten nun die Formel:

$$\forall P.\, (\underbrace{\exists x.\, P(x)}_{P \neq \emptyset}) \rightarrow (\underbrace{\exists y.\, P(y) \wedge (\forall z. z < y \rightarrow \neg P(z))}_{y \text{ minimal in } P})$$

Sei nun φ die Konjunktion dieser Formel mit den Axiomen für partielle Ordnungen. Dann sind die Modelle von φ genau die Noetherschen partiellen Ordnungen.

Bisher: Welche Eigenschaften von Strukturen lassen sich durch (abgeschlossene) Formeln zweiter Stufe ausdrücken?

Jetzt: Welche Eigenschaften von Elementen, Funktionen und Prädikaten lassen sich innerhalb einer Struktur $\mathcal{A}$ (durch offene Formeln zweiter Stufe) formulieren?

Wir haben bereits gesehen:

- F ist injektiv
- F ist surjektiv (also auch: F ist bijektiv)
- P ist nichtleer
- P ist endlich
- x ist kleinstes (größtest, minimales) Element, obere (kleinste obere) Schranke von P mit $S = \{<, \ldots\}$

Weitere definierbare Eigenschaften:

- $P \subseteq Q$: $\forall x.\, P(x) \rightarrow P(y)$
- $P = Q$: $\forall x.\, P(x) \leftrightarrow P(y)$
- $F = G$: $\forall x.\, F(x) = G(x)$
- $P = F(Q)$: $\forall x.\, P(x) \leftrightarrow (\exists y.\, Q(y) \wedge x \equiv F(y))$
- $P = F^{-1}(Q)$: $\forall x.\, P(x) \leftrightarrow Q(F(x))$

Zunächst drei weitere Beispiele

Beispiel 7.2.2 („Induktive Definition“). *(1) Einfaches Beispiel einer induktiv definierten Menge: Die Menge $G \subseteq \mathbb{N}$ der (positiven) geraden Zahlen läßt sich induktiv definieren durch:*

(a) $0 \in G$

(b) Für alle $n \in \mathbb{N}$ gilt: $n \in G \Rightarrow n + 2 \in G$

Was heißt „induktiv definiert“? Es bedeutet, daß G (bezüglich der Teilmengenbeziehung „$\subseteq$“) die kleinste Menge M oder der Durchschnitt aller Mengen M ist mit den Eigenschaften

(a) $0 \in M$

(b) Für alle $n \in \mathbb{N}$ *gilt:* $n \in M \Rightarrow n + 2 \in M$

Die obige Definition reicht nicht aus, um G eindeutig festzulegen, denn sie gilt zudem auch für die Menge der natürlichen Zahlen selbst, daher der Zusatz „kleinste Menge“ bzw. „Durchschnitt aller Mengen“.
Wenn wir noch den Begriff „Menge M“ durch den Begriff „Eigenschaft P“ ersetzen, so erhalten wir: Ein Element $n \in \mathbb{N}$ gehört genau dann zu G, wenn es alle Eigenschaften P erfüllt, für die gilt:

(a) $P(0)$

(b) $\forall x.\, P(x) \to P(x+2)$

Also läßt sich G in der S_{Ar}-Struktur $\mathcal{N}$ durch folgende Formel (zweiter Stufe) definieren:

$$\forall P.\, (P(0) \wedge (\forall x.\, P(x) \to P(x+2))) \to P(v_0)$$

Nochmal in Worten: Eine natürliche Zahl v_0 ist genau dann gerade, wenn für alle Eigenschaften P gilt: Wenn Induktionsanfang $P(0)$ und Induktionsschritt $\forall x.\, P(x) \to P(x+2)$ gelten, dann gilt $P(v_0)$
$\rightsquigarrow$ Man kann ein neues Prädikatzeichen „even“ als syntaktischen Zucker einführen:

$$\mathit{even}(t) =_{\mathrm{def}} \forall P.\, P(0) \wedge (\forall x.\, P(x) \to P(x+2)) \to P(t)$$

für jeden Term $t \in T^S$. Dann kann man beweisen, daß „even“ die „gewünschten Eigenschaften“ erfüllt:

(a) $\mathit{even}(0)$, *d.h.*

$$\forall P.\, P(0) \wedge (\forall x.\, P(x) \to P(x+2)) \to P(0)$$

Diese Formel ist allgemeingültig (sie hätte eigentlich nur in $\mathcal{N}$ gültig sein müssen).

(b) $\forall y.\, \mathit{even}(y) \to \mathit{even}(y+1)$, *d.h.*

$$\begin{aligned} &\forall y.\, (\forall P.\, P(0) \wedge (\forall x.\, P(x) \to P(x+2)) \to P(y)) \\ \to\ &(\forall P.\, P(0) \wedge (\forall x.\, P(x) \to P(x+2)) \to P(y+2)) \end{aligned}$$

Diese Formel ist auch allgemeingültig!

(c) $\forall P.\, P(0) \wedge (\forall x.\, P(x) \rightarrow P(x+2)) \rightarrow (\forall y.\ even(y) \rightarrow P(y))$, *das „Induktionsprinzip“ für gerade Zahlen, ausgeschrieben also:*

$$\forall P.\, P(0) \wedge (\forall x.\, P(x) \rightarrow P(x+2)) \rightarrow (\forall y.\, (\forall P.\, P(0) \wedge (\forall x.\, P(x) \rightarrow P(x+2)) \rightarrow P(y)) \rightarrow P(y)$$

Diese Formel ist ebenfalls allgemeingültig, wie man sich leicht überlegt.

Die Forderungen (a), (b) und (c) genügen dann, um mit dem neuen Prädikat „even“ zu arbeiten, die eigentliche Definition von „even“ (als Abkürzung) spielt dann keine Rolle mehr.

Die gleichen Überlegungen lassen sich für alle induktiv definierten Mengen ($\subseteq A^k$, A Trägermenge) durchführen.

(2) *Sei A eine Menge und R eine Relation. Dann läßt sich der* reflexive und transitive Abschluß *R^* von R induktiv definieren durch:*

(a) *Für alle $a \in A$ gilt: $(a,a) \in R^*$*

(b) *Für alle $a,b,c \in A$ gilt: Wenn $(a,b) \in R$ und $(b,c) \in R^*$, dann $(a,c) \in R^*$*

Sei nun $S = \{r\}$, wobei r ein zweistelliges Relationszeichen ist, und sei $\mathcal{A}$ eine S-Struktur mit Trägermenge A. Dann läßt sich der reflexive und transitive Abschluß der Relation $r^{\mathcal{A}}$ durch folgende Formel (zweiter Stufe) definieren:

$$\forall P.\, (\forall x.\, P(x,x)) \wedge (\forall x,y,z.\, r(x,y) \wedge P(y,z) \rightarrow P(x,z)) \rightarrow P(v_0,v_1)$$

Wenn wir nun noch „$\forall v_0, v_1.$“ über diese Formel setzen, so erhalten wir eine Formel φ zweiter Stufe mit:

$$\mathcal{A} \models \varphi \Leftrightarrow \textit{Alle Paare } (a,b) \in A^2 \textit{ liegen im refl., trans. Abschluß von } r^{\mathcal{A}}$$

Sei dann

$$\psi =_{\text{def}} \varphi \wedge (\forall x.\, \neg r(x,x)) \wedge (\forall x,y.r(x,y) \rightarrow r(y,x))$$

Dann gilt offensichtlich:

$$\mathcal{A} \models \psi \Leftrightarrow \mathcal{A} \textit{ ist zusammenhängender Graph}$$

(3) *Beispiel eine induktiv definierten Funktion: Die* Fakultät *läßt sich induktiv definierten durch*

- $fact(0) = 1$
- $fact(n+1) = (n+1) * fact(n)$

Das ist nichts anderes als eine induktive Definition des Graphen Fact der Funktion fact:

(a) $(0,1) \in \mathit{Fact}$

(b) $(x,y) \in \mathit{Fact} \Rightarrow (x+1,(x+1)*y) \in \mathit{Fact}$

Also läßt sich die Relation Fact definieren durch die Formel:

$$\begin{aligned} \mathit{Fact}(v_0,v_1) =_{\text{def}} \forall P.\, P(0,1) \\ \wedge(\forall x,y.\, P(x,y) \rightarrow P(x+1,(x+1)*y)) \rightarrow P(v_0,v_1) \end{aligned}$$

Man kann dann schließlich zeigen, daß:

$$\mathcal{N} \models \forall v_0.\, \exists^{=1} v_1.\, \mathit{Fact}(v_0,v_1)$$

und anschließend ein neues Funktionszeichen *einführen durch das „Axiom“:*

$$\forall v_0, v_1.\, \mathit{fact}(v_0) \equiv v_1 \leftrightarrow \mathit{Fact}(v_0,v_1)$$

7.3 Fazit

Die Prädikatenlogik zweiter Stufe ist sehr ausdrucksstark (sowohl bei Eigenschaften von Strukturen, al1s auch bei der Definierbarkeit von Mengen oder Funktionen).

Grenzen der Ausdruckskraft

Nun drängt sich wieder die Frage auf „Gibt es auch Grenzen?“ Die Antwort liegt wieder auf der Hand: Ja, denn es gibt zum Beispiel überabzählbare viele Teilmengen von $\mathbb{N}$, aber nur abzählbar viele Formeln zweiter Stufe über S_{Ar}.

Beispiel einer nicht definierbaren Menge:
Wie in der Prädikatenlogik erster Stufe zeigt man:

$$\#\text{Th}(\mathcal{N}) = \{\#\varphi \mid \mathcal{N} \models \varphi\}$$

ist nicht definierbar durch eine Formel zweiter Stufe über der Signatur der Arithmetik S_{Ar}. (*„Truth in $\mathcal{N}$ ist not definable in $\mathcal{N}$“*)

Folgerung: *Sei $M = \{\#\varphi \mid \models \varphi\}$. Dann ist M nicht definierbar (durch eine Formel zweiter Stufe) in $\mathcal{N}$.*

Beweis: Angenommen, M ist definierbar. Sei

$$\begin{array}{rcl} f : \mathbb{N} & \longrightarrow & \mathbb{N} \\ \#\varphi & \mapsto & \#(\psi \rightarrow \varphi) \end{array}$$

wobei ψ die Konjunktion der Axiome zweiter Stufe für $\mathrm{Th}(\mathcal{N})$ ist. f ist eine total berechenbare Funktion, also definierbar, sogar durch eine Formel erster Stufe. Es gilt:

$$\begin{aligned} f^{-1}(M) &= \{\#\varphi \mid \underbrace{\#(\psi \to \varphi) \in M}_{\models \psi \to \varphi}\} \\ &= \{\#\varphi \mid \psi \models \varphi\} \\ &= \{\#\varphi \mid \varphi \in \mathrm{Th}(\mathcal{N})\} \\ &= \#\mathrm{Th}(\mathcal{N}) \end{aligned}$$

Aus der Definierbarkeit von M und f folgt die Definierbarkeit von $f^{-1}(M)$ (vgl. hierzu auch Übung), also die Definierbarkeit von $\#\mathrm{Th}(\mathcal{N})$, Widerspruch! $\square$

Anhang A

Ausgewählte Aufgaben

Aufgabe 1: Ordnen Sie den folgenden sprachlichen Gebilden einen Wahrheitswert zu, falls dies möglich ist! Begründung!

(a) „$a^2 + b^2 = c^2$“

(b) „Jedes Quadrat ist ein Rechteck.“

(c) „Jedes Parallelogramm ist ein Rechteck.“

(d) „Dieser Satz ist falsch.“

(e) „Dieser Satz ist wahr.“

(f) „Eis ist ein Wort mit drei Buchstaben.“

(g) „Eis ist gefrorenes Wasser.“

(h) „Dieser Satz besteht aus sechs Wörtern.“

(i) „Dieser Satz kein Verb.“

(j) „Eine Rose ist eine Rose.“

(k) „Fährmann, hol' über!“

Aufgabe 2: Wo liegt beim folgenden Beweis der Hase im Pfeffer?

Beh.: Es gibt ein Einhorn.

Bew.: Wir zeigen die stärkere Aussage, daß es ein existierendes Einhorn gibt.

Wir untersuchen die folgenden Fälle:

1. Ein existierendes Einhorn existiert.
2. Ein existierendes Einhorn existiert nicht.

Fall 2 trifft offensichtlich nicht ein, wie soll denn ein existierendes Einhorn nocht existieren? Somit kann also nur Fall 1 eintreten, womit gezeigt ist, daß ein existierendes Einhorn existiert, also, daß insbeosndere ein Einhorn existiert. *q.e.d.*

Aufgabe 3: Auf einer Insel leben Ritter und Schurken, wobei Ritter immer die Wahrheit sagen und Schurken immer lügen. Wir treffen auf der Insel drei Personen A, B und C, die das folgende sagen:

A: „Wir sind alle Schurken."

B: „Genau einer von uns ist ein Ritter."

Der Vollständigkeit und guten Ordnung halber sei erwähnt, daß C gar nichts sagt. Was sind A, B und C?

Aufgabe 4: Geben Sie eine induktive Definition für die Menge der Teilformeln einer gegebenen Formel an.

Aufgabe 5: Formalisieren Sie die folgenden Aussagen für natürliche Zahlen a, b, c in der Sprache der Logik mit der Signatur $S_{\mathrm{Ar}} = \{0, 1, +, *\}$. Benutzen Sie dabei die intuitive Bedeutung der Funktions- und Konstantensymbole.

(a) „a teilt b."

(b) „a ist ungerade."

(c) „a ist gemeinsamer Teiler von b und c."

(d) „a ist der ggT von b und c."

(e) „a ist eine Quadratzahl."

Aufgabe 6: Zeigen Sie: Ist S eine endliche oder abzählbar unendliche Signatur, so sind die Menge T^S der Terme über S und die Menge L^S der Formeln über S abzählbar unendlich.

Aufgabe 7: Sei S eine Signatur. Wie sieht die Menge T^S der Terme und die Menge L^S der Formeln über S aus, wenn

(a) S leer ist,

(b) S nur aus Konstantenzeichen besteht,

(c) S nur aus Funktionszeichen besteht,

(d) S nur aus Relationszeichen besteht?

Aufgabe 8: Sei A eine endliche, nichtleere Menge und S eine endliche Signatur. Zeigen Sie, daß es nur endlich viele S-Strukturen mit Träger A gibt. Wie viele sind es im Fall $|A| = 2$?

Aufgabe 9: Zeigen Sie, daß doe Klasse der in einer gegebenen Struktur definierbaren Mengen gegen

(a) Schnitt,

(b) Vereinigung,

(c) Komplement und

(d) kartesisches Produkt

abgeschlossen ist.

Aufgabe 10: Für eine Menge M heißt eine surjektive Funktion $\nu : \mathbb{N} \longrightarrow M$ *Numerierung von* M und eine injektive Funktion $\gamma : M \longrightarrow \mathbb{N}$ *Kodierung von* M.
Zeigen Sie, daß es eine Numerierung und eine Kodierung der Menge der Formeln über einer endlichen Signatur gibt. Sind diese bijektiv? Wie sieht es bei abzählbaren Signaturen aus?

Aufgabe 11: Die Signatur S enthalte nur das zweistellige Relationszeichen $<$. Geben Sie eine Formel über S an, die nur von Modellen mit unendlicher Trägermenge erfüllt wird.

Aufgabe 12: Sei S eine beliebige Signatur.

(a) Geben Sie für $n \geq 1$ eine Formel $\varphi_{\leq n}$ an, deren Modelle genau die Strukturen $\mathcal{A} = (A, \alpha)$ mit $|A| \leq n$ sind.

(b) Geben Sie für $n \geq 2$ eine Formel $\varphi_{=n}$ an, deren Modelle genau die Strukturen $\mathcal{A} = (A, \alpha)$ mit $|A| = n$ sind.

Aufgabe 13: Zeigen Sie, daß die folgenden Formeln allgemeingültig sind:

(a) $((\varphi \to \chi) \wedge (\chi \to \psi)) \to (\varphi \to \psi)$

(b) $\varphi \to (\chi \to \varphi)$

(c) $(\exists x.\, \varphi) \leftrightarrow \neg(\forall x.\, \neg\varphi)$

(d) $((\varphi_1 \vee \varphi_2) \to \psi) \leftrightarrow ((\varphi_1 \to \psi) \wedge (\varphi_2 \to \psi))$

(e) $((\exists .\, \varphi) \to \psi) \leftrightarrow (\forall x.\, \varphi \to \psi)$, falls $x \notin \text{frei}(\psi)$

Warum kann man in (e) auf die Bedingung $x \notin \text{frei}(\psi)$ nicht verzichten?

Aufgabe 14: Zeigen Sie, daß für eine definierbare Funktion f und eine definierbare Menge M auch

(a) $f(M)$ und

(b) $f^{-1}(M)$

definierbar sind.

Aufgabe 15: Welche der folgenden Behauptungen gelten? Beweis oder Gegenbeispiel!

(a) $\mathcal{A} \not\models \varphi \Leftrightarrow \mathcal{A} \models \neg\varphi$

(b) $\mathcal{A} \models \varphi \wedge \psi \Leftrightarrow \mathcal{A} \models \varphi$ und $\mathcal{A} \models \psi$

(c) $\mathcal{A} \models \varphi \vee \psi \Leftrightarrow \mathcal{A} \models \varphi$ oder $\mathcal{A} \models \psi$

Vergleichen Sie diese Ergebnisse mit Lemma II.5.

Aufgabe 16: Sei S eine Signatur. Welche der folgendne Behauptungen gelten? Geben Sie Beweise oder Gegenbeispiel an.

(a) $\varphi \wedge \phi$ erfüllbar gdw. φ und ψ erfüllbar

(b) $\varphi \vee \psi$ erfüllbar gdw. φ oder ψ erfüllbar

(c) $\neg\varphi$ erfüllbar gdw. φ nicht erfüllbar

Aufgabe 17: Die Formeln *symm*, *refl* und *trans* seien wie in Beispiel II.3 (c) bzw. (e) definiert. Zeigen Sie, daß

(a) $\{\mathit{refl}, \mathit{symm}\} \not\models \mathit{trans}$ und

(b) $\{\mathit{refl}, \mathit{trans}\} \not\models \mathit{symm}$

Aufgabe 18: Für eine Formelmenge Φ sei ihr *Abschluß unter logischer Folgerung* $\Phi^{\models}$ definiert als

$$\Phi^{\models} =_{\text{def}} \{\varphi \mid \Phi \models \varphi\}$$

Zeigen Sie:

(a) $\Phi \subseteq \Phi^{\models}$

(b) $\Phi \subseteq \Psi \Rightarrow \Phi^{\models} \subseteq \Psi^{\models}$ (Monotonie)

(c) $(\Phi^{\models})^{\models} = \Phi^{\models}$ (Idempotenz)

(d) $\mathcal{I} \models \Phi \Leftrightarrow \mathcal{I} \models \Phi^{\models}$

Aufgabe 19: In welchen der Strukturen $\mathcal{N}$, $\mathcal{Z}$, $\mathcal{Q}$, $\mathcal{R}$ sind die folgenden Eigenschaften erfüllbar?

(a) $\Phi_1 = \{v_i < v_{i+1} \mid i \in \mathbb{N}\}$

(b) $\Phi_2 = \{v_{i+1} < v_i \mid i \in \mathbb{N}\}$

(c) $\Phi_3 = \{v_{2i} < v_{2i+1} \wedge v_{2i} < v_{2i+2} \wedge v_{2i+3} < v_{2i+1} \mid i \in \mathbb{N}\}$

(d) $\Phi_4 = \{\exists v_0.\, v_0 * v_0 \equiv 2\}$

Aufgabe 20: Eine Formel heißt *existenziell*, wenn sie mitHilfe von $\exists$, $\wedge$, $\vee$ aus quantorenfreien Formeln aufgebaut ist.
Zeigen Sie, daß für Strukturen mit $\mathcal{A} \subseteq \mathcal{B}$ und eine abgeschlossene existenzielle Formel φ aus $\mathcal{A} \models \varphi$ auch $\mathcal{B} \models \varphi$ folgt.
Hinweis: Man formuliere zuerst eine passende Behauptung für beliebige existenzielle Formeln. Zeigen Sie, daß man in der obigen Behauptung nicht auf die Abgeschlossenheit von φ verzichten kann.

Aufgabe 21: Geben Sie induktiv über den Aufbau von Termen und Formeln eine Kodierung der Terme bzw. Formeln über der Signatur der Arithmetik an, die die abstrakte Syntax wiederspiegelt. Verwenden Sie dazu die (injektive und primitv-rekursive) Tupelkodierung

$$\langle . \rangle : \mathbb{N}^* \longrightarrow \mathbb{N},\ (x_0, \ldots, x_{n-1}) \mapsto \langle x_0, \ldots, x_{n-1} \rangle := \prod_{i<n} p_i^{x_i+1}$$

Hierbei bezeichne p_i die i-te Primzahl (also $p_0 = 2$, $p_1 = 3$,...).

Aufgabe 22: Mit der Substitution läßt sich der Quantor „es gibt genau ein“ wiedergeben.

(a) Führen Sie $\exists^{=1} x.\, \varphi$ („es gibt genau ein x, so daß φ“) als Kurzschreibweise (syntaktischen Zucker) für eine entsprechende Formel an und zeigen Sie, daß für jede Interpretation $\mathcal{I} = (\mathcal{A}, \beta)$ gilt:

$$\mathcal{I} \models \exists^{=1} x.\, \varphi \Leftrightarrow \text{es gibt genau ein } a \in A \text{ mit } \mathcal{I}[a/x] \models \varphi$$

(b) Für $n \geq 1$ gebe man in ähnlicher Weise die Quantoren „es gibt genau n“, „es gibt höchstens n“ und „es gibt mindestens n“ wieder.

Aufgabe 23: Sei S die Signatur mit $C = \{0\}$ und $F_1 = \{\sigma\}$ und $\mathcal{N}^\sigma = (\mathbb{N}, \sigma^{\mathcal{N}}, 0^{\mathcal{N}})$ die Struktur der natürlichen Zahlen mit $\sigma^{\mathcal{N}}(n) = n + 1$ für alle $n \in \mathbb{N}$.
Zeigen Sie, daß jede Struktur $\mathcal{A} = (A, \sigma^{\mathcal{A}}, 0^{\mathcal{A}})$, die die Axiome

(P1) $\forall x.\, \neg(\sigma(x) \equiv 0)$

(P2) $\forall x.\, \forall y.\, (\sigma(x) \equiv \sigma(y) \rightarrow x \equiv y)$

(P3) $\forall P.\, ((P0 \wedge \forall x.\, (Px \rightarrow P(\sigma(x))) \rightarrow \forall y.\, Py$

erfüllt, zu $\mathcal{N}^\sigma$ isomorph ist.
Man beachte, daß (P3) eine Formel zweiter Stufe ist, da über ein einstelliges Prädikat P quantifiziert wird. Überlegen Sie zunächst, wie sich eine zweistufige Formel in sinnvoller Weise interpretieren läßt.

Aufgabe 24: Die Formel

$$(\exists x.\, \forall y.\, x \leq y) \rightarrow \forall y.\, \exists x.\, x \leq y$$

läßt sich in sechs Schritten mit Hilfe der Regel ($\rightarrow$ S), ($\forall$ S), ($\forall$ A), ($\exists$ S), ($\exists$ A) und (Vor) herleiten. In welcher Reihenfolge muß man die Regeln (im Rückwärtsbeweis) anwenden? Kommen unterschiedliche Reihenfolgen in Frage? Wenn ja, wieviele?

Aufgabe 25: Leiten Sie die folgenden Regeln im Sequenzenkalkül Σ ab.

($\neg\neg$ S) $\dfrac{\Gamma \quad \varphi}{\Gamma \quad \neg\neg\varphi}$ ($\neg\neg$ A) $\dfrac{\Gamma \quad \varphi \qquad \psi}{\Gamma \quad \neg\neg\varphi \quad \psi}$ ($\forall$ $\exists$) $\dfrac{\Gamma \quad \forall x.\, \varphi}{\Gamma \quad \exists x.\, \varphi}$

Aufgabe 26: Welche der folgenden Formeln sind (für beliebige φ und ψ) allgemeingültig? Leiten Sie die allgemeingültigen im Sequenzenkalkül Σ her. Benutzen Sie dabei auch die abgeleiteten Regeln.

(a) $((\forall x.\, \varphi) \wedge (\forall x.\, \psi)) \rightarrow (\forall x.\, \varphi \wedge \psi)$

(b) $((\exists x.\, \varphi) \wedge (\exists x.\, \psi)) \rightarrow (\exists x.\, \varphi \wedge \psi)$

(c) $((\forall x.\, \varphi) \vee (\forall x.\, \psi)) \rightarrow (\forall x.\, \varphi \vee \psi)$

(d) $((\exists x.\, \varphi) \vee (\exists x.\, \psi)) \rightarrow (\exists x.\, \varphi \vee \psi)$

(e) $((\exists x.\, \varphi) \to (\exists x.\, \psi)) \to (\exists x.\, \varphi \to \psi)$

Aufgabe 27: Sei Σ' der Kalkül, der aus dem Sequenzenkalkül Σ entsteht, indem wir die Regel

$$(\forall\ \exists)\quad \frac{\Gamma \quad \forall x.\, \varphi}{\Gamma \quad \exists x.\, \varphi}$$

(a) Lassen sich mit Σ' mehr Formeln (aus $\emptyset$) ableiten als mit Σ?

(b) Läßt sich mit Σ' ein Widerspruch (aus $\emptyset$) ableiten, d.h. gibt es eine Formel $\psi \in L^S$ so, daß sowohl ψ als auch $\neg\psi$ ableitbar sind?

(c) Lassen sich mit Σ' alle Formeln (aus $\emptyset$) ableiten?

(d) Welche Formeln lassen sich mit Σ' (aus $\emptyset$) ableiten? Geben Sie eine semantische Charakterisierung dieser Formeln an.

Aufgabe 28: Sei $S = \{0, \sigma\}$ und sei $\Phi \subseteq L^S$ die Formelmenge, die aus den folgenden Axiomen besteht.

(P1) $\forall x.\, \neg(\sigma(x) \equiv 0)$

(P2) $\forall x.\, \forall y.\, (\sigma(x) \equiv \sigma(y) \to x \equiv y)$

(P3) $\varphi[0/x] \wedge (\forall x.\, \varphi \to \varphi[\sigma(x)/x]) \to \forall x.\, \varphi$ (für jedes $\varphi \in L^S$)

Machen Sie sich zunächst klar, was diese Axiome bedeuten, und geben Sie dann eine Ableitung der Formel

$$\forall x.\, \neg(\sigma(x) \equiv x)$$

aus Φ an. Benutzen Sie dabei (zusätzlich zu den bisher bekannten Regeln) die folgende Variante des *modus ponens*

$$(\to \mathrm{A})\quad \frac{\Gamma \quad \varphi \qquad\qquad}{\Gamma \quad \varphi \to \psi \quad \psi}$$

Aufgabe 29: Sei $S = \{r\}$ mit einstelligem Relationszeichen r, und sei $\Phi = \{r(v_0) \vee r(v_1)\}$.

(a) Zeigen Sie, daß Φ widerspruchsfrei, aber *nicht* negationstreu ist.

(b) Wie sieht die Terminterpretation $\mathcal{I}^\Phi$ aus? Gilt $\mathcal{I}^\Phi \models \Phi$?

(c) Geben Sie eine widerspruchsfreie negationstreue Menge Ψ an mit $\Phi \subseteq \Psi \subseteq L^S$

Aufgabe 30: Sei S eine beliebige Signatur, und sei $\Phi = \{v_0 \equiv t \mid t \in T^S\} \cup \{\exists v_0, v_1\, \neg(v_0 \equiv v_1)\}$. Zeigen Sie:

(a) Φ ist widerspruchsfrei.

(b) Es gibt *keine* widerspruchsfreie Menge Θ mit $\Phi \subseteq \Theta \subseteq L^S$, die Beispiele enthält.

Diese Betrachtungen zeigen, daß wir im Beweis des Vollständigkeitssatzes tatsächlich zu einer größeren Signatur S' übergehen mußten.

Aufgabe 31: Wie sieht die Terminterpretation $\mathcal{I}^\Phi$ für eine widerspruchsvolle Menge Φ aus?

Aufgabe 32: Zeigen Sie: Wenn S abzählbar ist und $\Phi \subseteq L^S$ ein unendliches Modell besitzt, dann besitzt Φ ein abzählbar unendliches Modell.

Aufgabe 33: Sei $S = \{<\}$, wobei $<$ ein zweistelliges Relationszeichen ist. Eine (*irreflexive*) *partielle Ordnung* ist eine S-Struktur, die die folgenden Axiome erfüllt:

$$\begin{array}{ll} \text{(irrefl)} & \forall x.\, \neg(x < x) \\ \text{(asymm)} & \forall x.y.\, \neg(x < y \wedge y < x) \\ \text{(trans)} & \forall x, y, z.\, (x < y \wedge y < z) \rightarrow (x < z) \end{array}$$

Eine irreflexive partielle Ordnung heißt *wohlfundiert* oder *Noethersch*, wenn es in ihr *keine* unendlich absteigenden Folgen $a_0 > a_1 > \ldots$ gibt, z.B. ist $(\mathbb{N}, <)$ wohlfundiert, aber $(\mathbb{Z}, <)$ nicht.
Zeigen Sie, daß die Klasse aller wohlfundierten partiellen Ordnungen *nicht* Δ-elementar ist.

Aufgabe 34: Seien $\varphi, \varphi_1, \ldots \in L_0^S$ und $\Phi, \Phi_1, \ldots \subseteq L_0^S$, und sei $\mathcal{K}^S$ die Klasse *aller* S-Strukturen. Ferner sei I eine beliebige (abzählbare) Indexmenge. Beweisen Sie die folgenden Eigenschaften des Mod-Operators:

(a) $\mathrm{Mod}^S(\varphi) = \mathcal{K}^S \Leftrightarrow \varphi$ allgemeingültig
(b) $\mathrm{Mod}^S(\varphi) = \emptyset \Leftrightarrow \varphi$ unerfüllbar
(c) $\mathrm{Mod}^S(\neg\varphi) = \mathcal{K}^S \setminus \mathrm{Mod}^S(\varphi)$
(d) $\mathrm{Mod}(\varphi_1 \wedge \ldots \wedge \varphi_n) = \bigcap_{i=1}^n \mathrm{Mod}^S(\varphi_i)$
(e) $\mathrm{Mod}(\varphi_1 \vee \ldots \vee \varphi_n) = \bigcup_{i=1}^n \mathrm{Mod}^S(\varphi_i)$
(f) $\mathrm{Mod}(\Phi) = \bigcap_{\varphi\in\Phi} \mathrm{Mod}^S(\varphi)$
(g) $\mathrm{Mod}(\{\varphi_1 \ldots \varphi_n\}) = \mathrm{Mod}(\varphi_1 \wedge \ldots \wedge \varphi_n)$
(h) $\mathrm{Mod}^S(\bigcup_{i\in I} \Phi_i = \bigcap_{i\in I} \mathrm{Mod}^S(\Phi_i)$
(i) $\mathrm{Mod}^S(\{\varphi_1 \vee \ldots \vee \varphi_n \mid \varphi_i \in \Phi_i \text{ für } i = 1, \ldots, n\}) = \bigcup_{i=1}^n \mathrm{Mod}^S(\Phi_i)$
(j) $\mathrm{Mod}^S(\Phi) = \emptyset \Leftrightarrow$ es gibt eine endliche Menge $\Phi_0 \subseteq \Phi$ mit $\mathrm{Mod}^S(\Phi_0) = \emptyset$
(k) $\mathrm{Mod}^S(\bigcup_{i\in I} \Phi_i) = \emptyset \Leftrightarrow$ es gibt eine endliche Menge $I_0 \subseteq I$ mit $\mathrm{Mod}^S(\bigcup_{i\in I_0} \Phi_i) = \emptyset$
(l) $\bigcap_{i\in I} \mathrm{Mod}^S(\Phi_i) = \emptyset \Leftrightarrow$ es gibt eine endliche Menge $I_0 \subseteq I$ mit $\bigcap_{i\in I_0} \mathrm{Mod}^S(\Phi_i) = \emptyset$

Aufgabe 35: Beweisen Sie die folgenden Eigenschaften von elementaren und Δ-elementaren Klassen:

(a) Jede elementare Klasse ist Δ-elementar.

(b) $\emptyset$ und $\mathcal{K}^S$ sind elementar.

(c) Komplement, endlicher Durchschnitt und endliche Vereinigung von elementaren Klassen sind wieder elementar.

(d) Jede Δ-elementare Klasse ist Durchschnitt von elementaren Klassen.

(e) Endliche Vereinigung und beliebiger Durchschnitt von Δ-elementaren Klassen sind wieder Δ-elementar.

(f) Für jede Δ-elementare Klasse $\mathcal{K}$ gilt $\mathcal{K} = \mathrm{Mod}^S(\mathrm{Th}(\mathcal{K}))$.

(g) Für Δ-elementare Klassen $\mathcal{K}_i$ $(i \in I)$ gilt:
$\bigcap_{i\in I} \mathcal{K}_i = \emptyset \Leftrightarrow$ es gibt eine endliche Menge $I_0 \subseteq I$ mit $\bigcap_{i\in I_0} \mathcal{K}_i = \emptyset$

(h) Für jede Klasse $\mathcal{K} \subseteq \mathcal{K}^S$ gilt: $\mathcal{K}$ elementar $\Leftrightarrow \mathcal{K}$ und $(\mathcal{K}^S \setminus \mathcal{K})$ sind Δ-elementar

(i) Sei $\mathcal{K}$ elementar, $\mathcal{K}' \subseteq \mathcal{K}$. Dann gilt: $\mathcal{K}'$ elementar $\Leftrightarrow \mathcal{K}'$ und $(\mathcal{K} \setminus \mathcal{K}')$ sind Δ-elementar

Aufgabe 36: Beweisen Sie die folgenden Eigenschaften des Th-Operators.

(a) $\mathrm{Th}(\emptyset) = L_0^S$

(b) $\mathrm{Th}(\mathcal{K}^S) = \{\varphi \in L_0^S \mid \models \varphi\}$

(c) $\mathcal{K} \neq \emptyset \Rightarrow \mathrm{Th}(\mathcal{K})$ erfüllbar

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

(e) $\mathrm{Th}(\bigcup_{i\in I} \mathcal{K}_i) = \bigcap_{i\in I} \mathrm{Th}(\mathcal{K}_i)$

(f) $\mathrm{Th}(\mathcal{K}) \models \varphi \Rightarrow \varphi \in \mathrm{Th}(\mathcal{K})$

(g) $\mathrm{Th}(\mathrm{Mod}(\Phi)) = \Phi^{\models}$

(h) Für jede Theorie $\mathrm{Th} \subseteq L_0^S$ existiert eine Formelmenge $\Phi \subseteq L_0^S$ mit $\mathrm{Th} = \Phi^{\models}$

(i) Für jede Theorie $\mathrm{Th} \subseteq L_0^S$ existiert eine Klasse $\mathcal{K} \subseteq \mathcal{K}S$ mit $\mathrm{Th} = \mathrm{Th}(\mathcal{K})$

Aufgabe 37: Sei Z ein Zeichenvorrat, seien $A, B \subseteq Z^*$ und $f : Z^* \rightharpoonup Z^*$ eine partielle Funktion. Zeigen Sie:

(a) Wenn A und B entscheidbar sind, dann sind auch $A \cap B$, $A \cup B$ und $A \times B$ entscheidbar.

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

(c) Wenn A rekursiv aufzählbar ist und f berechenbar, dann sind auch $f(A)$ und $f^{-1}(A)$ rekursiv aufzählbar.

Aufgabe 38: Sei $\mathcal{K}$ eine Klasse von S-Strukturen, und sei $\mathrm{Th} \subseteq L_0^S$ eine Theorie. Zeigen Sie:

(a) Wenn $\mathcal{K}$ elementar ist, dann ist $\mathrm{Th}(\mathcal{K})$ endlich axiomatisierbar.

(b) Wenn Th endlich axiomatisierbar ist, dann ist Mod(Th) elementar.

Gelten auch die Umkehrungen?

Aufgabe 39: Sei Th eine endlich axiomatisierbare Theorie, und sei $\Phi \subseteq L_0^S$ eine *beliebige* Formelmenge mit $\mathrm{Th} = \Phi^{\models}$. Zeigen Sie, daß es dann eine endliche Menge $\Phi_0 \subseteq \Phi$ gibt mit $\mathrm{Th} = \Phi_0^{\models}$

Aufgabe 40: Sei S eine endliche Signatur und $\mathcal{A}$ eine S-Struktur mit endlicher Trägermenge. Zeigen Sie:

(a) $\mathrm{Th}(\mathcal{A})$ ist entscheidbar.

(b) $\mathrm{Th}(\mathcal{A})$ ist axiomatisierbar.

(c) $\mathrm{Th}(\mathcal{A})$ ist endlich axiomatisierbar.

Welche dieser Aussagen gelten auch für eine abzählbare Signatur S?

Aufgabe 41: (a) Sei $\mathcal{A}$ eine S-Struktur und $\mathcal{B}$ eine Unterstruktur von $\mathcal{A}$, deren Trägermenge in der Struktur $\mathcal{A}$ definierbar ist. Zeigen Sie: Wenn $\mathrm{Th}(\mathcal{A})$ entscheidbar ist, dann ist auch $\mathrm{Th}(\mathcal{B})$ entscheidbar.

(b) Sei $\mathcal{Z}^<$ die übliche Struktur der ganzen Zahlen über der Signatur $S_{\mathrm{Ar}} = \{0, 1, +, *, <\}$. Zeigen Sie, daß $\mathrm{Th}(\mathcal{Z}^<)$ unentscheidbar ist.

(c) Sei $\mathcal{Z}$ die Struktur der ganzen Zahlen über der Signatur S_{Ar}. Zeigen Sie, daß $\mathrm{Th}(\mathcal{Z})$ unentscheidbar ist. (Hinweis: Jede natürliche Zahl läßt sich als Summe von vier Quadratzahlen schreiben.)

Aufgabe 42: Für jede Menge $M \subseteq \mathbb{N}^{k+1}$ $(k \geq 1)$ seien die Mengen $\exists M \subseteq \mathbb{N}^k$ und $\forall M \subseteq \mathbb{N}^k$ definiert durch:

$$\begin{aligned} \exists M &= \{(n_1, \ldots, n_k) \mid \text{es existiert eine } n \in \mathbb{N} \text{ mit } (n_1, \ldots, n_k, n) \in M\} \\ \forall M &= \{(n_1, \ldots, n_k) \mid \text{für alle } n \in \mathbb{N} \text{ gilt } (n_1, \ldots, n_k, n) \in M\} \end{aligned}$$

Zeigen Sie:

(a) Wenn M entscheidbar ist, dann ist $\exists M$ rekursiv aufzählbar und $\forall M$ co-rekursiv aufzählbar.

(b) Für jede rekursiv aufzählbare Menge $M \subseteq \mathbb{N}^k$ existiert eine entscheidbare Menge $M' \subseteq \mathbb{N}^{k+1}$ mit $M = \exists M'$.

(c) Für jede co-rekursiv aufzählbare Menge $M \subseteq \mathbb{N}^k$ existiert eine entscheidbare Menge $M' \subseteq \mathbb{N}^{k+1}$ mit $M = \forall M'$.

Index

W

Z