Logik - SS13

Hannes Diener

basierend auf dem Skript von Dieter Spreen

Inhaltsverzeichnis

Vorwort

In der Erforschung ihrer Grundlagen hat sich die Informatik seit langem mancher Teilgebiete der mathematischen Logik bedient. Durch die Entwicklung neuerer Anwendungen wie Expertensysteme und Logik–Programmierung hat die Logik einen neuen und wichtigen Stellenwert in der Informatik erhalten. Ziel dieser Vorlesung ist, durch Vermittlung von Resultaten und Methoden der mathematischen Logik ein Verständnis solcher Anwendungen zu ermöglichen.

Einleitung

Als Informatiker stehen wir vor der Entscheidung, uns mit Logik — genauer, mit mathematischer Logik — zu beschäftigen, also werden wir uns zunächst nach dem Anliegen dieser Wissenschaft und ihrer Bedeutung für die Informatik fragen:

Was ist das Anliegen von Logik überhaupt?
Sie ist jedenfalls nicht die Wissenschaft vom richtigen (logischen) Denken, wie die Schule von Port Royal zu Beginn der Neuzeit lehrte. Wie Menschen denken, ist eine Frage, die etwa von der experimentellen Psychologie beantwortet werden kann. Logik ist aber keine Erfahrungswissenschaft, ihre Sätze sollen ja wie die der Mathematik unabhängig von Experimenten gelten. Eine verbreitete Auffassung ist die, daß

> *Logik* die Lehre von den *Schlüssen* zur *Herleitung allgemeingültiger* Sachverhalte ist,

wobei die kursiv gedruckten Begriffe noch zu definieren sind. Interessant ist hierbei vor allem die Form der Schlüsse und weniger der Inhalt des Arguments. Betrachten wir hierzu das

Beispiel 0.0.1

1. Alle Menschen sind sterblich. Sokrates ist ein Mensch. Also ist Sokrates sterblich.
2. Alle Kaninchen sind rot. Sebastian ist ein Kaninchen. Also ist Sebastian rot.

Beide Schlüsse sind von der gleichen Gestalt:

> Alle A sind B. S ist ein A. Also ist S ein B.

Die Wahrheit oder Falschheit der in einem Schluß auftretenden Prämissen und Konklusionen interessiert den Logiker nicht. Er möchte wissen, ob der Schluß *korrekt* ist. Wie das folgende Beispiel zeigt, ist es hierbei nützlich, einen vorgegebenen Schluß zu formalisieren und in Elementarschlüsse zu zerlegen:

> Wenn Manfred Aktien jener AG kauft, dann erhält er viel Dividende, falls der gegenwärtige Direktor jener AG von seinem Posten abgelöst wird. Manfred wird sich kein Haus bauen, falls er viel Dividende erhält und falls er heiratet. Wenn Manfred im Sommer nicht nach Marokko fährt, dann wird er

heiraten und sich ein Haus bauen. Falls *also* Manfred Aktien jener AG kauft, dann fährt er im Sommer nach Marokko, wenn der gegenwärtige Direktor dieser AG von seinem Posten abgelöst wird.

Übung 0.0.1 Zeige durch geeignete Formalisierung, daß dieser Schluß korrekt ist.

Ziel der Logik ist es also auch, geeignete Methoden zur Formalisierung sprachlicher Sätze zu finden, so daß die logische Struktur des Satzes leicht an seiner Formalisierung abgelesen werden kann, und Systeme von Elementarschlüssen anzugeben, aus denen sich alle Schlüsse einer vorgegebenen Familie von Schlüssen aufbauen lassen.

Was ist das Anliegen der mathematischen Logik?

Zum einen ist es die Anwendung mathematischer Methoden in der Logik, z.B. bei der Untersuchung der Syntax und Semantik der in der Logik behandelten formalen Sprachen oder der schon genannten Systeme von Schlußregeln.

Zum anderen ist es die Untersuchung der Grundlagen der Mathematik, z.B. der Widerspruchsfreiheit von mathematischen Theorien, der Beweisstärke von Systemen von Axiomen und Schlußregeln.

Anlaß zur Untersuchung der logischen Grundlagen ihrer Wissenschaft war für die Mathematiker die Entdeckung von Widersprüchen in der (naiven) Mengenlehre zu Beginn dieses Jahrhunderts, welche die sogenannte Grundlagenkrise auslöste.

Ist $R(x)$ eine Eigenschaft, so erlaubt das *Komprehensionsaxiom*

$$\exists M \forall x (x \in M \leftrightarrow R(x))$$

die Zusammenfassung aller mengentheoretischen Objekte x mit der Eigenschaft R zu einer Menge M. Betrachtet wir nun die Eigenschaft

$$R(x) \leftrightarrow x \notin x,$$

so gibt es also die Menge

$$M = \{x \mid x \notin x\}.$$

Fragen wir, ob $M \in M$ oder $M \notin M$, so gilt aufgrund des Komprehensionsaxioms

$$M \in M \leftrightarrow M \notin M.$$

Das heißt also, es ist sowohl $M \in M$ wie auch $M \notin M$. Dies ist die *Russellsche Antinomie*. Sie zeigt, daß die „naive“ Mengenlehre widerspruchsvoll ist. Nun gut, könnten wir sagen, was ist so schlimm daran? Eine schon in der scholastischen Logik bekannte Schlußregel besagt, daß aus einem Widerspruch jede Aussage folgt:

$$\frac{A, \neg A}{B}$$ „ex falso quod libet“.

Eine mathematische Theorie aber, in der jede Aussage ein Satz ist, ist von keinem besonderen Interesse.

Als Ausweg aus der schon erwähnten Grundlagenkrise sind nun verschiedene Modifikationen der Mengenlehre vorgeschlagen worden, so daß (hoffentlich) keine neuen Widersprüche auftreten können. Andererseits ist aber die mathematische Gemeinschaft aufgerüttelt worden, über ihre Methoden nachzudenken. Möglicherweise treten auch in anderen wichtigen Theorien, wie etwa der Analysis, Widersprüche auf. Um das mathematische Vorgehen auf ein sicheres Fundament zu stellen, hat Hilbert, der damals als

eine Art Papst unter den Mathematikern galt, vorgeschlagen, die Sprache der Mathematik und vor allen die Beweise zu formalisieren und zu kalkülisieren, derart daß ein Beweis ein endliches Objekt ist und mittels einer Maschine in endlich vielen Schritten überprüft werden kann, ob ein vorgelegtes Objekt ein Beweis ist. Solche formalen Systeme sollten dann daraufhin untersucht werden, ob in ihnen widersprüchliche Aussagen bewiesen werden können (*Hilbertsches Programm*). Da Widersprüche vor allem beim allzu großzügigen Umgang mit unendlichen Objekten aufgetreten waren, sollte diese Reduktion aufs Endliche die Mathematik auf ein sicheres Fundament stellen. Wie spätere Resultate von Gödel (die *Gödelschen Unvollständigkeitssätze*) gezeigt haben, läßt sich das Hilbertsche Programm in dieser Allgemeinheit aber nicht durchführen.

Warum Logik in der Informatik?

Wir könnten nun sagen, was geht das die Informatiker an, zumal deren Objekte, die Daten und Programme, i.w. endlich sind. Anlaß für das starke Interesse der Informatiker an logischen Kalkülen ist die Softwarekrise, die sich wegen der Zunahme von kundenspezifischen VLSI–Chips zu einer Hardwarekrise ausweitet.

Nehmen wir an, wir sollen ein Programm p schreiben, welches zu gegebenem Datum x einen Wert y berechnet, so daß

$$R(x, y) \ .$$

R heißt dann die *Spezifikation* unseres Problems. Das Programm p wird also eine Funktion f_p berechnen, so daß

$$\forall x \ R(x, f_p(x)) \ .$$

Hat p diese Eigenschaft, so heißt es *korrekt*. Ist unser Programm p recht klein, so bereitet der Korrektheitbeweis keine Mühe. Anders sieht es aus, wenn wir es mit einem unmfangreichen Programmpaket zu tun haben, das möglicherweise von vielen Personen geschrieben worden ist. Hier ist sich bisher damit abgeholfen worden, daß Programme für verschiedene sogenannte kritische Werte getestet wurden. Dies ist aber kein Beweis: Wir wissen dann streng genommen nur, daß das Programm für eben diese Werte korrekt arbeitet. Auslöser der sogenannten Softwarekrise waren kritische Fehlalarme in US–militärischen Angriffserkennung– und Abwehrprogrammen. Wir haben hier gesehen, daß die Testmethode zu unsicher ist, jeder Fehler kann einen Krieg auslösen. Andererseits läßt sich bei einem umfangreichen Softwarepaket der zugehörige Korrektheitsbeweis nicht mehr mit Bleistift und Papier ausführen. Hier muß der Rechner eingesetzt werden. Aus prinzipiellen Gründen läßt sich aber durch ein Programm nicht entscheiden, ob eine gegebene Aussage beweisbar ist oder nicht. Es wurden daher Kalküle entwickelt, so daß die Korrektheit eines gegebenen Programmes vom Rechner im Dialog mit dem Programmierer bewiesen werden kann. Dies ist aber insgesamt eine sehr aufwendige Vorgehensweise: erst Programmentwicklung, dann Beweiserstellung. Wir möchten beide Schritte kombinieren. Das ist das Ziel der *Logikprogrammierung*. Die Idee ist hierbei, mit weitestgehender Rechnerunterstützung zu gegebenem x die Aussage

$$\exists z \ R(x, z)$$

zu beweisen, und zwar so, daß im Beweisprozeß ein Wert y gefunden wird und für ihn

$$R(x, y)$$

mitbewiesen wird. Dieser Wert y ist dann das gesuchte Resultat, und wir wissen, daß es der Spezifikation genügt.

Im vorliegenden Buch sollen die Grundlagen dieses Ansatzes behandelt werden. Auf dem Wege hierzu werden wir wichtige Resultate der mathematischen Logik kennenlernen.

1 — Aussagenlogik

1.1 Einleitung

In der Aussagenlogik werden einfache Verknüpfungen — wie „und“, „oder“, „nicht“ — zwischen atomaren sprachlichen Gebilden untersucht. Solche atomaren Gebilde sind etwa:

A = „Paris ist die Hauptstadt von Frankreich“ B = „Mäuse jagen Elefanten“

Diese atomaren Bestandteile können wahr oder falsch sein (von der inhaltlichen Interpretation wissen wir, daß A wahr und B falsch ist). Gegenstand der Aussagenlogik ist es nun, festzustellen, ob und wie sich solche „Wahrheitswerte“ der atomaren Bestandteile zu Wahrheitswerten von komplizierteren sprachlichen Gebilden fortsetzen lassen, wie z.B.

A und B .

(Wir wissen, daß im obigen Beispiel A *und* B falsch ist, da bereits B falsch ist.)

Wir interessieren uns also nur dafür, wie sich Wahrheitswerte in komplizierteren Gebilden aus den Wahrheitswerten der einfacheren Gebilde ergeben. In diesen Untersuchungen wird letzlich ignoriert, was die zugrundeliegenden inhaltlichen Bedeutungen der atomaren Gebilde sind; unser ganzes Interesse ist auf ihre Wahrheitswerte reduziert. Falls z.B.

A = „Otto wird krank“ B = „Der Arzt verschreibt Otto eine Medizin“,

so ist es in der Umgangssprache durchaus ein Unterschied, ob wir „A *und* B“ oder „B *und* A“ sagen. Von solchen „Feinheiten“ wollen wir uns hier befreien, indem wir alle denkbaren atomaren Gebilde ohne eine inhaltliche Interpretation betrachten und mit $A_1, A_2, A_3, \ldots$ bezeichnen. Die Verknüpfungen, die wir im folgenden betrachten wollen, sind die, welche auch in mathematischen Texten am häufigsten gefunden werden: „*oder*“, „*und*“, „*nicht*“, „*impliziert*“ und „*genau dann, wenn*“.

1.2 Syntax der Aussagenlogik

Wir wollen nun die Sprache der Aussagenlogik definieren. Hierzu geben wir zuerst das Alphabet an.

Definition 1.2.1 Das *Alphabet* der *Sprache der Aussagenlogik* besteht aus folgenden Symbolen:

1. *Verknüpfungen*: $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$,
2. *Klammern*:), (,
3. *Propositionalzeichen*: $\bot (= A_1), A_2, A_3, \ldots$

$\bot$ heißt das *Falsum*.

Die folgende *induktive* Definition aussagenlogischer Ausdrücke, *Formeln* oder auch *Aussagen* genannt, beschreibt, wie aus elementaren Ausdrücken komplexe Ausdrücke aufgebaut werden.

Definition 1.2.2

1. Jedes Propositionalzeichen ist eine Formel.
2. Sind α, β Formeln, so sind auch $(\neg\alpha), (\alpha \vee \beta), (\alpha \wedge \beta), (\alpha \rightarrow \beta)$, $(\alpha \leftrightarrow \beta)$ Formeln.
3. Nur die mittels der Regeln (1), (2) und (3) gebildeten Wörter über der Sprache der Aussagenlogik sind Formeln.

Da jede Formel aus Propositionalzeichen als Elementarbestandteilen aufgebaut ist, heißen diese zuweilen auch *atomare Formeln*. Eine Formel β, die als Teil einer Formel α auftritt, heißt *Teilformel* von α.

Beispiel 1.2.3 $\alpha = (\neg((A_5 \wedge (\neg A_8)) \vee A_9))$ ist eine Formel und sämtliche Teilformeln von α sind:

$$\alpha, ((A_5 \wedge (\neg A_8)) \vee A_9), (A_5 \wedge (\neg A_8)), (\neg A_8), A_5, A_8, A_9 \ .$$

Um die Klammerschreibweise etwas zu vereinfachen, wollen wir annehmen, daß $\neg$ stärker bindet als die anderen Verknüpfungen und $\neg\alpha$ statt $(\neg\alpha)$ schreiben. Außerdem lassen wir in Zukunft die äußeren Klammern einer Formel weg. Wir schreiben also $\neg((A_5 \wedge \neg A_8) \vee A_9)$ statt $(\neg((A_5 \wedge (\neg A_8)) \vee A_9))$.

1.3 Induktive Definitionen

Die Art, in der wir definiert haben, was eine Formel ist, weicht etwas von der sonst in der Mathematik üblichen Definitionsweise ab. Wir haben gesagt, daß es eine *induktive Definition* ist. Jede solche Definition besteht aus drei Bedingungen (1), (2) und (3):

- In (1) werden die atomaren Elemente der zu definierenden Menge festgelegt.
- In (2) wird gesagt, wie aus Elementen dieser Menge weitere Elemente gebildet werden können.
- In (3) werden die Elemente der Menge auf diejenigen eingeschränkt, die entweder in (1) aufgeführt sind oder ausgehend von diesen sukzesssive gemäß (2) gebildet werden können.

Wir wollen nun präzisieren, was hier gemeint ist, und sehen, daß auf diese Weise tatsächlich eine Menge definiert wird.

Definition 1.3.1 Sei X eine Menge, F eine Menge von Funktionen $f : X^n \rightarrow X$ $(n > 0)$, und $Y, Z \subseteq X$.

1. Z ist *abgeschlossen unter* F, falls für jedes $f \in F$, sagen wir der Stelligkeit n, mit $y_1, \ldots, y_n \in Z$ auch $f(y_1, \ldots, y_n) \in Z$ ist.
2. Die Menge

$$\mathrm{IND}(Y, F) = \bigcap \{\, Z \subseteq X \mid Y \subseteq Z \text{ und } Z \text{ ist abgeschlossen unter } F \,\}$$

heißt die *induktive Hülle von* Y *unter* F.

Satz 1.3.2 Sei X, Y und F wie oben. Dann gilt

- $Y \subseteq \mathrm{IND}(Y, F)$,
- Die Menge $\mathrm{IND}(Y, F)$ ist unter F abgeschlossen, und
- für jede andere Menge $Z \subseteq X$, für die $Y \subset Z$ und die unter F abgeschlossen ist, gilt, daß $\mathrm{IND}(Y, F) \subseteq Z$; d.h. $\mathrm{IND}(Y, F)$ ist die *kleinste* solche Menge.

Beweis. Übung. ■

Nun können wir die obigen Bedingungen (1)–(3) verstehen: (1) gibt an, von welcher Menge Y wir die Hülle bilden wollen, (2) legt die Abschlußbedingungen fest, und (3) sagt, daß wir uns für die kleinste Y enthaltende und unter den in (2) genannten Funktionen abgeschlossene Menge interessieren, d.h. für die induktive Hülle von Y unter diesen Funktionen.

Ist X die Menge der Wörter über dem Alphabet der Aussagenlogik, für $\alpha \in X$ sei $f_\neg(\alpha) = (\neg\alpha)$, und sind $f_\vee, f_\wedge, f_\to$, und $f_\leftrightarrow$ entsprechend definiert, so ist die Menge der Formeln die induktive Hülle der Menge der Präpositionalzeichen unter $\{f_\neg, f_\vee, f_\wedge, f_\to, f_\leftrightarrow\}$.

Wollen wir zeigen, daß alle Elemente einer induktiv definierten Menge eine bestimmte Eigenschaft haben, so kann dies mittels *Induktion über den Aufbau* getan werden. Wir werden dieses Beweisprinzip im folgenden häufig anwenden.

Satz 1.3.3 — Prinzip der Induktion über den Aufbau. Ist E eine auf $\mathrm{IND}(Y, F)$ definierte Eigenschaft, so daß gilt:

1. Jedes Element aus Y hat die Eigenschaft E,
2. Für alle $f \in F$ (n–stellig) folgt für alle $y_1, \ldots, y_n \in \mathrm{IND}(Y, F)$, welche die Eigenschaft E haben, daß auch $f(y_1, \ldots, y_n)$ die Eigenschaft E hat,

dann haben alle Elemente von $\mathrm{IND}(Y, F)$ die Eigenschaft E.

Beweis. Sei $\widehat{E} = \{\, x \in X \mid E(x) \,\}$. Nach (1) ist $Y \subseteq \widehat{E}$. Außerdem ist $\widehat{E}$ wegen der Bedingung (2) unter F abgeschlossen. Da $\mathrm{IND}(Y, F)$ die kleinste Y enthaltende, unter F abgeschlossene Menge ist (Satz 1.3.2) folgt, daß $\mathrm{IND}(Y, F) \subseteq \widehat{E}$. D.h. alle Elemente aus $\mathrm{IND}(Y, F)$ haben die Eigenschaft E. ■

Bemerkung 1.3.4 Die Elemente einer induktiv definierten Menge $\mathrm{IND}(Y, F)$ sind entweder atomar oder Entstehen durch Anwendung einer Funktion $f \in F$ auf Elemente $(y_1, \ldots, y_n) \in \mathrm{IND}(Y, F)$.

Beweis. Trivial; Induktion über den Aufbau. ■

Es liegt also nahe, Funktionen auf induktiv definierten Mengen durch Rekursion über ihren Aufbau zu definieren. Sei B eine Menge, $h : Y \to B$ und für jedes $f \in F$ einer Stelligkeit n sei $g_f : B^n \to B$. Dann möchten wir eine Funktion $\hat{h} : \mathrm{IND}(Y, F) \to B$ definieren, so daß

$$\hat{h}(y) = h(y), \text{ für } y \in Y, \text{ und}$$
$$\hat{h}(f(y_1, \ldots, y_n)) = g_f(\hat{h}(y_1), \ldots, \hat{h}(y_n)),$$

für alle $f \in F$ und $y_1, \ldots, y_n \in \mathrm{IND}(Y, F)$. Dies geht aber nur, wenn jedes Element von $\mathrm{IND}(Y, F)$ *eindeutig* in seine Bestandteile zerlegt werden kann.

Definition 1.3.5 $\mathrm{IND}(Y, F)$ heißt *von Y und F frei erzeugt*, wenn jedes $y \in \mathrm{IND}(Y, F)$ eindeutig in seine Bestandteile zerlegt werden kann, d.h., entweder $y \in Y$ ist oder genau ein $f \in F$ mit der Stelligkeit n und genau ein Tupel $(y_1, \ldots, y_n) \in \mathrm{IND}(Y, F)^n$ existieren, so daß $y = f(y_1, \ldots, y_n)$.

Wie das folgende Beispiel zeigt, ist nicht jede induktiv erzeugte Menge auch frei erzeugt. Sei X die Menge der ganzen Zahlen, $Y = \{0\}$ und $F = \{S, P\}$, wobei S die Nachfolger– und P die Vorgängerfunktion ist. Dann ist $S(0) = P(S(S(0)))$.

Satz 1.3.6 — Prinzip der *Rekursion über den Aufbau*. Sei $\mathrm{IND}(Y, F)$ von Y und F frei erzeugt. Sei ferner $h : Y \to B$ und für jedes $f \in F$ mit der Stelligkeit n $g_f : B^n \to B$. Dann gibt es genau eine Funktion $\hat{h} : \mathrm{IND}(Y, F) \to B$, so daß

1. für alle $y \in Y$ ist $\hat{h}(y) = h(y)$,
2. für alle $f \in F$ der Stelligkeit n und alle $y_1, \ldots, y_n \in \mathrm{IND}(Y, F)$

$$\hat{h}\left(f\left(y_1, \ldots, y_n\right)\right) = g_f\left(\hat{h}\left(y_1\right), \ldots, \hat{h}\left(y_n\right)\right) .$$

Beweis. Der Beweis ist etwas abstrakt. Die Idee ist, das wir den Graph der gesuchten Funktion als induktive Menge definieren können. Sei $I = \mathrm{IND}(Y, F)$,

$$\hat{Y} = \{\, (y, h(y)) \mid y \in Y \,\} ,$$

für jedes n-stellige $f \in F$ sei $\hat{f} : (I \times B)^n \to (I \times B)$ definiert durch

$$\hat{f}\left((y_1, b_1), \ldots, (y_n, b_n)\right) = \left(f(y_1, \ldots, y_n), g_f(b_1, \ldots, b_n)\right) ,$$

und $\hat{F} = \left\{\, \hat{f} \mid f \in F \,\right\}$. Betrachten wir nun $G = \mathrm{IND}(\hat{Y}, \hat{F}) \subseteq I \times B$. Wir wollen zeigen, daß G ein Graph, daß heißt total und rechtseindeutig, ist. Dazu zeigen wir, zunächst, daß

$$E = \{\, x \in X \mid \text{es gibt ein } b \text{ mit } (x, b) \in G \,\}$$

die Menge Y enthält und unter F abgeschlossen ist. Da $(y, h(y)) \in \hat{Y} \subseteq G$ für alle $y \in Y$, ist auch $y \in E$. Sei als nächstes $f \in F$ n-stellig und $y_1, \ldots, y_n \in E$ mit $y = f(y_1, \ldots, y_n)$. Nach Definition von E gibt es $b_1, \ldots, b_n$ so daß $(y_i, b_i) \in G$ für $1 \leqslant i \leqslant n$. Da G unter $\hat{f}$ abgeschlossen ist, ist $(f(y_1, \ldots, y_n), g_f(b_1, \ldots, b_n))) \in G$, also $f(y_1, \ldots, y_n) \in E$. Also ist $I \subseteq E$, d.h. G ist total. Sei nun

$$D = \{\, x \in X \mid \text{es gibt höchstens ein } b \text{ mit } (x, b) \in G \,\} .$$

Wie oben wollen wir zeigen, daß D die Menge Y enthält und unter F abgeschlossen ist. Sei hierzu $y \in Y$ und b, b' so daß $(y, b), (y, b') \in G$. Man sieht leicht, daß, da die Menge I frei erzeugt ist, gelten muss, daß $(y, b), (y, b') \in \hat{Y}$. Damit ist aber $b = h(y) = b'$. Also gilt $Y \subseteq D$. Sei nun y so dass es eindeutig bestimmte $f \in F$ und $y_1, \ldots, y_n \in D$ mit $y = f(y_1, \ldots, y_n)$ gibt. Da es jeweils höchstens ein b_i mit $(y_i, b_i) \in G$ gibt es auch höchstens ein $b \in B$, nämlich $b = g_f(b_1, \ldots, b_n)$, so daß $(y, b) \in G$. Also ist $I \subseteq D$, d.h. G ist rechtseindeutig. Es ist ausserdem klar, daß die durch G definierte Funktion $\hat{h} : I \to B$ die gesuchten Eigenschaften hat. ■

Wie wir schon gesehen haben, ist die Menge der aussagenlogischen Formeln die induktive Hülle der Propositionalzeichen unter $\{f_\neg, f_\wedge, f_\vee, f_\to, f_\leftrightarrow\}$. Wir zeigen jetzt noch:

Satz 1.3.7 Die Menge der aussagenlogischen Formeln wird von den Propositionalzeichen und den Funktionen $f_\neg$, $f_\wedge$, $f_\vee$, $f_\to$, $f_\leftrightarrow$ frei erzeugt.

Beweis. Sei für ein Wort α über der Sprache der Aussagenlogik $Kl(\alpha)$ die Differenz zwischen der Anzahl der öffnenden Klammern „(“ in α und der Anzahl der schließenden Klammern „)“. Durch Induktion über den Formelaufbau zeigen wir zuerst die folgende

Zwischenbehauptung. *Für alle Formeln α und alle Präfixe β von α ist $Kl(\beta) \geq 0$. Ausserdem ist $Kl(\beta) = 0$ genau denn, wenn β das leere Wort ε oder $\beta = \alpha$ ist.*

Beweis der Zwischenbehauptung: Ist α ein Propositionalzeichen, so ist die Behauptung offensichtlich wahr. Seien nun α_1, α_2 Formeln und sei α eine der Formeln $(\neg\alpha_1)$, $(\alpha_1 \vee \alpha_2)$, $(\alpha_1 \wedge \alpha_2)$, $(\alpha_1 \to \alpha_2)$, $(\alpha_1 \leftrightarrow \alpha_2)$. Wir betrachten nur den Fall, daß $\alpha = (\alpha_1 \,\square\, \alpha_2)$ mit $\square \in \{\vee, \wedge, \to, \leftrightarrow\}$. Der Fall $\alpha = (\neg\alpha_1)$ läßt sich analog behandeln. Nehmen wir hierzu an, daß die obige Behauptung für α_1 und α_2 und die zugehörigen Präfixe gilt. Dann ist $Kl(\alpha) = Kl(\alpha_1) + Kl(\alpha_2) = 0$. Sei jetzt β ein Präfix von α. Dann treten folgende Fälle auf:

β ist Präfix von $(\alpha_1$. Dann ist $\beta = \varepsilon$ oder $\beta = (\beta_1$ für ein Präfix β_1 von α_1. Im ersten Fall ist $Kl(\beta) = 0$ und im zweiten aufgrund der Induktionsannahme $Kl(\beta) = 1 + Kl(\beta_1) \geq 1$. Also folgt aus $Kl(\beta) = 0$, daß $\beta = \varepsilon$.

β ist Präfix von $(\alpha_1 \,\square\, \alpha_2$, aber nicht von $(\alpha_1$. Dann ist entweder $\beta = (\alpha_1\square$ und also $Kl(\beta) = 1 + Kl(\alpha_1) = 1$, oder es gibt ein Präfix β_2 von α_2, so daß $\beta = (\alpha_1 \,\square\, \beta_2$. In diesem Fall ist $Kl(\beta) = 1 + Kl(\alpha_1) + Kl(\beta_2) \geq 1$.

Hiermit ist die Zwischenbehauptung bewiesen. Sei nun α eine Formel. Besteht α nur aus einem Zeichen, so ist α ein Propositionalzeichen. Anderenfalls gibt es Formeln α_1, α_2, so daß α eine der Formeln $(\neg\alpha_1)$, $(\alpha_1 \vee \alpha_2)$, $(\alpha_1 \wedge \alpha_2)$, $(\alpha_1 \to \alpha_2)$, oder $(\alpha_1 \leftrightarrow \alpha_2)$ ist. Nehmen wir nun an, α ließe sich auch auf andere Weise aus Teilformeln aufbauen, d.h., es existiere eine weitere Formel α' mit Teilformeln α'_1, α'_2, so daß $\alpha = \alpha'$. Betrachten wir zuerst den Fall, daß $\alpha = (\neg\alpha_1)$. Da die Wörter α und α' gleich sind, muß dann auch α' mit den Zeichen „$(\neg$“ anfangen und mit „$)$“ enden, d.h., $\alpha' = (\neg\alpha'_1)$. Ferner muß $\alpha_1 = \alpha'_1$ sein. Betrachten wir nun den Fall, daß $\alpha = (\alpha_1 \,\square\, \alpha_2)$ mit $\square \in \{\vee, \wedge, \to, \leftrightarrow\}$. Da das Wort α' jetzt nicht mit den Zeichen „$(\neg$“ beginnen kann, muß $\alpha' = (\alpha'_1 \,\Diamond\, \alpha'_2)$ sein mit $\Diamond \in \{\vee, \wedge, \to, \leftrightarrow\}$. Dann ist entweder α'_1 ein Präfix von α_1 oder α_1 ein Präfix von α'_1. Es genügt, den ersten Fall zu betrachten. Da α'_1 eine Formel ist, ist $\alpha'_1 \neq \varepsilon$. Außerdem ist nach der Zwischenbehauptung $Kl(\alpha'_1) = 0$. Nehmen wir nun an, daß $\alpha'_1 \neq \alpha_1$. Dann folgt mit eben dieser Zwischenbehauptung, daß $Kl(\alpha'_1) > 0$, ein Widerspruch. Also ist $\alpha'_1 = \alpha_1$ und folglich auch $\Diamond = \square$ und $\alpha'_2 = \alpha_2$. Somit ist gezeigt, daß jede Formel eindeutig in ihre Bestandteile zerlegt werden kann. ■

1.4 Wahrheitsfunktionen

Die Betrachtungen des letzten Abschnitts zeigen, daß wir nicht nur Beweise durch Induktion über den Formelaufbau führen, sondern auch Funktionen durch Rekursion über den Formelaufbau definieren können. Hiervon wollen wir im folgenden Gebrauch machen, wenn wir aussagenlogischen Formeln als Bedeutung einen *Wahrheitswert* **w** bzw. **f** zuordnen. Dazu müssen wir aber zuerst den aussagenlogischen Verknüpfungen $\vee, \neg, \wedge, \rightarrow, \leftrightarrow$ eine Bedeutung $H_\vee, H_\neg, H_\wedge, H_\rightarrow, H_\leftrightarrow$ zuordnen. Dies müssen Funktionen von $\{\mathbf{w}, \mathbf{f}\}$ bzw. $\{\mathbf{w}, \mathbf{f}\}^2$ in $\{\mathbf{w}, \mathbf{f}\}$ sein, da sich der Wahrheitswert einer Formel mit ihnen aus den Wahrheitswerten der Propositionalzeichen bestimmen lassen soll. Die Funktionen $H_\neg$ und $H_\wedge$ werden durch die folgenden Tabellen definiert und geben die übliche Bedeutung der sprachlichen Verknüpfungen „nicht“, „und“ wieder:

p	$H_\neg(p)$
w	**f**
f	**w**

p	q	$H_\wedge(p,q)$
w	**w**	**w**
w	**f**	**f**
f	**w**	**f**
f	**f**	**f**

Tabellen dieser Art heißen *Wahrheitstafeln*. $H_\neg$ heißt *Negation* und $H_\wedge$ *Konjunktion*. Die Bedeutung von „$\vee$“ ist das einschließende „oder“:

p	q	$H_\vee(p,q)$
w	**w**	**w**
f	**w**	**w**
w	**f**	**w**
f	**f**	**f**

In der Umgangssprache wird die oder–Verknüpfung mehr im ausschließenden Sinne gebraucht. $H_\vee$ heißt *Disjunktion*. Die Bedeutung von „$\rightarrow$“ ist die *Implikation*. Wollen wir hierfür eine Wahrheitstafel aufstellen, so stoßen wir auf große Schwierigkeiten. Offensichtlich ist die Aussage „Falls A, dann B“ falsch, wenn die Prämisse A wahr und die Konklusion B falsch ist. In allen anderen Fällen gibt es jedoch keinen wohldefinierten Wahrheitswert. Betrachten wir folgende Beispiele:

- Falls $1 + 1 = 2$, dann ist Paris die Hauptstadt Frankreichs.
- Falls $1 + 1 \neq 2$,dann ist Paris die Hauptstadt Frankreichs.
- Falls $1 + 1 \neq 2$, dann ist Rom die Hauptstadt Frankreichs.

In einer Alltagsdiskussion werden diese Aussagen weder für wahr noch für falsch gehalten werden, denn wir erwarten bei einem Konditionalsatz, daß zwischen Prämisse und Konklusion eine (i.a. kausale) Beziehung besteht. Um diesem Dilemma zu entrinnen, treffen wir in der Aussagenlogik folgende Festsetzung: „Falls A, dann B“ ist *genau dann* falsch, wenn A wahr und B falsch ist. Wir definieren daher die Funktion $H_\rightarrow$ durch

p	q	$H_\rightarrow(p,q)$
w	**w**	**w**
w	**f**	**f**
f	**w**	**w**
f	**f**	**w**

Dies entspricht dem in der Mathematik üblichen Gebrauch der Implikation. Betrachten wir folgendes Beispiel:

> Falls x eine ungerade, positive ganze Zahl ist, dann ist x^2 eine ungerade ganze Zahl.

Nun wollen wir die Fälle, in denen x keine ungerade, positive ganze Zahl ist, gewiß nicht als Gegenbeispiel für diese Aussage ansehen, d.h., die Implikation soll in diesen Fällen wahr sein. Dies entspricht den letzten beiden Zeilen in der Definition von $H_{\to}$. Auf der anderen Seite bestätigt jeder Fall, in dem x ungerade, positiv und ganz und ebenso x^2 ungerade, positiv und ganz ist, unsere Behauptung. Dies entspricht der ersten Zeile in der Definition von $H_{\to}$.

Die Definition von $H_{\leftrightarrow}$ bereitet keine Schwierigkeiten. $H_{\leftrightarrow}$ heißt *Äquivalenz* oder auch *Bikonditional*. $H_{\leftrightarrow}(p, q)$ ist genau dann wahr, wenn p und q den gleichen Wahrheitswert haben, d.h.

p	q	$H_{\leftrightarrow}(p,q)$
w	**w**	**w**
w	**f**	**f**
f	**w**	**f**
f	**f**	**w**

Durch Substitution der so definierten Funktionen ineinander lassen sich weitere Funktionen erzeugen, deren Werte sich leicht mittels der Wahrheitstafeln bestimmen lassen.

Beispiel 1.4.1 Betrachten wir die Funktion $H_{\to}(H_{\wedge}(H_{\neg}(p), q), r)$. Dann erhalten wir die zugehörige Wahrheitstafel wie folgt:

p	q	r	$H_{\neg}(p)$	$H_{\wedge}(H_{\neg}(p), q)$	$H_{\to}(H_{\wedge}(H_{\neg}(p), q), r)$
w	**w**	**w**	**f**	**f**	**w**
w	**w**	**f**	**f**	**f**	**w**
w	**f**	**w**	**f**	**f**	**w**
w	**f**	**f**	**f**	**f**	**w**
f	**w**	**w**	**w**	**w**	**w**
f	**w**	**f**	**w**	**w**	**f**
f	**f**	**w**	**w**	**f**	**w**
f	**f**	**f**	**w**	**f**	**w**

Die Spalten für $H_{\neg}(p)$ und $H_{\wedge}(H_{\neg}(p), q)$ dienen hierbei nur der Rechenerleichterung und können weggelassen werden.

Allgemein heißt jede Funktion $H : \{\mathbf{w}, \mathbf{f}\}^n \to \{\mathbf{w}, \mathbf{f}\}$ mit $n > 0$ *Wahrheitsfunktion*. Da es 2^n n–Tupel mit den Komponenten **w** und **f** gibt und jedem solchen Tupel durch eine Wahrheitsfunktion der Wert **w** bzw. **f** zugewiesen wird, haben wir

Lemma 1.4.2 Es gibt 2^{2^n} verschiedene n-stellige Wahrheitsfunktionen.

Dies ist eine große Zahl. Es stellt sich daher die Frage, ob es eine kleine — überschaubare — Menge solcher Funktionen gibt, so daß sich alle Wahrheitsfunktionen durch Verschachtelung dieser Funktionen erzeugen lassen.

Definition 1.4.3 1. Sei $n > 0$. Eine n–stellige Wahrheitsfunktion H heißt *explizit definierbar* aus den Wahrheitsfunktionen $H_1, \ldots, H_k$, wenn H definierbar ist in der Form $H(a_1, \ldots, a_n) = \ldots$, wobei die rechte Seite durch Einsetzen der Funktionen

$H_1, \ldots, H_k$ ineinander entsteht und hierbei höchstens die Argumente $a_1, \ldots, a_n$ auftreten.

2. Eine Menge M von Wahrheitsfunktionen ist *adäquat*, falls sich jede Wahrheitsfunktion explizit aus Funktionen aus M definieren läßt.

Satz 1.4.4 $\{H_\neg, H_\vee, H_\wedge\}$ ist adäquat.

Beweis. Seien für $n > 0$ $H_\wedge^{(n)}$ und $H_\vee^{(n)}$ wie folgt definiert:

$$\begin{array}{rclcrcl} H_\vee^{(1)}(p) & = & p; & & H_\vee^{(n+1)}(p_1, \ldots, p_{n+1}) & = & H_\vee(p_1, H_\vee^{(n)}(p_2, \ldots, p_{n+1})) \\ H_\wedge^{(1)}(p) & = & p; & & H_\wedge^{(n+1)}(p_1, \ldots, p_{n+1}) & = & H_\wedge(p_1, H_\wedge^{(n)}(p_2, \ldots, p_{n+1})) \end{array}$$

$(p, p_1, \ldots, p_{n+1} \in \{\mathbf{w}, \mathbf{f}\})$. Sei nun H eine k–stellige Wahrheitsfunktion. Wir betrachten zuerst den Fall, daß für alle $p_1, \ldots, p_k \in \{\mathbf{w}, \mathbf{f}\}$ $H(p_1, \ldots, p_k) = \mathbf{f}$. In diesem Fall ist

$$H(p_1, \ldots, p_k) = H_\wedge(p_1, H_\neg(p_1)).$$

Nehmen wir nun an, daß für gewisse $p_1, \ldots, p_k \in \{\mathbf{w}, \mathbf{f}\}$ $H(p_1, \ldots, p_k) = \mathbf{w}$. Sei dann für i, j mit $1 \leq i, j \leq k$ $q_{ij} = p_j$, falls der Eintrag in Zeile i und Spalte j der Wahrheitstafel für H gleich $\mathbf{w}$ ist, und $q_{ij} = H\neg(p_j)$ im anderen Fall. Sei ferner

$$R_i^{(k)}(p_1, \ldots, p_k) = H_\wedge^{(k)}(q_{i_1}, \ldots, q_{i_k})$$

und stehe in den Zeilen $i_1, \ldots, i_m$ ein $\mathbf{w}$ in der letzten Spalte der Wahrheitstafel für H. Dann ist

$$H(p_1, \ldots, p_k) = H_\vee^{(m)}(R_{i_1}^{(k)}(p_1, \ldots, p_k), \ldots, R_{i_m}^{(k)}(p_1, \ldots, p_k)). \qquad \blacksquare$$

Der obige Beweis gibt uns ein Verfahren, wie wir eine beliebige, durch eine Wahrheitstafel gegebene Wahrheitsfunktion durch $H_\wedge, H_\vee$ und $H_\neg$ darstellen können. Wir wollen dies an einem Beispiel verdeutlichen.

Beispiel 1.4.5 Habe $H : \{\mathbf{w}, \mathbf{f}\}^3 \to \{\mathbf{w}, \mathbf{f}\}$ die folgende Wahrheitstafel: Wir bestimmen

	p	q	r	H
1	**w**	**w**	**w**	**w**
2	**w**	**w**	**f**	**f**
3	**w**	**f**	**w**	**f**
4	**w**	**f**	**f**	**f**
5	**f**	**w**	**w**	**w**
6	**f**	**w**	**f**	**f**
7	**f**	**f**	**w**	**f**
8	**f**	**f**	**f**	**w**

zuerst die Zeilen mit einem $\mathbf{w}$ in der letzten Spalte. Das sind hier die Zeilen 1, 5 und 8. Für jeder dieser Zeilen konstruieren wir dann die zugehörige Wahrheitsfunktion $R_i^{(3)}$. Sie hat genau für die Wertekombination in dieser Zeile den Wert $\mathbf{w}$ und ansonsten den Wert $\mathbf{f}$. Wir erhalten

$$\begin{array}{rcl} R_1^{(3)}(p, q, r) & = & H_\wedge^{(3)}(p, q, r) \\ R_5^{(3)}(p, q, r) & = & H_\wedge^{(3)}(H_\neg(p), q, r) \\ R_8^{(3)}(p, q, r) & = & H_\wedge^{(3)}(H_\neg(p), H_\neg(q), H_\neg(r)). \end{array}$$

Dann ist

$$H(p,q,r) = H_{\vee}^{(3)}(H_{\wedge}^{(3)}(p,q,r), H_{\wedge}^{(3)}(H_{\neg}(p),q,r), H_{\wedge}^{(3)}(H_{\neg}(p),H_{\neg}(q),H_{\neg}(r))).$$

Korollar 1.4.6 Die Mengen $\{H_{\neg}, H_{\vee}\}, \{H_{\neg}, H_{\wedge}\}, \{H_{\neg}, H_{\rightarrow}\}$ und $\{F, H_{\rightarrow}\}$ sind ebenfalls adäquat. Hierbei ist F die einstellige Wahrheitsfunktion mit $F(p) = \mathbf{f}$ für $p \in \{\mathbf{w}, \mathbf{f}\}$.

Beweis. Für $p, q \in \{\mathbf{w}, \mathbf{f}\}$ ist

$$\begin{aligned} H_{\neg}(p) &= H_{\rightarrow}(p, F(p)) \\ H_{\vee}(p,q) &= H_{\rightarrow}(H_{\rightarrow}(p,\mathbf{f}),q) \\ &= H_{\rightarrow}(H_{\neg}(p),q) \\ &= H_{\neg}(H_{\wedge}(H_{\neg}(p),H_{\neg}(q))) \\ H_{\wedge}(p,q) &= H_{\rightarrow}(H_{\rightarrow}(p,H_{\rightarrow}(q,\mathbf{f})),\mathbf{f}) \\ &= H_{\neg}(H_{\rightarrow}(p,H_{\neg}(q))) \\ &= H_{\neg}(H_{\vee}(H_{\neg}(p),H_{\neg}(q))). \end{aligned}$$

Wie wir in Satz 1.4.4 gesehen haben, läßt sich jede Wahrheitsfunktion durch die Funktionen $H_{\neg}, H_{\vee}, H_{\wedge}$ ausdrücken. Mit den obigen Identitäten erhalten wir hieraus eine Darstellung durch $H_{\neg}, H_{\vee}$; $H_{\neg}, H_{\wedge}$; $H_{\neg}, H_{\rightarrow}$ bzw. $H_{\neg}, F$. ■

Das obige Ergebnis zeigt, daß alle Wahrheitsfunktionen von zwei Funktionen dieser Art erzeugt werden können. Wie wir jetzt sehen werden, reicht schon eine zweistellige Wahrheitsfunktion aus. Seien $H_{\downarrow}, H_{|} : \{\mathbf{w}, \mathbf{f}\}^2 \rightarrow \{\mathbf{w}, \mathbf{f}\}$ definiert durch

p	q	$H_{\mid}$	$H_{\downarrow}$
w	**w**	**f**	**f**
w	**f**	**w**	**f**
f	**w**	**w**	**f**
f	**f**	**w**	**w**

$H_{|}$ heißt *Shefferschе Strichfunktion* und $H_{\downarrow}$ *Peircesche Pfeilfunktion*. Wie wir der Wahrheitstafel entnehmen, ist genau dann $H_{|} = \mathbf{w}$, wenn nicht sowohl $p = \mathbf{w}$ als auch $q = \mathbf{w}$. Deswegen wird $H_{|}$ auch **NAND**–*Funktion* (**N**ot**AND**) genannt. Genauso ist genau dann $H_{\downarrow}(p,q) = \mathbf{w}$, wenn weder $p = \mathbf{w}$ noch $q = \mathbf{w}$. $H_{\downarrow}$ heißt auch **NOR**–*Funktion*.

Satz 1.4.7 Die Mengen $\{H_{|}\}$ und $\{H_{\downarrow}\}$ sind adäquat.

Beweis. Aufgrund von Korollar1.4.6 genügt es, die Funktion $H_{\neg}$ und $H_{\vee}$ bzw. $H_{\neg}$ und $H_{\wedge}$ durch $H_{|}$ und $H_{\downarrow}$ auszudrücken. Für $p, q \in \{\mathbf{w}, \mathbf{f}\}$ ist

$$\begin{aligned} H_{\neg}(p) &= H_{|}(p,p) = H_{\downarrow}(p,p) \\ H_{\vee}(p,q) &= H_{|}(H_{|}(p,p), H_{|}(q,q)) \\ H_{\wedge}(p,q) &= H_{\downarrow}(H_{\downarrow}(p,p), H_{\downarrow}(q,q)). \end{aligned}$$

■

Satz 1.4.8 $H_{|}$ und $H_{\downarrow}$ sind die einzigen zweistelligen Wahrheitsfunktionen, die alleine adäquat sind.

Beweis. Sei H eine zweistellige Wahrheitsfunktion, so das $\{H\}$ adäquat ist. Wäre $H(\mathbf{w},\mathbf{w}) = \mathbf{w}$, dann könnte aber $H_\neg$ nicht durch H definiert werden, im Widerspruch zur Adäquatheit von $\{H\}$. Also ist $H(\mathbf{w},\mathbf{w}) = \mathbf{f}$. Entsprechend folgt, daß $H(\mathbf{f},\mathbf{f}) = \mathbf{w}$.

Betrachten wir nun die Werte von H für die Argumentepaare $(\mathbf{w},\mathbf{f})$ und $(\mathbf{f},\mathbf{w})$. Ist $H(\mathbf{w},\mathbf{f}) = H(\mathbf{f},\mathbf{w}) = \mathbf{w}$ oder $H(\mathbf{w},\mathbf{f}) = H(\mathbf{f},\mathbf{w}) = \mathbf{f}$ so ist $H = H_|$, bzw. $H = H_\downarrow$. Ist dagegen $H(\mathbf{w},\mathbf{f}) = \mathbf{w}$ und $H(\mathbf{f},\mathbf{w}) = \mathbf{f}$ oder umgekehrt, so ist $H(p,q) = H_\neg(q)$ bzw. $H(p,q) = H_\neg(p)$. In beiden Fällen wäre also H durch $H_\neg$ definierbar, d.h., $\{H_\neg\}$ wäre adäquat. Dies ist aber nicht der Fall, da die einzigen durch $H_\neg$ definierbaren einstelligen Wahrheitsfunktionen $H_\neg$ selbst und die Identität Id auf $\{\mathbf{w},\mathbf{f}\}$ sind, wobei die Funktion Id durch $Id(p) = p$ $p \in \{\mathbf{w},\mathbf{f}\}$ definiert ist. Die konstante Wahrheitsfunktion, die immer den Wert $\mathbf{w}$ hat, ist daher nicht durch $H_\neg$ definierbar. ■

1.5 Semantik der Aussagenlogik

Wie im letzten Abschnitt schon angedeutet wurde, ist die Bedeutung einer aussagenlogischen Formel ein Wahrheitswert, also $\mathbf{w}$ oder $\mathbf{f}$. Es ist zu beachten, daß die Formeln selbst reine Zeichenreihen sind. Da die Bedeutung der Verknüpfungen $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ die intendierte sein soll, also $H_\neg, H_\vee, H_\wedge, H_\rightarrow$ bzw. $H_\leftrightarrow$, hängt der Wahrheitswert einer Formel von den Wahrheitswerten der in dieser Formel auftretenden Propositionalzeichen ab.

Definition 1.5.1 Eine *Wahrheitsbelegung* ist eine Abbildung $\mathcal{B}$ der Menge der Propositionalzeichen in die Menge $\{\mathbf{w},\mathbf{f}\}$ der Wahrheitswerte, so daß $\mathcal{B}(\bot) = \mathbf{f}$.

Nach Satz 1.3.6 läßt sich nun jede solche Wahrheitsbelegung $\mathcal{B}$ eindeutig zu einer *Wahrheitsbewertung* $\hat{\mathcal{B}}$ der aussagenlogischen Formeln fortsetzen, und zwar so, daß

1. $\hat{\mathcal{B}}(\alpha) = \mathcal{B}(\alpha)$, falls α ein Propositionalzeichen ist,
2. $\hat{\mathcal{B}}(\neg\alpha) = H_\neg(\hat{\mathcal{B}}(\alpha))$,
3. $\hat{\mathcal{B}}(\alpha_1 \vee \alpha_2) = H_\vee(\hat{\mathcal{B}}(\alpha_1), \hat{\mathcal{B}}(\alpha_2))$,
4. $\hat{\mathcal{B}}(\alpha_1 \wedge \alpha_2) = H_\wedge(\hat{\mathcal{B}}(\alpha_1), \hat{\mathcal{B}}(\alpha_2))$,
5. $\hat{\mathcal{B}}(\alpha_1 \rightarrow \alpha_2) = H_\rightarrow(\hat{\mathcal{B}}(\alpha_1), \hat{\mathcal{B}}(\alpha_2))$,
6. $\hat{\mathcal{B}}(\alpha_1 \leftrightarrow \alpha_2) = H_\leftrightarrow(\hat{\mathcal{B}}(\alpha_1), \hat{\mathcal{B}}(\alpha_2))$.

Beispiel 1.5.2 Sei $\mathcal{B}(A_1) = \mathbf{w}$, $\mathcal{B}(A_3) = \mathbf{w}$ und $\mathcal{B}(\eta) = \mathbf{f}$ für alle sonstigen Propositionalzeichen η. Dann ist

$$\begin{aligned}\hat{\mathcal{B}}(\neg((A_1 \wedge A_3) \vee A_6)) &= H_\neg(H_\vee(H_\wedge(\mathcal{B}(A_1), \mathcal{B}(A_3)), \mathcal{B}(A_6))) \\ &= H_\neg(H_\vee(H_\wedge(\mathbf{w},\mathbf{w}),\mathbf{f})) = \mathbf{f}.\end{aligned}$$

In der obigen Definition ist der Wahrheitswert $\hat{\mathcal{B}}(\alpha)$ einer Formel α für Wahrheitsbelegungen definiert, die allen Propositionalzeichen einen Wahrheitswert zuweisen, also auch den unendlichen vielen, nicht in α vorkommenden Zeichen. Wie aber das obige Beispiel zeigt, hängt $\hat{\mathcal{B}}(\alpha)$ nur von den Wahrheitswerten ab, die den in α vorkommenden Propositionalzeichen zugewiesen sind. Dies ist auch die Aussage des folgenden

Lemma 1.5.3 — Koinzidenzlemma. Sei α eine Formel, und seien $\mathcal{B}$ und $\mathcal{B}'$ Wahrheitsbelegungen, die bezüglich der in α vorkommenden Propositionalzeichen übereinstimmen. Dann ist $\hat{\mathcal{B}}(\alpha) = \hat{\mathcal{B}'}(\alpha)$.

Beweis. Wir führen den Beweis durch Induktion über den Formelaufbau. Ist α ein Propositionalzeichen, so gilt die behauptete Gleichheit aufgrund der Voraussetzung über $\mathcal{B}$ und $\mathcal{B}'$. Betrachten wir als nächstes den Fall, daß $\alpha = \neg\beta$. Da in α und β diegleichen Propositionalzeichen vorkommen, ist nach Induktionsvoraussetzung $\hat{\mathcal{B}}(\beta) = \widehat{\mathcal{B}'}(\beta)$ und also

$$\hat{\mathcal{B}}(\alpha) = H_\neg(\hat{\mathcal{B}}(\beta)) = H_\neg(\widehat{\mathcal{B}'}(\beta)) = \widehat{\mathcal{B}'}(\alpha).$$

Es bleibt der Fall, daß $\alpha = \alpha_1 \square \alpha_2$ mit $\square \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$. Da die in α_1 bzw. α_2 vorkommenden Propositionalzeichen auch in α vorkommen, stimmen $\mathcal{B}$ und $\mathcal{B}'$ bezüglich dieser Zeichen überein. Daher ist nach Induktionsvoraussetzung $\hat{\mathcal{B}}(\alpha_1) = \widehat{\mathcal{B}'}(\alpha_1)$ und $\hat{\mathcal{B}}(\alpha_2) = \widehat{\mathcal{B}'}(\alpha_2)$, woraus

$$\hat{\mathcal{B}}(\alpha) = H_\square(\hat{\mathcal{B}}(\alpha_1), \hat{\mathcal{B}}(\alpha_2)) = H_\square(\hat{\mathcal{B}'}(\alpha_1), \hat{\mathcal{B}'}(\alpha_2)) = \widehat{\mathcal{B}'}(\alpha)$$

folgt. ■

Wir sehen, daß es zur Bestimmung des Wahrheitswertes einer Formel bezüglich einer Wahrheitsbelegung genügt, die Werte der in der gegebenen Formel auftretenden Propositionalzeichen unter der Belegung zu kennen. In Anwendungen wollen wir daher die Werte einer Wahrheitsbelegung auch nur soweit wie nötig angeben.

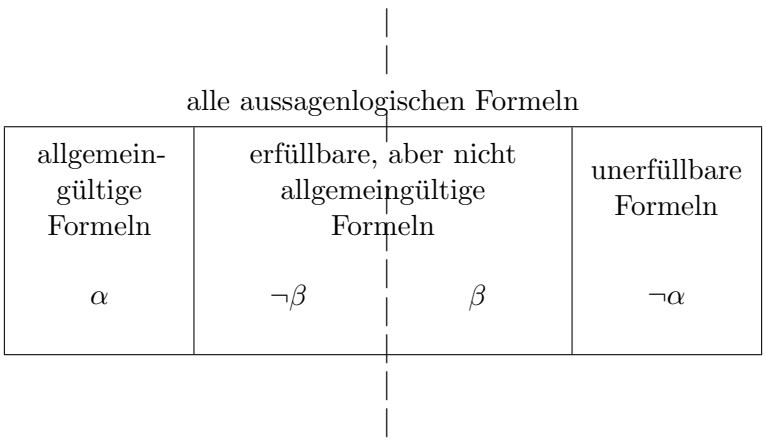
Definition 1.5.4

1. Ist $\mathcal{B}$ eine Wahrheitsbelegung und α eine Formel, so *gilt* α *unter der Belegung* $\mathcal{B}$, falls $\hat{\mathcal{B}}(\alpha) = \mathbf{w}$. Wir sagen in diesem Fall auch: $\mathcal{B}$ ist ein *Modell für* α, bzw. α *gilt in dem Modell* $\mathcal{B}$ und schreiben: $\mathcal{B} \models \alpha$. Falls $\mathcal{B}(\alpha) = \mathbf{f}$ ist, so schreiben wir: $\mathcal{B} \not\models \alpha$. Ist Γ eine Menge von Formeln, so ist $\mathcal{B}$ *Modell* von Γ, falls jede Formel aus Γ unter $\mathcal{B}$ gilt. In diesem Fall schreiben wir $\mathcal{B} \models \Gamma$:
2. Γ heißt *erfüllbar*, falls Γ ein Modell besitzt. Anderenfalls heißt Γ *unerfüllbar*. (Ist $\Gamma = \{\alpha\}$, so identifizieren wir α und $\{\alpha\}$).
3. α heißt *allgemeingültig* oder auch *Tautologie*, falls α unter jeder Belegung gilt. Wir schreiben in diesem Fall: $\models \alpha$. Ist α keine Tautologie, so schreiben wir: $\not\models \alpha$.

Lemma 1.5.5 Eine Formel α ist genau dann eine Tautologie, wenn $\neg\alpha$ unerfüllbar ist.

Beweis. α ist genau dann Tautologie, wenn α unter jeder Belegung gilt. Dies ist genau dann der Fall, wenn $\neg\alpha$ unter keiner Belegung gilt, was nichts anderes heißt, als daß $\neg\alpha$ unerfüllbar ist. ■

Der Übergang von α zu $\neg\alpha$ (bzw. von $\neg\alpha$ zu α) kann durch folgendes „Spiegelungsprinzip“ veranschaulicht werden.



Hierbei bedeutet die Anwendung der Negation eine Spiegelung an der gestrichelten Achse. So wird aus einer allgemeingültigen eine unerfüllbare Formel (oder umgekehrt), während aus einer erfüllbaren, aber nicht allgemeingültigen Formel wieder eine erfüllbare, nicht allgemeingültige Formel wird.

Definition 1.5.6 Sei Γ eine Formelmenge. Eine Formel β ist *logische Folgerung* von Γ, falls jedes Modell von Γ auch Modell von β ist Wir schreiben in diesem Fall: $\Gamma \models \beta$. Ist α eine weitere Formel und $\Gamma \cup \{\alpha\} \models \beta$, so schreiben wir stattdessen auch: $\Gamma, \alpha \models \beta$.

Lemma 1.5.7

1. Ist $\Gamma, \alpha \models \beta$ und $\Gamma, \alpha \models \neg\beta$, so ist $\Gamma \models \neg\alpha$.
2. Die folgenden Aussagen sind äquivalent:
   (a) $\Gamma, \alpha \models \beta$,
   (b) $\Gamma \models \alpha \to \beta$,
   (c) $\Gamma \cup \{\alpha \wedge \neg\beta\}$ ist unerfüllbar.

Beweis. (1) Sei $\mathcal{B}$ ein Modell von Γ und werde angenommen, das $\mathcal{B}$ auch Modell von α ist. Dann ist sowohl $\hat{\mathcal{B}}(\beta) = \mathbf{w}$ wie auch $\hat{\mathcal{B}}(\neg\beta) = \mathbf{w}$, ein Widerspruch. Also ist $\hat{\mathcal{B}}(\alpha) = \mathbf{f}$, woraus folgt, daß $\mathcal{B}$ Modell von $\neg\alpha$ ist.

(2) Wir zeigen zuerst, daß (b) aus (a) folgt. Sei hierzu $\mathcal{B}$ ein Modell von Γ. Ist nun $\mathcal{B}$ auch ein Modell von α, d.h. $\hat{\mathcal{B}}(\alpha) = \mathbf{w}$, so ist nach (a) auch $\hat{\mathcal{B}}(\beta) = \mathbf{w}$. Also ist in diesem Fall $\hat{\mathcal{B}}(\alpha \to \beta) = \mathbf{w}$. Ist dagegen $\mathcal{B}$ kein Modell von α, d.h. $\hat{\mathcal{B}}(\alpha) = \mathbf{f}$, so ist $\hat{\mathcal{B}}(\alpha \to \beta) = \mathbf{w}$, unabhängig vom Wahrheitswert von β unter $\mathcal{B}$.

Als nächstes zeigen wir, daß (c) aus (b) folgt. Sei $\mathcal{B}$ wieder ein Modell von Γ und werde angenommen, daß $\hat{\mathcal{B}}(\alpha \wedge \neg\beta) = \mathbf{w}$. Dann ist sowohl $\hat{\mathcal{B}}(\alpha) = \mathbf{w}$ wie auch $\hat{\mathcal{B}}(\neg\beta) = \mathbf{w}$, d.h. $\hat{\mathcal{B}}(\beta) = \mathbf{f}$. Da nach (b) $\hat{\mathcal{B}}(\alpha \to \beta) = \mathbf{w}$, folgt andererseits, daß $\hat{\mathcal{B}}(\beta) = \mathbf{w}$. Also ist $\mathcal{B}$ kein Modell von $\alpha \wedge \neg\beta$.

Als letztes zeigen wir nun, daß (a) aus (c) folgt. Sei dazu $\mathcal{B}$ ein Modell von $\Gamma \cup \{\alpha\}$, und werden angenommen, daß $\hat{\mathcal{B}}(\beta) = \mathbf{f}$. Dann ist $\mathcal{B}$ auch Modell von $\Gamma \cup \{\alpha \wedge \neg\beta\}$, im Widerspruch zu (c). Also ist $\mathcal{B}$ Modell von β. ■

Definition 1.5.8 Ist Γ eine Formelmenge, so daß für jede Formel α mit $\Gamma \models \alpha$ schon $\alpha \in \Gamma$, dann heißt Γ *Theorie*. Interessant sind natürlich nur solche Theorien, die nicht alle Formeln umfassen: Γ heißt *widerspruchsfrei* (*konsistent*), falls es eine Formel α gibt, so daß $\Gamma \not\models \alpha$.

Lemma 1.5.9 Die folgenden Aussagen sind äquivalent:

1. Γ ist widerspruchsfrei,
2. für jede Formel β ist $\Gamma \not\models \beta \wedge \neg\beta$,
3. es gibt keine Formel β mit $\Gamma \models \beta$ und $\Gamma \models \neg\beta$,
4. Γ ist erfüllbar.

Beweis. Offensichtlich folgt (1) aus (2) und (2) aus (3). Gelte nun (1), sei α eine Formel, und werde angenommen, daß Γ unerfüllbar ist. Dann gilt α in jedem Modell von Γ. (Beachte, daß Γ nach Annahme kein Modell besitzt.) Also ist jede Formel logische Folgerung von Γ, im Widerspruch zur Widerspruchsfreiheit von Γ. Somit ist Γ erfüllbar.

Gelte jetzt (4), sei $\mathcal{B}$ ein Modell von Γ und β eine Formel. Da nicht zugleich $\hat{\mathcal{B}}(\beta) = \mathbf{w}$ und $\hat{\mathcal{B}}(\neg\beta) = \mathbf{w}$ sein kann, folgt, daß $\mathcal{B}$ kein Modell von $\Gamma \cup \{\beta\}$ oder kein Modell von $\Gamma \cup \{\neg\beta\}$ ist. ■

Korollar 1.5.10 $\Gamma \not\models \alpha$ genau dann, wenn $\Gamma \cup \{\neg\alpha\}$ widerspruchsfrei ist.

Wie wir sehen, sind also die widerspruchsvollen Formelmengen gerade diejenigen, die auch unerfüllbar sind. Das nächste Resultat zeigt, daß die Unerfüllbarkeit eine lokale Eigenschaft ist, d.h., ist eine unendliche Formelmenge unerfüllbar, so liegt das nicht daran, daß sie unendlich ist.

Satz 1.5.11 — Kompaktheitssatz. Eine Formelmenge ist genau dann unerfüllbar, wenn sie eine endliche unerfüllbare Teilmenge besitzt.

Offensichtlich ist eine Formelmenge mit einer unerfüllbaren Teilmenge auch selbst unerfüllbar. Die umgekehrte (wesentliche) Richtung des Satzes wollen wir im nächsten Abschnitt beweisen. Vorher soll aber noch erläutert werden, warum dieser Satz als Kompaktheitssatz bezeichnet wird. Der Begriff der Kompaktheit ist ja aus der Topologie bekannt. Ein topologischer Raum X heißt *kompakt*, wenn sich aus jeder Klasse von offenen Mengen, die X überdecken, eine endliche Teilklasse auswählen läßt, so daß X auch von diesen Mengen überdeckt wird. Auf der Menge $\mathbb{W}$ aller Wahrheitsbelegungen läßt sich nun eine Topologie einführen: Die offenen Mengen sind hierbei die für Formelklassen Γ definierten Mengen

$$O_\Gamma = \{\mathcal{B} \in \mathbb{W} \mid \exists \alpha \in \Gamma\ \mathcal{B} \not\models \alpha\}.$$

Wir wollen uns kurz überzeugen, daß hierdurch eine Topologie auf Γ definiert wird: Sei α eine unerfüllbare Formel und β eine Tautologie.[1] Dann ist $\mathbb{W} = O_\alpha$ und $\emptyset = O_\beta$. Also sind $\mathbb{W}$ und $\emptyset$ offen.

Sei als nächstes I eine Indexmenge und $\{\Gamma_i \mid i \in I\}$ eine Klasse von Formelmengen. Setzen wir $\Gamma = \bigcup\{\Gamma_i \mid i \in I\}$, so ist $\bigcup\{O_{\Gamma_i} \mid i \in I\} = O_\Gamma$. Das heißt, die Klasse der oben definierten Mengen ist abgeschossen unter der Bildung der Vereinigung von beliebig vielen Mengen aus dieser Klasse.

Wir haben jetzt noch zu zeigen, daß dasgleiche für die Bildung des Durchschnitts von endlich vielen dieser Mengen gilt. Seien hierzu $\Gamma_1, \ldots, \Gamma_n$ Formelmengen und $\Gamma = \{((\alpha_1 \vee \alpha_2) \vee \cdots) \vee \alpha_n \mid \alpha_i \in \Gamma_i\ (1 \leq i \leq n)\}$. Dann ist $\bigcap\{\Gamma_i \mid 1 \leq i \leq n\} = O_\Gamma$.

Bezüglich dieser Topologie ist $\mathbb{W}$ genau dann kompakt, wenn es zu jeder Formelmenge Γ, so daß $\mathbb{W} = O_\Gamma = \bigcup\{O_{\{\alpha\}} \mid \alpha \in \Gamma\}$ eine endliche Teilmenge Γ' gibt, so daß $\mathbb{W} = O_{\Gamma'}$. Da für eine Formelmenge Δ genau dann $\mathbb{W} = O_\Delta$, wenn Δ unerfüllbar ist, ist also die Kompaktheit von $\mathbb{W}$ gleichbedeutend mit der nichtrivialen Richtung des obigen Satzes. Wir erhalten somit

Korollar 1.5.12 Die Menge der Wahrheitsbelegungen ist kompakt.

Bevor wir uns nun dem Beweis der noch ausstehenden Richtung des Kompaktheitssatzes zuwenden, wollen wir noch ein äquivalentes Resultat angeben, das in der Literatur oft anstelle des obigen Satzes als Kompaktheitssatz bezeichnet wird.

Satz 1.5.13 Sei Γ eine Formelmenge und α eine Formel. Dann ist genau dann $\Gamma \models \alpha$, wenn es eine endliche Teilmenge Γ' von Γ gibt, so daß $\Gamma' \models \alpha$.

[1] Z.B. $\alpha = \bot$ und $\beta = \neg\bot$

Beweis. Mit Lemma 1.5.9, Korollar 1.5.10 und Satz 1.5.11 gilt

$$\begin{array}{lll} \Gamma \models \alpha & \text{gdw.} & \Gamma \cup \{\neg\alpha\} \text{ ist widerspruchsvoll} \\ & \text{gdw.} & \Gamma \cup \{\neg\alpha\} \text{ ist unerfüllbar} \\ & \text{gdw.} & \text{es gibt } \Gamma' \subseteq \Gamma : \ \Gamma' \text{ ist endlich und} \\ & & \Gamma' \cup \{\neg\alpha\} \text{ ist unerfüllbar} \\ & \text{gdw.} & \text{es gibt } \Gamma' \subseteq \Gamma : \Gamma' \text{ endlich und } \Gamma' \models \alpha. \end{array}$$

■

Wie wir jetzt noch zeigen wollen, folgt umgekehrt Satz 1.5.11 auch aus dem obigen Satz. Mit Lemma 1.5.9 gilt wieder:

$$\begin{array}{lll} \Gamma \text{ ist unerfüllbar} & \text{gdw.} & \text{es gibt } \beta : \ \Gamma \models \beta \wedge \neg\beta \\ & \text{gdw.} & \text{es gibt } \beta, \Gamma' \subseteq \Gamma : \ \Gamma' \text{ ist endlich und} \\ & & \Gamma' \models \beta \wedge \neg\beta \\ & \text{gdw.} & \text{es gibt } \Gamma' \subseteq \Gamma : \ \Gamma' \text{ ist endlich und unerfüllbar.} \end{array}$$

1.6 Das Lemma von König und der Beweis des Kompaktheitssatzes

Identifizieren wir **w** mit 1 und **f** mit 0, so lassen sich Wahrheitsbelegungen als binäre Folgen auffassen; also als Wörter $\{0,1\}^*$. Das i-te Element eines Wortes ist $u(i)$. Also ist $u = u(1)u(2)\dots u(n)$, wobei n die Länge des Wortes u ist, für die wir auch $|u|$ schreiben. Ist $u \in \{0,1\}^*$ ein Binärwort und $0 \leqslant n \leqslant |u|$, so soll mit $\overline{u}n$ das Präfix von u der Länge n bezeichnen. Diese Definition macht auch für *unendliche Pfade* Sinn; das sind Elemente $\sigma \in \{0,1\}^{\mathbb{N}}$.

Definition 1.6.1

1. Ein *(binär-)* Baum ist eine Teilmenge $T \subseteq \{0,1\}^*$, so daß mit $u \in T$ auch $\overline{u}n \in T$ für alle $n \leqslant |u|$.
2. Ein Baum ist ein *unendlicher Baum*, wenn er als Menge unendlich ist.
3. Ein Element $\sigma \in \{0,1\}^{\mathbb{N}}$ ist ein *(unendlicher) Pfad durch* einen Baum T, falls $\overline{\sigma}n \in T$ für alle $n \in \mathbb{N}$.

Eines der wichtigsten Resultate über unendliche Bäume ist das (schwache) Lemma von König:

Satz 1.6.2 — schwaches Königs Lemma. Ein unendlicher Baum besitzt einen unendlichen Pfad.

Beweis. Sei T ein Baum. Für $u \in \{0,1\}^*$ mit $|u| = n$ definieren wir

$$T_u = \{w \in T \mid \forall i \leqslant |u|\ \overline{w}i = \overline{u}i\}\ .$$

Anschaulich erhalten wir T_u wenn wir uns den Teilbaum von T betrachten, der durch den Knoten u geht. Wie man einfach zeigen kann ist auch T_u ein Baum (Übung). Der entscheidende Trick ist nun, daß wenn T_u unendlich ist entweder T_{u0} oder T_{u1} unendlich sein müssen (oder beide), da wenn beide endlich wären auch T_u endlich sein müsste. Man beachte ausserdem, daß $T_\varepsilon = T$ und $T_u \subseteq T$ für alle u. Rekursiv können wir also ein $\sigma \in \{0,1\}^{\mathbb{N}}$ finden, so daß

- $\overline{\sigma}n \in T$, und
- $T_{\overline{\sigma}n}$ ist unendlich.

Dies ist das gesuchte σ. ■

Mithilfe dieses Satzes wollen wir nun die nichttriviale Richtung des Kompaktheitssatzes beweisen.

Beweis von Satz 1.5.11: Wir zeigen nun, daß eine Formelmenge erfüllbar ist, wenn jede ihrer endlichen Teilmengen erfüllbar sind. Offensichtlich brauchen wir hierbei nur den Fall unendlicher Formelmengen zu betrachten. Sei $\Gamma = \{\alpha_i \mid i = 1, 2, \dots\}$ eine solche. Sei nun

$$T = \{u \in \{0,1\}^* \mid \text{es gibt eine Wahrheitsbelegung } \mathcal{B}, \text{ so daß für alle natürlichen Zahlen } i \text{ mit } 1 \leq i \leq |u|$$

1. genau dann $\mathcal{B}(A_i) = \mathbf{w}$, wenn $u(i) = 1$, und
2. $\hat{\mathcal{B}}(\alpha_i) = \mathbf{w}\}$.

Wir lassen in T also alle endlichen Folgen u zu, die — als Anfang einer Wahrheitsbelegung interpretiert — allen α_i mit $1 \leq i \leq |u|$ den Wert $\mathbf{w}$ zuweisen. Wie wir jetzt zeigen wollen, gilt: wenn T einen unendlichen Pfad besitzt, dann ist Γ erfüllbar. Sei also σ ein unendlicher Pfad in T. Daher ist durch

$$\mathcal{B}(A_i) = \begin{cases} \mathbf{w}, & \text{falls } \sigma(i) = 1 \\ \mathbf{f}, & \text{sonst} \end{cases}$$

eine Wahrheitsbelegung definiert, von der wir jetzt zeigen wollen, daß sie Modell von Γ ist. Sei dazu $\alpha_m \in \Gamma$ und enthalte α_m höchstens die Propositionalzeichen $A_1, \ldots, A_k$. Sei ferner $n = \max\{k, m\}$. Dann ist, da σ ein Pfad durch T ist, $\overline{\sigma}n \in T$. Daher gibt es eine Wahrheitsbelegung $\mathcal{B}'$, so daß für alle i mit $1 \leq i \leq n$ $\widehat{\mathcal{B}'}(\alpha_i) = \mathbf{w}$. Ferner ist genau dann $\mathcal{B}'(A_i) = \mathbf{w}$, wenn $\sigma(i) = 1$. Nach dem Koinzidenzlemma (1.5.3) gilt, daß $\hat{\mathcal{B}}(\alpha_m) = \widehat{\mathcal{B}'}(\alpha_m) = \mathbf{w}$. D.h. $\mathcal{B}$ ist unsere gesuchte Wahrheitsbelegung, die Modell von Γ ist.

Offensichtlich haben wir jetzt nur noch zu zeigen, daß T einen unendlichen Pfad besitzt. Dies folgt nach Königs Lemma, wenn T unendlich ist. Aufgrund unserer Annahme ist jede endliche Teilmenge von Γ erfüllbar. Daher gibt es für jedes n eine Wahrheitsbelegung $\mathcal{B}$ mit $\hat{\mathcal{B}}(\alpha_i) = \mathbf{w}$ für $1 \leq i \leq n$. Sei nun für i mit $1 \leq i \leq n$ $u(i) = 1$, falls $\mathcal{B}(A_i) = \mathbf{w}$, und $u(i) = 0$ im anderen Fall, dann ist $u \in T$ und $|u| = n$. Also enthält T für jede natürliche Zahl n eine binäre Folge der Länge n, d.h., T ist unendlich. ■

1.7 Äquivalenz und Normalformen

Aus der Art und Weise, wie wir Formeln interpretieren, wissen wir, daß $F \wedge G$ und $G \wedge F$ „dasselbe bedeuten“, d.h., dengleichen Wahrheitswert haben, obwohl sie syntaktisch gesehen verschiedene Objekte sind. Die semantische Gleichheit oder Äquivalenz erfassen wir mit folgender Definition.

Definition 1.7.1 Zwei Formeln α und β heißen *(semantisch) äquivalent*, falls für alle Wahrheitsbelegungen $\mathcal{B}$ gilt $\hat{\mathcal{B}}(\alpha) = \hat{\mathcal{B}}(\beta)$. Wir schreiben in diesem Fall $\alpha \equiv \beta$.

Offensichtlich gilt

Lemma 1.7.2 $\alpha \equiv \beta$ genau dann, wenn $\alpha \leftrightarrow \beta$ eine Tautologie ist.

Satz 1.7.3 — Äquivalenztheorem. Seien α und β äquivalente Formeln. Sei γ eine Formel mit (mindestens) einem Vorkommen der Teilformel α. Dann ist γ äquivalent zu γ', wobei γ' aus γ hervorgeht, indem (irgend–)ein Vorkommen von α in γ durch β ersetzt wird.

Beweis. Wir beweisen den obigen Satz durch Induktion über den Formelaufbau. Ist γ ein Propositionalzeichen, so kann nur $\gamma = \alpha$ sein. Dann ist aber $\gamma' = \beta$ und also $\gamma \equiv \gamma'$. Dies gilt auch, falls γ kein Propositionalzeichen, aber $\gamma = \alpha$ ist.

Betrachten wir nun den Fall, daß γ kein Propositionalzeichen und α eine Teilformel von γ mit $\alpha \neq \gamma$ ist. Dann haben wir die folgenden Fälle zu betrachten:

1. γ hat die Bauart $\gamma = \neg\eta$.

Nach Induktionsvorraussetzung ist η dann äquivalent zu η', wobei η' aus η durch Ersetzung eines Vorkommens von α durch β hervorgeht. Da $\gamma' = \neg\eta'$, folgt aus der Definition der Wahrheitsbewertungen, daß auch γ und γ' äquivalent sind.

2. γ hat die Bauart $\gamma_1 \Box \gamma$ mit $\Box \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$.

Dann wird α entweder in γ_1 oder γ_2 ersetzt. Betrachten wir ohne Einschränkung den ersten Fall. Dann ist nach Induktionsannahme γ_1 äquivalent zu γ_1', wobei γ_1' aus γ durch Ersetzung von α durch β hervorgeht. Also ist auch $\gamma \equiv \gamma_1' \Box \gamma_2 = \gamma'$. ■

Mit Hilfe der Wahrheitstafeln läßt sich nun leicht überprüfen, daß auch die folgenden Äquivalenzen gelten:

Satz 1.7.4

$\alpha \wedge \alpha$	$\equiv$	α	
$\alpha \vee \alpha$	$\equiv$	α	(Idempotenz)
$\alpha \wedge \beta$	$\equiv$	$\beta \wedge \alpha$	
$\alpha \vee \beta$	$\equiv$	$\beta \vee \alpha$	(Kommutativität)
$(\alpha \wedge \beta) \wedge \gamma$	$\equiv$	$\alpha \wedge (\beta \wedge \gamma)$	
$(\alpha \vee \beta) \vee \gamma$	$\equiv$	$\alpha \vee (\beta \vee \gamma)$	*(Assoziativität)*
$\alpha \wedge (\alpha \vee \beta)$	$\equiv$	α	
$\alpha \vee (\alpha \wedge \beta)$	$\equiv$	α	*(Absorption)*
$\alpha \wedge (\beta \vee \gamma)$	$\equiv$	$(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$	
$\alpha \vee (\beta \wedge \gamma)$	$\equiv$	$(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$	*(Distributivität)*
$\neg\neg\alpha$	$\equiv$	α	*(Doppelnegation)*
$\neg(\alpha \wedge \beta)$	$\equiv$	$\neg\alpha \vee \neg\beta$	*(de Morgansche-*
$\neg(\alpha \vee \beta)$	$\equiv$	$\neg\alpha \wedge \neg\beta$	*Regeln)*
$\alpha \vee \beta$	$\equiv$	α , falls α eine Tautologie ist	*(Tautologie-*
$\alpha \wedge \beta$	$\equiv$	β , falls α eine Tautologie ist	*regeln)*
$\alpha \vee \beta$	$\equiv$	β , falls α unerfüllbar ist	*(Unerfüllbarkeits-*
$\alpha \wedge \beta$	$\equiv$	α , falls α unerfüllbar ist	*regeln)*

Mit Hilfe dieser Äquivalenzen und des Äquivalenztheorems (ÄT) lassen sich nun weitere Äquivalenzen nachweisen:

Beispiel 1.7.5 Es ist

$$(A \vee (B \vee C)) \wedge (C \vee \neg A) \equiv (B \wedge \neg A) \vee C,$$

denn es gilt: $(A \vee (B \vee C)) \wedge (C \vee \neg A)$

$\equiv$	$((A \vee B) \vee C) \wedge (C \vee \neg A)$	(Assoziativität und ÄT)
$\equiv$	$(C \vee (A \vee B)) \wedge (C \vee \neg A)$	(Kommutativität und ÄT)
$\equiv$	$C \vee ((A \vee B) \wedge \neg A)$	(Distributivität)
$\equiv$	$C \vee (\neg A \wedge (A \vee B))$	(Kommutativität und ÄT)
$\equiv$	$C \vee ((\neg A \wedge A) \vee (\neg A \wedge B))$	(Distributivität und ÄT)
$\equiv$	$C \vee (\neg A \wedge B)$	(Unerfüllbarkeitsregel und ÄT)
$\equiv$	$C \vee (B \wedge \neg A)$	(Kommutativität und ÄT)
$\equiv$	$(B \wedge \neg A) \vee C$	(Kommutativität).

Das Assoziativgesetz im obigen Satz gibt uns die Möglichkeit, etwas freier beim Aufschreiben von Formeln vorzugehen. So soll etwa die Schreibweise

$$A \wedge B \wedge C \wedge D$$

eine beliebige der folgenden Formeln bedeuten:

$$((A \wedge B) \wedge C) \wedge D$$
$$(A \wedge B) \wedge (C \wedge D)$$
$$(A \wedge (B \wedge C)) \wedge D$$
$$A \wedge ((B \wedge C) \wedge D)$$

$$A \wedge (B \wedge (C \wedge D)),$$

ohne daß festgelegt sein soll, welche. Da alle diese Formeln semantisch äquivalent sind, spielt dies in vielen Fällen auch keine Rolle. Entsprechend verfahren wir bezüglich der Verknüpfungsoperation $\vee$.

In Satz 1.7.4 fällt auf, daß die dort aufgeführten Äquivalenzen gültig bleiben, wenn alle Vorkommen von $\wedge$ durch $\vee$ ersetzt werden und umgekehrt. Dies ist ein allgemeines Gesetz.

Satz 1.7.6 — Dualitätsprinzip. Seien α und β Formeln, die nur die Zeichen $\neg$, $\vee$ und $\wedge$ enthalten (und kein $\bot$), und gehen α^d und β^d aus α bzw. β hervor, indem alle Vorkommen von $\wedge$ durch $\vee$ und umgekehrt ersetzt werden. D.h. ^{d} is induktiv definiert durch

- $\alpha^d = \alpha$, falls $\alpha = A_i$, also ein Propositionalzeichen ist,
- $(\neg\alpha)^d = \neg(\alpha^d)$
- $(\alpha_1 \wedge \alpha_2)^d = \alpha_1^d \vee \alpha_2^d$,
- $(\alpha_1 \vee \alpha_2)^d = \alpha_1^d \wedge \alpha_2^d$

Ist dann $\alpha \equiv \beta$, so auch $\alpha^d \equiv \beta^d$.

Beweis. Ist $\mathcal{B}$ eine Wahrheitsbelegung, so bezeichne $\overline{\mathcal{B}}$ diejenige Wahrheitsbelegung, für welche genau dann $\overline{\mathcal{B}}(\eta) = \mathbf{w}$, wenn $\mathcal{B}(\eta) = \mathbf{f}$ (natürlich ausser für $A_1 = \bot$). Durch Induktion über den Formelaufbau zeigen wir nun, daß für jede Wahrheitsbelegung gilt $\mathcal{B}$

$$\hat{\overline{\mathcal{B}}}(\alpha^d) = H_\neg(\hat{\mathcal{B}}(\alpha)) \ .$$

Da mit $\mathcal{B}$ auch $\overline{\mathcal{B}}$ alle Wahrheitsbelegungen durchläuft, folgt hieraus, daß $\alpha' \equiv \beta'$, falls $\alpha \equiv \beta$.

Betrachten wir zuerst den Fall, daß α ein Propositionalzeichen ist. Dann gilt die behauptete Gleichheit aufgrund der Definition von $\overline{\mathcal{B}}$. Nehmen wir als nächstes an, α habe die Form $\alpha = \neg\gamma$. Dann ist nach Induktionsvoraussetzung $\hat{\overline{\mathcal{B}}}(\gamma^d) = H_\neg(\hat{\mathcal{B}}(\gamma))$. Hieraus folgt aufgrund der Definition von $\hat{\mathcal{B}}$ bzw. $\hat{\overline{\mathcal{B}}}$, daß

$$\hat{\overline{\mathcal{B}}}(\alpha^d) = H_\neg(\hat{\overline{\mathcal{B}}}(\gamma^d)) = H_\neg(H_\neg(\hat{\mathcal{B}}(\gamma)) = H_\neg(\hat{\mathcal{B}}(\alpha)).$$

Betrachten wir schließlich noch den Fall, daß α die Form $\alpha = \alpha_1 \vee \alpha_2$ hat. Der Fall, daß α die Form $\alpha_1 \wedge \alpha_2$ hat, kann in der gleichen Weise behandelt werden. Es gilt unter Verwendung der Induktionsvoraussetzung

$$\begin{aligned}\hat{\mathcal{B}}(\alpha^d) = H_\wedge(\hat{\overline{\mathcal{B}}}(\alpha_1^d), \hat{\overline{\mathcal{B}}}(\alpha_2^d)) &= H_\wedge(H_\neg(\hat{\mathcal{B}}(\alpha_1)), H_\neg(\hat{\mathcal{B}}(\alpha_2))) \\ &= H_\neg(H_\vee(\hat{\mathcal{B}}(\alpha_1), \hat{\mathcal{B}}(\alpha_2))) = H_\neg(\hat{\mathcal{B}}(\alpha)) \ . \quad \blacksquare\end{aligned}$$

Wir wollen nun zeigen, daß jede — auch noch so kompliziert aussehende — Formel in eine gewisse Normalform überführt werden kann, und zwar mit Hilfe der Umformungsregeln aus Satz 1.7.4

Definition 1.7.7

1. Ein *Literal* ist ein Propositionalzeichen oder die Negation eines Propositionalzeichens. (Im ersten Fall sprechen wir von einem *positiven*, im zweiten von einem *negativen* Literal.)

2. Eine Formel α ist in *konjunktiver Normalform (KNF)*, falls sie eine Konjunktion von Disjunktionen von Literalen ist:

$$\alpha = \bigwedge_{i=1}^{n} (\bigvee_{j=1}^{m_i} L_{i,j})$$

mit $L_{i,j} \in \{A_1, A_2, \ldots\} \cup \{\neg A_1, \neg A_2, \ldots\}$.

3. Eine Formel α ist in *disjunktiver Normalform (DNF)*, falls sie eine Disjunktion von Konjunktionen von Literalen ist:

$$\alpha = \bigvee_{i=1}^{n} (\bigwedge_{j=1}^{m_i} (L_{i,j})$$

mit $L_{i,j} \in \{A_1, A_2, \ldots\} \cup \{\neg A_1, \neg A_2, \ldots\}$.

In dieser Definition ist $\bigvee_{i=1}^{n} \alpha_i$ eine Abkürzung für $(\ldots((\alpha_1 \vee \alpha_2) \vee \alpha_3) \vee \cdots) \vee \alpha_n)$ und $\bigwedge_{i=1}^{n} \alpha_i$ eine Abkürzung für $(\ldots((\alpha_1 \wedge \alpha_2) \wedge \alpha_3) \wedge) \cdots \wedge \alpha_n)$.

Satz 1.7.8 Zu jeder Formel α gibt es eine äquivalente Formel in *KNF* und eine äquivalente Formel in *DNF*.

Beweis. Wir ersetzen zuerst in α jedes Vorkommen einer Teilformel der Art $\alpha_1 \to \alpha_2$ durch $\neg\alpha_1 \vee \alpha_2$ und jedes Vorkommen einer Teilformel vom Typ $\alpha_1 \leftrightarrow \alpha_2$ durch $(\alpha_1 \wedge \alpha_2) \vee (\neg\alpha_1 \wedge \neg\alpha_2)$. Aufgrund des Äquivalenztheorems erhalten wir auf diese Weise eine zu α äquivalente Formel α', in der höchstens die Verknüpfungen $\neg$, $\vee$ und $\wedge$ vorkommen. Durch Induktion über den Formelaufbau zeigen wir nun, daß es zu α' eine äquivalente Formel in KNF bzw. in DNF gibt.

Falls α' ein Propositionalzeichen ist, so ist nichts zu zeigen, denn α' liegt bereits in KNF und in DNF vor.

Betrachten wir nun den Fall, daß α' von der Form $\alpha' = \neg\gamma$ ist. Dann gibt es nach Induktionsannahme zu γ äquivalente Formeln γ_1 in KNF bzw. γ_2 in DNF. Sei

$$\gamma_1 = \bigwedge_{i=1}^{n} (\bigvee_{j=1}^{m_i} L_{i,j}).$$

Mehrfaches Anwenden der de Morganschen Regeln auf $\neg\gamma_1$ liefert

$$\alpha' \equiv \bigvee_{i=1}^{n} \neg(\bigvee_{j=1}^{m_i} L_{i,j}) \equiv \bigvee_{i=1}^{n} (\bigwedge_{j=1}^{m_i} \neg L_{i,j}),$$

woraus wir mittels des Doppelnegationsgesetzes erhalten, daß

$$\alpha' \equiv \bigvee_{i=1}^{n} (\bigwedge_{j=1}^{m_i} \overline{L_{i,j}})$$

mit $\overline{L_{i,j}} = \eta$, falls $L_{i,j} = \neg\eta$, und $\overline{L_{i,j}} = \neg\eta$, falls $L_{i,j} = \eta$. Somit haben wir eine zu α' äquivalente Formel in DNF erhalten. Analog erhalten wir aus γ_2 eine zu α' äquivalente Formel in KNF.

Als nächstes betrachten wir den Fall, daß α' die Form $\alpha' = \gamma \vee \delta$ hat. Wegen des Dualitätsprinzips gibt es dann auch im Fall, daß α' von der Form $\alpha' = \gamma \wedge \delta$ ist,

Formeln der gewünschten Art. Nach Induktionsvoraussetzung gibt es zu γ und δ jeweils äquivalente Formeln in KNF und DNF.

Um eine zu α' äquivalente Formel in DNF zu erhalten, verknüpfen wir die Formeln in DNF zu γ und δ mittels $\vee$. Mehrfaches Anwenden des Assoziativgesetzes liefert dann die gewünschte Linksklammerung.

Um eine zu α' äquivalente Formel in KNF zu erhalten, wählen wir zunächst nach Induktionsannahme zu γ und δ äquivalente Formeln in KNF:

$$\gamma \equiv \bigwedge_{i=1}^{n} \gamma_i, \quad \delta \equiv \bigwedge_{l=1}^{k} \delta_l.$$

Hierbei sind die γ_i und δ_l Disjunktionen von Literalen. Mittels Distributivität und Assoziativität erhalten wir hieraus:

$$\alpha' = \gamma \vee \delta \equiv \bigwedge_{i=1}^{n} (\bigwedge_{l=1}^{k} (\gamma_i \vee \delta_l)).$$

Durch weitere Anwendung des Assoziativgesetzes erhält diese Formel die gewünschte Bauart

$$\alpha \equiv \bigwedge_{j=1}^{nk} \alpha_j,$$

wobei die α_j Disjunktionen von Literalen sind. Eventuell vorkommende identische Disjunktionen oder identische Literale innerhalb einer Disjunktion können nun mittels der Idempotenzgesetze eliminiert werden. Falls einige Disjunktionen Tautologien sind, z.B. $\eta \vee \neg\eta$, so können diese noch mittels der Tautologieregeln beseitigt werden. Auf diese Weise erhalten wir eine zu α' äquivalente Formel in KNF. ■

Im obigen Induktionsbeweis verbirgt sich ein rekursiver Algorithmus zur Herstellung von Formeln in KNF wie auch in DNF. Eine etwas direktere Umformungsmethode zur Herstellung der KNF ist die folgende:

Gegeben: eine Formel α.

1. Ersetze in α $(\gamma \to \delta)$ durch $(\neg\gamma \vee \delta)$ und $(\gamma \leftrightarrow \delta)$ durch $(\gamma \wedge \delta) \vee (\neg\gamma \wedge \neg\delta)$.
2. Ersetze in α jedes Vorkommen einer Teilformel der Form

$$\begin{array}{rll} \neg\neg\gamma & \text{durch} & \gamma, \\ \neg(\gamma \wedge \delta) & \text{durch} & (\neg\gamma \vee \neg\delta), \\ \neg(\gamma \vee \delta) & \text{durch} & (\neg\gamma \wedge \neg\delta), \end{array}$$

   bis keine derartige Teilformel mehr vorkommt.
3. Ersetze jedes Vorkommen einer Teilformel der Form

$$\begin{array}{lll} \beta \vee (\gamma \wedge \delta) & \text{durch} & (\beta \vee \gamma) \wedge (\beta \vee \delta), \\ (\beta \wedge \gamma) \vee \delta & \text{durch} & (\beta \vee \delta) \wedge (\gamma \vee \delta), \end{array}$$

   bis keine derartige Teilformel mehr auftritt.

Die resultierende Formel ist nun in KNF. Es kommen eventuell noch überflüssige, aber zulässige Disjunktionen vor, die Tautologien sind.

Eine weitere Methode zur Herstellung einer äquivalenten Formel in DNF haben wir schon im Beweis von Satz 1.4.4 kennengelernt. Sie bietet sich an, wenn von der gegebenen Formel α, bzw. der analog aufgebauten Wahrheitsfunktion eine Wahrheitstafel vorliegt. Um mittels der Wahrheitstafel eine zu α äquivalente Formel in KNF zu erhalten, vertauschen wir in der gerade erwähnten Methode die Rollen von **w** und **f**, sowie von Konjunktion und Disjunktion.

Zum Abschluß dieser Betrachtungen soll noch darauf hinwiesen werden, daß die mit den erläuterten Methoden gebildeten Formeln in DNF oder KNF nicht notwendigerweise die kürzest möglichen sind. Beachte ferner, daß der Umformungsprozeß in eine Formel in KNF oder DNF diese exponentiell aufblähen kann. Aus einer Ausgangsformel der Länge n kann eine Formel entstehen, deren Länge in der Größenordnung von 2^n liegt. Da die DNF bezüglich einer gegebenen Wahrheitstafel durch die Zeilen mit einem **w** in der letzten Spalte und die KNF durch die Zeilen mit einem **f** in der letzten Spalte bestimmt ist, hat eine Formel mit kurzer DNF–Darstellung i.a. eine lange KNF–Darstellung und umgekehrt.

1.8 Das Erfüllbarkeitsproblem

Wir wollen uns in diesem Abschnitt mit dem Problem **SAT** (satisfiatibility) beschäftigen:

Gegeben: Eine aussagenlogische Formel α.
Frage: Ist α erfüllbar?

Da die Erfüllbarkeit einer Formel nach dem Koinzidenzlemma nur von den Wahrheitswerten abhängt, die den in der Formel auftretenden Propositionalzeichen zugewiesen werden, können wir uns bei der Untersuchung der Erfüllbarkeit auf die Betrachtung der Restriktionen von Wahrheitsbelegungen auf diese Zeichen beschränken. Dies wollen wir in diesem Abschnitt tun. Wahrheitsbelegungen sind dann also endliche Folgen. Dann ist die Erfüllbarkeit einer Formel aber algorithmisch feststellbar, indem die endlich vielen möglichen Zuweisungen von Wahrheitswerten an die in der Formel auftretenden Propositionalzeichen durchprobiert werden, bis eine erfüllende gefunden wird bzw. nach Betrachtung aller dieser Belegungen feststellt wird, daß die Formel unerfüllbar ist. Der Aufwand bei diesem Verfahren ist jedoch gewaltig: Für eine Formel mit n Propositionalzeichen müssen 2^n Belegungen betrachtet werden. Nehmen wir einmal an, der Wahrheitswert einer gegebenen Formel mit 100 Propositionalzeichen könnte in einer Mikrosekunde berechnet werden, so wäre der Rechner im schlechtesten Fall 10^{20} Jahre beschäftigt, um die Erfüllbarkeit der Formel festzustellen.

Probleme, die nur von Algorithmen gelöst werden, deren maximale Schrittzahl exponentiell in der Länge der Eingabe wächst, heißen *nicht behandelbar*. Sind sie durch einen Algorithmus lösbar, dessen Schrittzahl höchstens polynomiell in der Länge der Eingabe wächst, so heißen sie *behandelbar*.

Es ist bis heute nicht bekannt, ob das Problem **SAT** behandelbar ist. Es ist allerdings mit polynomiell beschränkter Schrittzahl lösbar, wenn wir zulassen, daß der Algorithmus polynomiell beschränkt viele Rateschritte ausführen darf, und nur die Überprüfung von richtig Geratenem bei der Zählung der Schritte berücksichtigt wird. Da mit polynomiell beschränkter Schrittzahl festgestellt werden kann, ob eine — geratene — Belegung eine gegebene Formel erfüllt, ist ein solches Verfahren in der Tat leicht konstruierbar.

Wir wollen diesen Sachverhalt nun etwas genauer diskutieren. Sei hierzu SP (STRING PASCAL) diejenige Teilsprache von PASCAL, in der nur die Datentypen *string* und *character* mit den zugehörigen Operationen zugelassen sind. Ausdrücke mit Wert *boolean* dürfen nur im Bedingungsteil von bedingten Anweisungen und Schleifenanweisungen auftreten.

Definition 1.8.1

1. Seien Σ_1, Σ_2 Alphabete, die mindestens zwei Elemente enthalten. Dann heißt $f : \Sigma_1^* \to \Sigma_2^*$ *in Polynomzeit berechenbar*, wenn es ein SP–Programm gibt, welches f berechnet, so daß die Laufzeit des Programms polynomiell in der Länge der Eingabe beschränkt ist.

2. $A \subseteq \Sigma_1^*$ heißt *in deterministischer Polynomzeit akzeptierbar*, wenn die Funktion $f : \Sigma_1^* \to \{0, 1\}$ mit $f(x) = 1$ genau dann wenn $x \in A$, in Polynomzeit berechenbar ist. f heißt *charakteristische Funktion* von A. Sei $\mathcal{P}$ die Klasse der in deterministischer Polynomzeit akzeptierbaren Mengen.

3. $A \subseteq \Sigma_1^*$ heißt *in nichtdeterministischer Polynomzeit akzeptierbar*, falls es ein Polynom p, ein Alphabet Σ und eine in deterministischer Polynomzeit akzeptierbare Menge $B \subseteq \Sigma^* \times \Sigma_1^*$ gibt, so daß genau dann $x \in A$, wenn es ein $y \in \Sigma^*$ mit $lth(y) \leq p(lth(x))$ und $(y, x) \in B$ gibt. Sei $\mathcal{NP}$ die Klasse der in nicht deterministischer Polynomzeit akzeptierbaren Mengen.

In der letzten Definition entspricht die Forderung nach der Existenz eines y mit den genannten Eigenschaften gerade der oben erwähnten Ratebedingung. Natürlich lassen sich Verfahren dieser Art deterministisch simulieren: Wir überprüfen alle $y \in B$ mit $lth(y) \leq p(lth(x))$. Nur gibt es davon leider $\|\Sigma\|^{p(lth(x))}$ viele. Bis heute ist nicht bekannt, ob $\mathcal{P} = \mathcal{NP}$, wohl aber wissen wir von vielen Problemen, auch solchen, für die schnelle (deterministische) Algorithmen von enormer wirtschaftlicher Bedeutung wären, daß sie in $\mathcal{NP}$ liegen.

Wie wir oben angedeutet haben, gilt:

Satz 1.8.2 $\mathcal{SAT} \in \mathcal{NP}$.

Unter den Problemen in $\mathcal{NP}$ gibt es nun besonders schwere.

Definition 1.8.3

1. Sei $A \subseteq \Sigma_1^*$ und $B \subseteq \Sigma_2^*$. A heißt *in Polynomzeit m–reduzierbar auf B*, falls es eine in Polynomzeit berechenbare Funktion $f : \Sigma_1^* \to \Sigma_2^*$ gibt, so daß genau dann $x \in A$, wenn $f(x) \in B$.
2. $B \in \mathcal{NP}$ heißt *$\mathcal{NP}$–vollständig,*wenn jede Menge $A \in \mathcal{NP}$ in Polynomzeit m–reduzierbar auf B ist.

Lemma 1.8.4

1. Ist $B \in \mathcal{P}$ und A in Polynomzeit m–reduzierbar auf B, so ist auch $A \in \mathcal{P}$.
2. Ist B $\mathcal{NP}$–vollständig, so ist genau dann $\mathcal{P} = \mathcal{NP}$, wenn $B \in \mathcal{P}$.

Beweis. Da offensichtlich $\mathcal{P} \subseteq \mathcal{NP}$, folgt (2) aus (1). Wir zeigen nun (1). Werde A durch die Funktion f in Polynomzeit auf B m–reduziert, und sei g die charakteristische Funktion von B. Da $x \in A$, genau dann wenn $f(x) \in B$, ist $g \circ f$ die charakteristische Funktion von A. Nach Voraussetzung sind f und g in Polynomzeit berechenbar. Seien p, q die zugehörigen, die Laufzeit beschränkenden Polynome. Dann ist $g \circ f$ in durch $p + q \circ p$ beschränkte Laufzeit berechenbar. Also ist $A \in \mathcal{P}$. ■

Der Teil (2) des obigen Lemmas zeigt, worin die Bedeutung der $\mathcal{NP}$–vollständigen Probleme liegt. In der Komplexitätstheorie wird gezeigt

Satz 1.8.5 — Cook 1971. **SAT** ist $\mathcal{NP}$–vollständig.

Nachdem wir die Schwierigkeit des allgemeinen Erfüllbarkeitproblems genauer untersucht haben, wollen wir uns nun einer Formelklasse zuwenden, für die das Erfüllbarkeitsproblem sehr einfach zu lösen ist, den Hornformeln, benannt nach dem Logiker *Alfred Horn*. Hornformeln sind vor allem in der Logikprogrammierung von großer Bedeutung.

Definition 1.8.6 Eine Formel α ist eine *Hornformel*, falls $\alpha = \beta_1 \wedge \ldots \wedge \beta_n$, wobei für $i = 1, \ldots, n$ entweder β_i ein von $\bot$ verschiedenes Propositionalzeichen ist oder $\beta_i = \gamma_i \to C_i$ mit einem Propositionalzeichen C_i und $\gamma_i = B_i^1 \wedge \ldots \wedge B_i^{m_i}$ für gewisse, von $\bot$ verschiedene Propositionalzeichen B_i^j $(1 \leq j \leq m_i)$.

Wie schon gesagt, gibt es für Hornformeln einen sehr effizienten Erfüllbarkeitstest, der wie folgt arbeitet:

Eingabe : eine Hornformel $\alpha = \beta_1 \wedge \ldots \wedge \beta_n$

1. Versehe jedes Vorkommen eines Propositionalzeichens A in α mit einer Markierung, falls für ein i mit $1 \leq i \leq n$ $\beta_i = A$;

2. **while** für ein i mit $1 \leq i \leq n$ ist $\beta_i = B_i^1 \wedge \ldots ... \wedge B_i^{m_i} \rightarrow C_i$ mit bereits markierten $B_i^1, \ldots, B_i^{m_i}$ und noch nicht markiertem C_i **do**
   if $C_i \neq \perp$ **then**
   markiere jedes Vorkommen von C_i
   else gib „unerfüllbar“ aus und stoppe;
3. Gib „erfüllbar“ aus und stoppe. (Die erfüllende Belegung $\mathcal{B}$ wird hierbei durch die Markierung gegeben: für ein Propositionalzeichen A ist genau dann $\mathcal{B}(A) = \mathbf{w}$ wenn A eine Markierung hat.)

Satz 1.8.7 Der obige Markierungsalgorithmus ist für Hornformeln als Eingabe korrekt und stoppt immer nach spätestens n Markierungsschritten, wobei n die Anzahl der Propositionalzeichen in der gegebenen Formel ist.

Beweis. Zunächst ist es klar, daß nicht mehr Propositionalzeichen markiert werden können, als vorhanden sind, und deshalb nach spätestens n Markierungsschritten entweder die Ausgabe „erfüllbar“ oder „unerfüllbar“ erreicht wird.

Zur Korrektheit des Algorithmus' beobachten wir zunächst, daß bezüglich jeder die Eingabeformel α erfüllenden Belegung $\mathcal{B}$ — sofern eine solche überhaupt existiert — für die im Laufe des Verfahrens markierten Propositionalzeichen A $\mathcal{B}(A) = \mathbf{w}$ gelten muß. Dies ist unmittelbar einleuchtend im Schritt 1 des Algorithmus', da eine konjunktive Verknüpfung von Formeln unter einer Belegung $\mathcal{B}$ nur dann den Wert $\mathbf{w}$ erhalten kann, wenn alle Konjunktionsglieder unter $\mathcal{B}$ den Wert $\mathbf{w}$ erhalten. Besteht ein solches Konjunktionsglied, wie im Schritt 1, nur aus einem Propositionalzeichen, so muß dies notwendigerweise mit $\mathbf{w}$ belegt werden. Damit ergibt sich auch die Notwendigkeit, im Schritt 2 alle Propositionalzeichen C_i mit $\mathbf{w}$ zu belegen, sofern $C_i \neq \perp$ und $B_i^1, \ldots, B_i^{m_i}$ bereits markiert sind. Diese Überlegung zeigt auch, daß im Schritt 2 korrekterweise „unerfüllbar“ ausgegeben wird, falls $C_i = \perp$ und die $B_i^1, \ldots, B_i^{m_i}$ markiert sind.

Kommt der Markierungsprozeß in Schritt 2 erfolgreich zu Ende, so liefert Schritt 3 korrekterweise die Ausgabe „erfüllbar“ und die Markierung liefert ein Modell $\mathcal{B}$ für α.

Dies sehen wir wie folgt: Sei β_i ein beliebiges Konjunktionsglied in α. Falls β_i ein Propositionalzeichen ist, so wird bereits im Schritt 1 $\mathcal{B}(\beta_i) = \mathbf{w}$ gesetzt. Falls $\beta_i = B_i^1 \wedge \ldots \wedge B_i^{m_i} \rightarrow C_i$, so ist entweder $C_i \neq \perp$ und alle Propositionalzeichen in β_i, wegen Schritt 2, insbesondere auch C_i, sind mit $\mathbf{w}$ belegt, oder für mindestens ein j mit $1 \leq j \leq m_i$ ist $\mathcal{B}(B_i^j) = \mathbf{f}$. In beiden Fällen folgt, daß $\hat{\mathcal{B}}(\beta_i) = \mathbf{w}$. ■

Aus dem obigen Beweis geht hervor, daß der Markierungsalgorithmus, wenn er mit Ausgabe „erfüllbar“ stoppt, das *kleinste Modell* $\mathcal{B}$ von α konstruiert: Für alle Modelle $\mathcal{B}'$ von α und alle Propositionalzeichen A in α ist $\mathcal{B}(A) \leq \mathcal{B}'(A)$. Hierbei wird die Ordnung $\mathbf{f} < \mathbf{w}$ angenommen.

Weiterhin beobachten wir, daß jede Hornformel erfüllbar ist, sofern sie keine Teilformel der Bauart $B_1 \wedge \ldots \wedge B_m \rightarrow \perp$ enthält. Genau diese Teilformeln führen in Schritt 2 möglicherweise zu der Ausgabe „unerfüllbar“.

Gleichfalls ist jede Hornformel erfüllbar, wenn sie keine Propositionalzeichen als Konjunktionsglied β_i enthält. In diesem Fall würde die **while**–Schleife nicht betreten.

1.9 Übungsaufgaben

1. Sei \$ eine weitere dreistellige logische Verknüpfung definiert durch

p	q	r	$H_{\$}(p,q,r)$
w	**w**	**w**	**w**
w	**w**	**f**	**w**
w	**f**	**w**	**w**
w	**f**	**f**	**f**
f	**w**	**w**	**w**
f	**w**	**f**	**f**
f	**f**	**w**	**f**
f	**f**	**f**	**f**

   d.h. intuitiv $\$(\alpha,\beta,\gamma)$ ist wahr genau dann, wenn mindestens zwei der Formeln wahr sind. Drücken Sie $H_{\$}$ durch $H_{\neg}$ und $H_{\vee}$.

2. Zeigen oder widerlegen Sie:
   (a) Falls $\Vdash \alpha \to \beta$ und $\Vdash \alpha$, so gilt auch $\Vdash \beta$.
   (b) Ist $\alpha \to \beta$ erfüllbar und α erfüllbar, so ist auch β erfüllbar.
   (c) Falls $\Vdash \alpha \to \beta$ und α erfüllbar ist, so ist auch β erfüllbar.

3. (Craigs Interpolationssatz) Sei $\Vdash \alpha \to \beta$ und nehmen wir an, daß α und β mindestens ein gemeinsames Propositionalzeichen enthalten. Zeigen Sie, daß es eine Formel γ gibt, die nur Propositionalzeichen enthält, die in α oder β vorkommen, so daß $\Vdash \alpha \to \gamma$ und $\Vdash \gamma \to \beta$.

4. Zeigen Sie, mit Hilfe von Satz 1.7.4, daß

$$((A \vee (B \wedge A)) \wedge (C \vee (D \wedge C)))$$

   logisch äquivalent zu $(C \vee D)$ ist.

5. Zeigen Sie, daß $\equiv$ eine Äquivalenzrelation ist.

6. Zeigen Sie die folgenden Verallgemeinerungen der de Morganschen- und Distributivitätsregeln mit Hilfe von natürlicher Induktion

$$\neg\left(\bigvee_{i=1}^{n}\alpha_i\right) \equiv \bigwedge_{i=1}^{n}\neg\alpha_i$$
$$\neg\left(\bigwedge_{i=1}^{n}\alpha_i\right) \equiv \bigvee_{i=1}^{n}\neg\alpha_i$$
$$\left(\left(\bigvee_{i=1}^{n}\alpha_i\right) \wedge \left(\bigvee_{j=1}^{m}\beta_i\right)\right) \equiv \bigvee_{i=1}^{n}\bigvee_{j=1}^{n}(\alpha_i \wedge \beta_j)$$
$$\left(\left(\bigwedge_{i=1}^{n}\alpha_i\right) \vee \left(\bigwedge_{j=1}^{m}\beta_i\right)\right) \equiv \bigwedge_{i=1}^{n}\bigwedge_{j=1}^{n}(\alpha_i \wedge \beta_j)$$

7. Überführen Sie die folgenden Formeln in DNF und KNF:
   (a) $\neg(A_1 \leftrightarrow A_2)$,

(b) $((A_1 \to A_2) \to A_2) \to A_2$,

(c) $(A_1 \to (A_1 \wedge \neg A_2)) \wedge (A_2 \to (A_2 \wedge \neg A_1))$.

8. Auf den Mengen aller Formeln können wir eine Relation $\sqsubset$ durch $\alpha \sqsubset \beta$ genau dann wenn $\Vdash \alpha \to \beta$ und $\nVdash \alpha \to \beta$.

   (a) Zeigen Sie, daß $\sqsubset$ transitiv und reflexiv ist.

   (b) Geben Sie ein Beispiel für Formeln α und β an, so daß weder $\alpha \sqsubset \beta$ noch $\beta \sqsubset \alpha$.

   (c) Finden Sie abzählbar viele Formeln $\varphi_1, \varphi_2, \ldots$, so daß

   $$\varphi_1 \sqsubset \varphi_2 \sqsubset \ldots \ .$$

2 — Prädikatenlogik

2.1 Einleitung

Die Prädikatenlogik ist eine Erweiterung der Aussagenlogik. Betrachten wir den folgenden Satz:

> Jeder von Martins Freunden ist ein Freund von Peter.

Wollen wir diesen Satz formalisieren, so reichen die Mittel der Aussagenlogik nicht aus. Neben der Implikationsverknüpfung treten in ihm noch die Relation „ist Freund von“ die Individuenkonstanten „Martin“ und „Peter“ und der Quantor „jeder“ auf. In der Prädikatenlogik lassen sich solche Sachverhalte formulieren. Ihre Sprache enthält als Basisbestandteil Zeichen für Relationen, die Beziehungen zwischen Objekten wiedergeben. Daneben können aber auch Zeichen für bestimmte Eigenschaften auftreten. Wir fassen hier Eigenschaften als einstellige Relationen auf. Wenn es nun schon einstellige Relationen gibt, macht es dann auch Sinn von nullstelligen Relationen zu sprechen. Da Aussagen Tatsachen wiedergeben, und zwar unabhängig von irgendwelchen Argumenten, ist es naheliegend sie als nullstellige Relationen aufzufassen. Bezeichne $R(x, y)$ zum Beispiel die über den natürlichen Zahlen definierte Relation „x ist kleiner als y“, dann bezeichnet $R(3, y)$ eine Eigenschaft (einstellige Relation), nämlich „3 ist kleiner als y“ und $R(3, 4)$ bezeichnet die (wahre) Aussage (die nullstellige Relation), daß 3 kleiner als 4 ist. In dem Beispiel werden x und y als *Variablen* benutzt, während 3 und 4 als Konstanten benutzt werden. Variablen fungieren als Platzhalter. Ihre Rolle kann am besten mit der folgenden Konvention verstanden werden: Zu Beginn einer Betrachtung wird ein nichtleerer Objektbereich festgelegt. Alle auftretenden Variablen werden dann als über diesem Bereich laufend aufgefasst. Konstanten sind Namen für Objekte (Individuen) in diesem Bereich. Eine weitere wichtige Art von Objekten sind *Funktionen*. Wir wollen hier nur Funktionen betrachten, die für alle Elemente des Objektbereiches definiert sind und deren Wert wieder ein Objekt des vorgegebenen Bereiches ist. So wie wir Aussagen als nullstellige Relationen auffassen können, lassen sich Konstanten als nullstellige Funktionen auffassen: Sie sind Objekte, die von keiner Eingabe abhängen. Ausdrücke, wie $f(x, g(y, 3))$, die sich aus Funktionszeichen und Variablen aufbauen lassen, heißen Terme. Wie bei den aussagenlogischen Formeln lassen sich in der Prädikatenlogik mit Hilfe der aussagenlogischen Verknüpfungen aus einfachen Relationen komplexere aufbauen.

Hierzu können aber auch der Allquantor „$\forall$“ und der Existenzquantor „$\exists$“ benutzt werden. Der Vorteil einer ausdrucksreicheren Sprache in mathematischen Untersuchungen ist offensichtlich.

2.2 Syntax der Prädikatenlogik

Wir beginnen wieder, indem wir die Sprache der Logik festlegen, mit der wir uns jetzt beschäftigen.

Definition 2.2.1 Das *Alphabet* einer Sprache erster Stufe $\mathcal{L}$ besteht aus folgenden Symbolen:

- abzählbar vielen *Variablen* $x_1, x_2, x_3, \ldots$,
- den *logischen Verknüpfungen* $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$,
- den *Quantoren* $\forall, \exists$, *All–* bzw. *Existenzquantor* genannt,
- den *Klammern*),(,
- dem nullstelligen Relationszeichen $\bot$ $(= R_0^0)$, *Falsum* genannt,
- höchstens abzählbar vielen *nichtlogischen Zeichen*:

  1. *Individuenkonstanten*: $c_1, c_2, c_3, \ldots$,
  2. *Funktionszeichen*: $f_1^1, f_1^2, \ldots, f_2^1, f_2^2, \ldots, \ldots$,
  3. *Relationszeichen*: $R_1^0, R_1^1, \ldots, R_2^0, R_2^1, \ldots, \ldots$

Der obere Index gibt bei den Funktions– und Relationszeichen die Stelligkeit an. Enthält das Alphabet das Zweistellige Relationszeichen $\doteq$, so sprechen wir von einer *Sprache erster Stufe mit Identität*. Entsprechend sprechen wir von einer *Sprache erster Stufe ohne Identität*, wenn es das Zeichen $\doteq$ nicht enthält. Jede solche Sprache ist vollständig durch ihre nichtlogischen Zeichen festgelegt.

Der Zusatz „erster Stufe“, in der obigen Defnition besagt, daß die in Ausdrücken einer solchen Sprache auftretenden Variablen nur Platzhalter für Objekte des Bereiches sind, über den wir Aussagen formulieren. Treten Variable auch als Platzhalter für Mengen von Objekten auf, so sprechen wir von einer *Sprache zweiter Stufe*. Allgemein sprechen wir von einer *Sprache n–ter Stufe*, falls in den zulässigen Ausdrücken Variablen auftreten, die über Mengen von Objekten $(n-1)$–ter Stufe laufen. Wir werden im folgenden nur Sprachen erster Stufe betrachten und diesen Zusatz daher meistens weglassen.

Was sind nun die zulässigen Ausdrücke einer Sprache erster Stufe? Wir beginnen mit der Definition der *Terme*.

Definition 2.2.2

1. Jede Variable und jede Individuenkonstante ist ein Term.
2. Ist f ein Funktionszeichen mit Stelligkeit k, und sind $t_1, \ldots, t_k$ Terme, so ist auch $f(t_1, \ldots, t_k)$ ein Term.

(In dieser wie auch den folgenden induktiven Definitionen lassen wir die zusätzliche Bedingung weg, daß nur die gemäß den genannten Bedingungen konstruierten Ausdrücke der gewünschten Art sind.) Nun können wir sagen, was die *Formeln* der Prädikatenlogik erster Stufe sind.

Definition 2.2.3

1. Ist R ein Relationszeichen der Stelligkeit k, und sind $t_1, \ldots, t_k$ Terme, so ist $R(t_1, \ldots, t_k)$ eine Formel.
2. Ist α eine Formel, dann auch $\neg\alpha$.
3. Sind α und β Formeln, so auch $(\alpha \vee \beta)$,$(\alpha \wedge \beta)$,$(\alpha \to \beta)$ und $(\alpha \leftrightarrow \beta)$.
4. Ist x eine Variable, α eine Formel dann sind auch $(\forall x\alpha)$ und $(\exists x\alpha)$ Formeln.

Die gemäß (1) gebildeten Formeln heißen *atomar*. Im Fall des Relationszeichens $\doteq$ schreiben wir $t_1 \doteq t_2$ statt $\doteq (t_1, t_2)$. Wie in der Aussagenlogik läßt sich nun zeigen:

Satz 2.2.4 Jeder Term und jede Formel läßt sich eindeutig zerlegen, d.h. , die induktiv definierten Mengen der Terme und Formeln sind frei erzeugt.

Ist α eine Formel und darüber hinaus Teilzeichenfolge einer Formel β, so heißt α *Teilformel* von β. Um die Schreibweise etwas zu vereinfachen, wollen wir auch hier die in der Aussagenlogik getroffenen Klammerkonventionen anwenden. Darüberhinaus wollen wir die Klammern über quantifizierte Formeln weglassen und annehmen, daß Quantoren stärker binden als logische Verknüpfungen. Wir schreiben also $\forall x\alpha$ und $\exists x\alpha$ statt $(\forall x\alpha)$ bzw. $(\exists x\alpha)$.

Definition 2.2.5

1. Ein Vorkommen einer Variablen x in einer Formel β heißt *gebunden*, falls x in einer Teilformel von β der Form $\forall x\alpha$ oder $\exists x\alpha$ vorkommt. Anderenfalls heißt dieses Vorkommen *frei*.
2. Wir sagen, eine Variable x *kommt in* β *frei vor*, wenn sie mindestens ein freies Vorkommen in β hat.
3. Eine Formel ohne freies Vorkommen von Variablen heißt *geschlossen* oder *Aussage*.
4. Die *Matrix* einer Formel α ist diejenige Formel, die man erhält, indem jedes Vorkommen von $\forall$ bzw. $\exists$ samt der dahinterstehenden Variablen entfernt wird. Wir bezeichnen sie mit α^*.

Eine Variable kann in einer Formel sowohl ein freies, wie auch ein gebundenes Vorkommen besitzen.

Beispiel 2.2.6 Sei $\mathcal{L}_\mathcal{A}$ die Sprache erster Stufe mit Identität, deren Alphabet außer $\doteq$ als nichtlogische Zeichen genau eine Individuenkonstante, ein einstelliges und zwei zweistellige Funktionszeichen enthält. Statt c_1, f_1^1, f_1^2 und f_2^2 benutzen wir die Bezeichnung $\dot{0}$, $\dot{s}$, $\dot{+}$ und $\dot{*}$. $\mathcal{L}_\mathcal{A}$ heißt Sprache der Arithmetik erster Stufe. Sei ferner

$$\alpha = (\neg x_1 \doteq \dot{0} \to \exists x_2(x_1 \doteq \dot{s}(x_2))) \wedge \exists x_1(x_3 \doteq x_3 \dot{+} x_1).$$

Dann ist α eine Formel dieser Sprache. Sämtliche Teilformeln sind:

α
$\neg x_1 \doteq \dot{0} \to \exists x_2(x_1 \doteq \dot{s}(x_2))$
$\neg x_1 \doteq \dot{0}$
$x_1 \doteq \dot{0}$
$\exists x_2(x_1 \doteq \dot{s}(x_2))$
$x_1 \doteq \dot{s}(x_2)$
$\exists x_1(x_3 \doteq x_3 \dot{+} x_1)$

$$x_3 \doteq x_3 \dot{+} x_1.$$

Alle in α vorkommenden Terme sind:

$$x_1, x_2, x_3, \dot{0}, \dot{s}(x_2), x_3 \dot{+} x_1$$

Alle Vorkommen von x_2 in α sind gebunden. Das erste Vorkommen von x_1 ist frei, das letzte gebunden. Ferner kommt x_3 frei in α vor. Die Formel α ist also keine Aussage.

Die Matrix von α ist die Formel

$$\alpha^* = (\neg x_1 \doteq \dot{0} \rightarrow (x_1 \doteq \dot{s}(x_2))) \wedge (x_3 \doteq x_3 \dot{+} x_1).$$

Ist α eine Formel und x eine in α frei vorkommende Variable, so schreiben wir auch $\alpha(x)$. Entsprechend schreiben wir $t(x)$, falls x in dem Term t vorkommt. Ist t' ein weiterer Term, so bezeichnet $[x/t']$ die Operation der Substitution von x durch t'. $t[x/t']$ ist also der Term, der entsteht, wenn jedes Vorkommen von x in t durch t' ersetzt wird, und $\alpha[x/t']$ ist die Formel, die wir erhalten, wenn jedes *freie* Vorkommen von x in α durch t' ersetzt wird. Wie wir nun zeigen können, kann die Ersetzung von freien Variablen in einer Formel zu unerwünschten Effekten führen.

Bezeichne $R(x, y)$ die über den natürlichen Zahlen definierte Relation, daß x kleiner y ist, und f die Addition zweier natürlicher Zahlen. Dann bezeichnet $\exists x R(x, y)$ die einstellige Relation „y ist eine von Null verschiedene Zahl“. Ersetzen wir nun y durch einen Term, indem freie Variable auftreten, so erwarten wir, daß das Ergebnis dieser Substitution wieder eine Relation bezeichnet. So besagt $\exists x R(x, f(w, w))$ z.B. , daß $2w$ eine von Null verschiedene natürliche Zahl ist. Dieses Prinzip wird aber verletzt, wenn wir y durch $f(x, x)$ ersetzen: $\exists x R(x, f(x, x))$ ist eine Aussage, die besagt, daß es eine natürliche Zahl x mit $x < x + x$ gibt.

Wir wollen aus diesem Grund nur solche Ersetzungen von x durch t in α zulassen, bei denen es keine in t vorkommenden Variablen y und keine Teilformeln von α der Art $\forall y \beta$ oder $\exists y \beta$ gibt, derart, daß x in β frei vorkommt. Die Variable x heißt in diesem Fall in α durch t *substituierbar*.

2.3 Semantik der Prädikatenlogik

Wie schon gesagt, ist eine Sprache erster Stufe durch ihre nichtlogischen Symbole festgelegt. Diese können in verschiedener Weise interpretiert werden. Es gibt für sie keine vorgegebene Standardinterpretation wie für die logischen Symbole.

Definition 2.3.1 Sei $\mathcal{L}$ eine Sprache erster Stufe. Eine *Struktur* $\mathcal{A}$ für $\mathcal{L}$ ist ein Paar $(U_\mathcal{A}, I_\mathcal{A})$, wobei U_A eine nichtleere Menge ist. Sie wird *Grundbereich*, *Individuenbereich* oder auch *Universum* genannt. $I_\mathcal{A}$ ist eine Abbildung, die

- jeder Individuenkonstanten von $\mathcal{L}$ ein Element aus $U_\mathcal{A}$,
- jedem k–stelligem Funktionszeichen von $\mathcal{L}$ eine k–stellige Funktion von $U_\mathcal{A}^k$ in $U_\mathcal{A}$ und
- jedem k–stelligem Relationszeichen von $\mathcal{L}$ eine Teilmenge von $U_\mathcal{A}^k$ zuweist, und zwar so, daß $I_\mathcal{A}(\bot) = \emptyset$ und —im Fall einer Sprache mit Identität— $I_\mathcal{A}(\doteq) = \{(a, a) \mid a \in U_\mathcal{A}\}$,

$I_\mathcal{A}$ heißt *Interpretation*.

Auch in der Prädikatenlogik ist die Bedeutung einer Aussage ein Wahrheitswert. Wir wollen nun sehen, wie dieser durch eine gegebene Struktur bestimmt ist. Hierzu dehnen wir die Interpretation auf die Menge der Terme aus. Da ein Term Variablen enthalten kann, können wir dies nur bezüglich einer vorgegebenen Belegung der Variablen mit den Werten aus dem Grundbereich tun.

Definition 2.3.2

1. Eine *Belegung* ist eine Abbildung s der Menge der Variablen in den Grundbereich $U_\mathcal{A}$. Statt Belegung sagen wir auch *Umgebung*.
2. Sei x eine Variable, s eine Umgebung und $a \in U_\mathcal{A}$. Dann ist $s[x \leftarrow a]$ diejenige Belegung, die x den Wert a und allen übrigen Variablen y den Wert $s(y)$ zuordnet.

Nach Satz 1.3.6 läßt sich die Interpretation $I_\mathcal{A}$ nun bezüglich jeder vorgegebenen Umgebung s eindeutig so zu einer Abbildung $\hat{I_\mathcal{A}}[s]$ auf der Menge der Terme fortsetzen, daß

$$\begin{aligned}
&\hat{I_\mathcal{A}}[s](t) = s(t), \text{ falls } t \text{ eine Variable ist}\\
&\hat{I_\mathcal{A}}[s](t) = I_\mathcal{A}(t), \text{ falls } t \text{ eine Konstante ist}\\
&\hat{I_\mathcal{A}}[s](t) = I_\mathcal{A}(f)(\hat{I_\mathcal{A}}[s](t_1), \ldots, \hat{I_\mathcal{A}}[s](t_k))
\end{aligned}$$

falls t die Form $t = f(t_1, \ldots, t_k)$ hat, wobei $t_1, \ldots, t_k$ Terme und f ein k–stelliges Funktionszeichen ist.

Definition 2.3.3 Sei α eine Formel und s eine Umgebung. Durch Rekursion über den Formelaufbau können wir nun definieren, wann α bezüglich s in $\mathcal{A}$ *gilt*. Wir schreiben hierfür $\mathcal{A} \models_s \alpha$.

1. Hat α die Form $\alpha = R(t_1, \ldots, t_k)$ mit einem k–stelligem Relationszeichen R und Termen $t_1, \ldots, t_k$, so

$$\mathcal{A} \models_s \alpha \iff (\hat{I_\mathcal{A}}[s](t_1), \ldots, \hat{I_\mathcal{A}}[s](t_k)) \in I_\mathcal{A}(R).$$

2. Hat α die Form $\alpha = (\neg\beta)$, so

$$\mathcal{A} \models_s \alpha \iff \mathcal{A} \not\models_s \beta.$$

3. Hat α die Form $\alpha = (\beta \vee \gamma)$, so

$$\mathcal{A} \models_s \alpha \iff \mathcal{A} \models_s \beta \quad \text{oder} \quad \mathcal{A} \models_s \gamma.$$

4. Hat α die Form $\alpha = (\beta \wedge \gamma)$, so

$$\mathcal{A} \models_s \alpha \iff \mathcal{A} \models_s \beta \quad \text{und} \quad \mathcal{A} \models_s \gamma.$$

5. Hat α die Form $\alpha = (\beta \to \gamma)$, so

$$\mathcal{A} \models_s \alpha \iff \mathcal{A} \not\models_s \beta \quad \text{oder} \quad \mathcal{A} \models_s \gamma.$$

6. Hat α die Form $\alpha = (\beta \leftrightarrow \gamma)$, so

$$\mathcal{A} \models_s \alpha \iff \text{entweder} \quad \mathcal{A} \models_s \beta \quad \text{und} \quad \mathcal{A} \models_s \gamma \quad \text{oder} \quad \mathcal{A} \not\models_s \beta \quad \text{und} \quad \mathcal{A} \not\models_s \gamma.$$

7. Hat α die Form $\alpha = (\forall x\beta)$, so

$$\mathcal{A} \models_s \alpha \iff \text{für alle } u \in U_{\mathcal{A}} \quad \mathcal{A} \models_{s[x \leftarrow u]} \beta.$$

8. Hat α die Form $\alpha = (\exists x\beta)$, so

$$\mathcal{A} \models_s \alpha \iff \text{es gibt ein } u \in U_{\mathcal{A}}, \text{ so daß } \mathcal{A} \models_{s[x \leftarrow u]} \beta.$$

Wie die obigen Definitionen vermuten lassen, hängt die Interpretation eines Terms, bzw. das Gelten einer Formel bezüglich einer Umgebung nur von den Werten ab, die den frei vorkommenden Variablen durch die Umgebung zugewiesen werden.

Lemma 2.3.4 Seien t ein Term, α eine Formel und s,$\hat{s}$ Umgebungen. Dann gilt:

1. Stimmen s und $\hat{s}$ bezüglich der in t vorkommenden Variablen überein, so

$$\hat{I}_{\mathcal{A}}[s](t) = \hat{I}_{\mathcal{A}}[\hat{s}](t) \ .$$

2. Stimmen s und $\hat{s}$ bezüglich der in α frei vorkommenden Variablen überein, so gilt genau dann $\mathcal{A} \models_s \alpha$, wenn $\mathcal{A} \models_{\hat{s}} \alpha$.

Beweis. Das obige Lemma läßt sich leicht durch Induktion über den Term– bzw. Formelaufbau beweisen. Wir betrachten nur den Fall, daß α die Form $\forall x\beta$ hat. Aus Symmetriegründen genügt es, eine der beiden Richtungen zu zeigen. Gelte also $\mathcal{A} \models_s \alpha$. Dann gilt für alle $u \in U_{\mathcal{A}}$, daß $\mathcal{A} \models_{s[x \leftarrow u]} \beta$. Da $s[x \leftarrow u]$ und $\hat{s}[x \leftarrow u]$ bezüglich der in β frei vorkommenden Variablen übereinstimmen, gilt nach Induktionsvoraussetzung auch für alle $u \in U_{\mathcal{A}}$, daß $\mathcal{A} \models_{\hat{s}[x \leftarrow u]} \beta$. Das heißt, es gilt $\mathcal{A} \models_{\hat{s}} \alpha$. ■

Auch das folgende Resultat läßt sich leicht durch Induktion über den Term– bzw. Formelaufbau beweisen. Es besagt, daß Substitution und Interpretation unabhängig voneinander ausgeführt werden können.

Lemma 2.3.5 — Substitutionslemma. Seien t und t' Terme, α eine Formel und x eine Variable derart, daß x in α durch t substituierbar ist. Dann gilt:

1. $\hat{I_{\mathcal{A}}}[s](t'[x/t]) = \hat{I_{\mathcal{A}}}[s[x \leftarrow \hat{I_{\mathcal{A}}}[s](t)]](t')$
2. $\mathcal{A} \models_s \alpha[x/t] \iff \mathcal{A} \models_{[s[x \leftarrow \hat{I_{\mathcal{A}}}[s](t)]}} \alpha$.

Beweis. Beweis durch Induktion über den Aufbau von t' bzw. α. ■

Definition 2.3.6 Sei α eine Formel, dann *gilt* α in $\mathcal{A}$, wenn α bezüglich jeder Umgebung in $\mathcal{A}$ gilt. In diesem Fall heißt $\mathcal{A}$ *Modell* von α. Ist Γ eine Menge von Formeln, so heißt $\mathcal{A}$ *Modell* von Γ, wenn alle Formeln aus Γ in $\mathcal{A}$ gelten. Wir schreiben hierfür: $\mathcal{A} \models \Gamma$.

Eine Aussage α erhält bezüglich einer Struktur A den Wahrheitswert **w**, wenn α in A gilt. Da die leere Menge keine Elemente enthält, auch nicht das 0–Tupel, gilt $\perp$ in keiner Struktur, erhält also, wie in der Aussagenlogik, immer den Wahrheitswert **f**. Kommen in einer Formel keine Variable frei vor, d.h. sie ist eine Aussage, so gilt sie aufgrund des Koinzidenzlemmas genau dann in einer Struktur, wenn sie bezüglich einer Umgebung in ihr gilt. Daher gilt für Aussagen α in A immer entweder α oder $\neg\alpha$. Dies ist im allgemeinen nicht mehr der Fall, wenn in α Variable frei vorkommen. Wir betrachten hierzu folgendes

Beispiel 2.3.7 Enthalte $\mathcal{L}$ die nichtlogischen Zeichen c, f, g, P und Q. Hierbei haben f und P die Stelligkeit 1 und g und Q die Stelligkeit 2. Seien ferner x und y Variablen. Dann ist

$$\alpha = \forall x Q(x, f(x)) \wedge P(g(c, y))$$

eine Formel. Wir wollen nun eine Struktur für L angeben. Sei hierzu $\mathcal{A} = (U, I)$, wobei U die Menge der natürlichen Zahlen und I durch

$$\begin{aligned}
I(c) &= 2 \\
I(f) &= \text{die Nachfolgerfunktion auf } U, \\
&\quad \text{also } I(f)(n) = n + 1, \\
I(g) &= \text{die Additionsfunktion auf } U, \\
&\quad \text{also } I(g)(m, n) = m + n, \\
I(P) &= \{n \in U \mid n \text{ ist Primzahl }\}, \\
I(Q) &= \{m, n \mid m, n \in U \text{ und } m < n\},
\end{aligned}$$

definiert ist. Sind dann s und s' Umgebungen mit $s(y) = 3$ bzw. $s'(y) = 4$ und $s(z) = s'(z) = 0$ für alle übrigen Variablen z, so gilt α bezüglich s in $\mathcal{A}$, denn jede natürliche Zahl ist kleiner als ihr Nachfolger und die Summe von 2 und 3 ist eine Primzahl. Da die Summe von 2 und 4 keine Primzahl ist, gilt α aber nicht bezüglich s' in A.

Besitzt eine Sprache mindestens eine Individuenkonstante, so läßt sich auch aus den Zeichen der Sprache eine zugehörige Struktur konstruieren. Wir wählen hierbei als Grundbereich U die Menge der variablenlosen Terme der Sprache. Im Fall der obigen Sprache ist dies die Menge

$$U = \{c, f(c), g(c, c), f(g(c, c)), g(f(c), c), \ldots\}.$$

Die nichtlogischen Zeichen der Sprache werden dann wie folgt interpretiert:

- $I(c)$ ist der Term c,
- $I(f)$ ist die Funktion, die jedem Term t den Term $f(t)$ zuordnet und
- $I(g)$ ist die Funktion, die zwei beliebigen Termen t_1 und t_2 denTerm $g(t_1, t_2)$ zuordnet.

Die Zeichen P und Q werden durch Teilmengen von U bzw. U^2 interpretiert, die je nach Aufgabenstellung so gewählt werden können, daß die Struktur (U, I) Modell von α oder aber kein Modell von α ist. Wie wir später sehen werden, hat jede Formelmenge, die überhaupt ein Modell hat, schon ein Modell der beschriebenen Art.

Definition 2.3.8 Ist α eine Formel, in der genau die Variablen $y_1, \ldots, y_n$ frei vorkommen, dann heißt die Aussage $\forall y_1 \ldots \forall y_n \alpha$ der *Allabschluß* und die Aussage $\exists y_1 \ldots \exists y_n \alpha$ der *Existenzabschluß* von α.

Hierfür gilt:

Lemma 2.3.9 Ist $\mathcal{A}$ eine Struktur für $\mathcal{L}$, so gilt α genau dann in $\mathcal{A}$, wenn der Allabschluß von α in $\mathcal{A}$ gilt, d.h. dort den Wahrheitswert **w** hat.

Definition 2.3.10

1. Ist Γ eine Menge von Formeln einer Sprache, so heißt Γ *erfüllbar*, wenn es eine Struktur $\mathcal{A}$ für diese Sprache und eine Umgebung s gibt, so daß jede Formel in Γ bezüglich s in $\mathcal{A}$ gilt. Anderenfalls heißt Γ *unerfüllbar*.
2. Gilt eine Formel α in jeder Struktur für die zugehörige Sprache, so heißt α *allgemeingültig*. Wir schreiben in diesem Fall: $\models \alpha$.

Lemma 2.3.11

1. α ist genau dann allgemeingültig, wenn der Allabschluß von α allgemeingültig ist.
2. α ist genau dann erfüllbar, wenn der Existenzabschluß erfüllbar ist.

Wie im aussagenlogischen Fall läßt sich ferner leicht zeigen, daß eine Formel α genau dann allgemeingültig ist, wenn $\neg\alpha$ unerfüllbar ist.

Die Prädikatenlogik ist im folgenden Sinn eine Erweiterung der Aussagenlogik: Falls nur nullstellige Relationszeichen auftreten (dann erübrigen sich automatisch Terme, Variablen und Quantoren), erhalten wir im Prinzip die Formeln der Aussagenlogik, wobei nun die nullstelligen Relationszeichen die Rolle der Propositionalzeichen der Aussagenlogik übernehmen. Die Begriffe „erfüllbar“ und „allgemeingültig“ aus der Aussagen– und der Prädikatenlogik sind dann identisch.

Es genügt sogar, lediglich die Variablen (und damit die Quantoren) zu verbieten, damit die Prädikatenlogik zur Aussagenlogik „degeneriert“. Sei z.B.

$$\alpha = (Q(a) \vee \neg R(f(b), c) \wedge P(a, b)$$

eine Formel ohne Variablen (aber mit mehr als nullstelligen Relationszeichen!). Indem wir die vorkommenden atomaren Formeln mit Propositionalzeichen der Aussagenlogik identifizieren

$$\begin{aligned} Q(a) &\longleftrightarrow A_2 \\ R(f(b), c) &\longleftrightarrow A_3 \\ P(a, b) &\longleftrightarrow A_4 \end{aligned}$$

erhalten wir die aussagenlogische Formel

$$\alpha' = (A_2 \vee A_3) \wedge A_4.$$

Offensichtlich ist (ein so gewonnenes) α' genau dann erfüllbar oder allgemeingültig, wenn α erfüllbar bzw. allgemeingültig ist.

Wie wir sehen, ist die Struktur aussagenlogischer Formeln in einem gewissen Sinn gröber als die prädikatenlogischer Formeln. Wir wollen nun zeigen, daß auch bei der „Verfeinerung“ aussagenlogischer Ausdrücke, d.h. beim Ersetzen von Propositionalzeichen durch prädikatenlogische Formeln zumindest die Allgemeingültigkeit erhalten bleibt.

Satz 2.3.12 Sei PZ eine Menge von Propositionalzeichen und σ eine Abbildung von PZ in die Menge der prädikatenlogischen Formeln. Sei ferner α eine aussagenlogische Formel, deren Propositionalzeichen in PZ enthalten sind. Bezeichne $\hat{\sigma}(\alpha)$ diejenige prädikatenlogische Formel, die wir erhalten, wenn jedes Propositionalzeichen A in α durch $\sigma(A)$ ersetzt wird. Ist dann α eine Tautologie, so ist $\hat{\sigma}(\alpha)$ allgemeingültig.

Beweis. Sei $\mathcal{A}$ eine Struktur für die Sprache $\mathcal{L}$ und s eine Umgebung. Definiere nun eine Wahrheitsbelegung $\mathcal{B}$, so daß für jedes Propositionalzeichen $A \in PZ$

$$\mathcal{B}(A) = \mathbf{w} \iff \mathcal{A} \models_s \sigma(A).$$

Wie sich durch Induktion über den Aufbau aussagenlogischer Formeln leicht zeigen läßt, ist dann

$$\hat{\mathcal{B}}(\alpha) = \mathbf{w} \iff \mathcal{A} \models_s \hat{\sigma}(\alpha).$$

Da α eine Tautologie ist, ist $\hat{\mathcal{B}}(\alpha) = \mathbf{w}$. Also haben wir, daß $\mathcal{A} \models_s \hat{\sigma}(\alpha)$. Nun waren $\mathcal{A}$ und s beliebig gewählt. Daher ist $\hat{\sigma}(\alpha)$ allgemeingültig. ■

Wir haben schon gesehen, daß die Definition von Begriffen wie „erfüllbar“ und „allgemeingültig“ fast wörtlich von der Aussagenlogik in die Prädikatenlogik übertragen wurden. Sie lassen sich in jede Logik mit einem sinnvollen Modellbegriff übertragen. Dies gilt auch für den Begriff der logischen Folgerung.

Definition 2.3.13 Sei Γ eine Formelmenge. Eine Formel β ist *logische Folgerung* von Γ, falls β in jedem Modell von Γ gilt. Wir schreiben hierfür wieder $\Gamma \models \beta$.

Lemma 2.3.14 Seien Γ eine Formelmenge, α und β Formeln, x eine Variable und t eine Term, so daß x in α durch t substituierbar ist. Dann gilt:

1. Ist $\Gamma, \alpha \models \beta$, so ist $\Gamma \models \alpha \to \beta$.
2. Ist $\Gamma \models \alpha \to \beta$, so ist $\Gamma, \alpha \models \beta$.
3. Ist $\Gamma \models \alpha$ und kommt x in keiner Formel aus Γ frei vor, so ist $\Gamma \models \forall x \alpha$.
4. Ist $\Gamma \models \forall x \alpha$, so ist auch $\Gamma \models \alpha[x/t]$.

Beweis. Die Aussagen (1) und (2) können wie in der Aussagenlogik bewiesen werden. (4) folgt mit dem Substitutionslemma sofort aus der Defintition 2.3.3. Wir zeigen nun (3).

Seien hierzu $\mathcal{A}$ eine Struktur und s eine Umgebung, so daß jede Formel aus Γ bezüglich s in $\mathcal{A}$ gilt. Sei nun $u \in U_{\mathcal{A}}$. Da x in keiner Formel aus Γ frei vorkommt, gilt nach dem Koinzidenzlemma jede solche Formel auch bezüglich $s[x \leftarrow u]$ in $\mathcal{A}$. Dann gilt auch α bezüglich $s[x \leftarrow u]$ in $\mathcal{A}$, woraus folgt, daß $\forall x \alpha$ bezüglich s in $\mathcal{A}$ gilt. ■

Lemma 2.3.15 Seien f und R ein n–stelliges Funktions– bzw. Relationszeichen einer Sprache mit Identität und $t, t_1, \ldots, t_n, t'_1, \ldots, t'_n$ Terme dieser Sprache. Dann gilt:

1. $\models t \doteq t$,
2. $t_1 \doteq t'_1, \ldots, t_n \doteq t'_n \models f(t_1, \ldots, t_n) \doteq f(t'_1, \ldots, t'_n)$.
3. $t_1 \doteq t'_1, \ldots, t_n \doteq t'_n \models R(t_1, \ldots, t_n) \leftrightarrow R(t'_1, \ldots, t'_n)$.

2.4 Äquivalenz und Normalform

Wie in der Aussagenlogik sagen wir:

Definition 2.4.1 Zwei Formeln α und β sind *(semantisch) äquivalent*, wenn für jede Struktur $\mathcal{A}$ und jede Umgebung s genau dann α bezüglich s in $\mathcal{A}$ gilt, wenn β bezüglich s in $\mathcal{A}$ gilt. Wir schreiben in diesem Fall wieder $\alpha \equiv \beta$.

Offensichtlich sind α und β genau dann äquivalent, wenn $(\alpha \leftrightarrow \beta)$ allgemeingültig ist. Mit Satz 2.3.12 lassen sich daher die in Abschnitt 1.8 behandelten aussagenlogischen Äquivalenzen in die Prädikatenlogik übertragen. Darüberhinaus gibt es aber in der Prädikatenlogik noch Äquivalenzen, welche die Vertauschbarkeit der Quantoren untereinander, sowie mit den logischen Verknüpfungen behandlen.

Satz 2.4.2 Seien α, β und γ Formeln, x und y Variablen und komme x nicht frei in γ vor. Dann gilt:

1. $\neg\forall x\ \alpha \equiv \exists x\ \neg\alpha$
   $\neg\exists x\ \alpha \equiv \forall x\ \neg\alpha$

2. $(\forall x\ \alpha \wedge \forall x\ \beta) \equiv \forall x\ (\alpha \wedge \beta)$
   $(\exists x\ \alpha \vee \exists x\ \beta) \equiv \exists x\ (\alpha \vee \beta)$

3. $(\forall x\ \alpha \wedge \gamma) \equiv \forall x\ (\alpha \wedge \gamma)$
   $(\forall x\ \alpha \vee \gamma) \equiv \forall x\ (\alpha \vee \gamma)$
   $(\exists x\ \alpha \wedge \gamma) \equiv \exists x\ (\alpha \wedge \gamma)$
   $(\exists x\ \alpha \vee \gamma) \equiv \exists x\ (\alpha \vee \gamma)$

4. $\forall x\ \forall y\ \alpha \equiv \forall y\ \forall x\ \alpha$
   $\exists x\ \exists y\ \alpha \equiv \exists y\ \exists x\ \alpha$

Beweis. Die genannten Äquivalenzen lassen sich sehr einfach mit Hilfe der entsprechenden Definitionen beweisen. Wir führen exemplarisch nur den Beweis für die erste Äquivalenz in (3) vor. Sei hierzu $\mathcal{A} = (U, I)$ eine Struktur für die zugrundeliegende Sprache und s eine Umgebung. Dann gilt:

$$
\begin{array}{ll}
& \mathcal{A} \models_s (\forall x\ \alpha \wedge \gamma) \\
\iff & \mathcal{A} \models_s (\forall x\ \alpha) \quad \text{und} \quad \mathcal{A} \models_s \gamma \\
\iff & \text{für alle } u \in U_{\mathcal{A}}\ \mathcal{A} \models_{s[x \leftarrow u]} \alpha \quad \text{und} \quad \mathcal{A} \models_s \gamma \\
\iff & \text{für alle } u \in U_{\mathcal{A}}\ \mathcal{A} \models_{s[x \leftarrow u]} \alpha \quad \text{und} \quad \mathcal{A} \models_{s[x \leftarrow u]} \gamma \\
& \qquad\qquad\qquad\qquad \text{wegen des Koinzidenzlemmas} \\
\iff & \text{für alle } u \in U_{\mathcal{A}}\ \mathcal{A} \models_{s[x \leftarrow u]} (\alpha \wedge \gamma) \\
\iff & \mathcal{A} \models_s \forall x\ (\alpha \wedge \gamma)
\end{array}
$$

■

Die in (2) gegenüber (3) nicht betrachteten Formelpaare sind nicht äquivalent:

$$
\begin{array}{lcl}
(\forall x\ \alpha \vee \forall x\ \beta) & \not\equiv & \forall x\ (\alpha \vee \beta) \\
(\exists x\ \alpha \wedge \exists x\ \beta) & \not\equiv & \exists x\ (\alpha \wedge \beta)
\end{array}
$$

Wie in der Aussagenlogik gilt auch in der Prädikatenlogik das folgende Äquivalenztheorem. Wir haben nur den in Abschnitt 1.8 gegebenen Beweis um die jetzt zusätzlich vorkommenden Fälle zu ergänzen.

Satz 2.4.3 — Äquivalenztheorem. Seien α und β äquivalente Formeln. Sei γ eine Formel mit (mindestens) einem Vorkommen der Teilformel α, und gehe γ' aus γ durch Ersetzen (irgend–)eines Vorkommens von α durch β hervor. Dann sind γ und γ' äquivalent.

Mit Hilfe der in Lemma 1.8.4 und Satz 2.4.2 angegebenen Äquivalenzumformungen lassen sich die in einer Formel eventuell vorkommenden Quantoren nach außen ziehen.

Beispiel 2.4.4

$$
\begin{aligned}
&\neg(\exists x Q(x,y) \vee \forall z P(z)) \wedge \exists w P(g(c,w)) \\
&\equiv (\neg\exists x Q(x,y) \wedge \neg\forall z P(z)) \wedge \exists w P(g(c,w)) && (deMorgan)\\
&\equiv (\forall x \neg Q(x,y) \wedge \exists z \neg P(z) \wedge \exists w P(g(c,w)) && (wegen Satz 2.4.2(1))\\
&\equiv \exists w P(g(c,w)) \wedge (\forall x \neg Q(x,y) \wedge \exists z \neg P(z)) && (\text{Kommutativität})\\
&\equiv \exists w (P(g(c,w)) \wedge (\forall x \neg Q(x,y) \wedge \exists z \neg P(z)) && (wegen Satz 2.4.2(3))\\
&\equiv \exists w ((\exists z \neg P(z) \wedge \forall x \neg Q(x,y)) \wedge P(g(c,w))) && (\text{Kommutativität})\\
&\equiv \exists w (\forall x \exists z (\neg P(z) \wedge \neg Q(x,y)) \wedge P(g(c,w))) && (wegen Satz 2.4.2(3))\\
&\equiv \exists w \forall x \exists z (\neg P(z) \wedge \neg Q(x,y) \wedge P(g(c,w))) && (wegen Satz 2.4.2(3))
\end{aligned}
$$

Beachte, daß die Quantorenreihenfolge, die sich am Ende der Umformungskette ergibt, nicht unbedingt von vornherein eindeutig festliegt. Sie hängt von der Art und Reihenfolge der Umformungsschritte ab. Im obigen Beispiel läßt sich jede mögliche Permutation von „$\exists w$“, „$\forall x$“ und „$\exists z$“ erreichen, was aber nicht immer so sein muß. Nebeneinanderstehende, gleichartige Quantoren können jedoch nach Teil (4) von Satz 2.4.2 immer vertauscht werden.

Um Teil (3) dieses Satzes anwenden zu können, müssen wir die Möglichkeit haben, Variablen gebunden umzubenennen.

Lemma 2.4.5 — gebundene Umbenennung. Seien α eine Formel, $Q \in \{\forall, \exists\}$ ein Quantor und x, y Variablen, so daß y nicht in α vorkommt. Dann sind $Qx\alpha$ und $Qy\alpha[x/y]$ äquivalent.

Der Beweis dieses Lemmas ist sehr einfach und wird hier übergangen. Durch systematisches Ausführen von gebundenen Umbenennungen, wobei immer neue, noch nicht vorkommende Variablen verwendet werden, können wir das nächste Lemma beweisen.

Lemma 2.4.6 Zu jeder Formel α läßt sich eine äquivalente, bereinigte Formel β angeben. Hierbei heißt eine Formel *bereinigt*, sofern es keine Variable gibt, die in der Formel sowohl gebunden als auch frei vorkommt, und sofern hinter allen vorkommenden Quantoren verschiedene Variablen stehen.

Wie im obigen Beispiel bereits angedeutet, lassen sich Formeln durch Anwendung von Äquivalenzumformungen und durch eventuelles gebundenes Umbenennen in äquivalente bereinigte Formeln überführen, bei denen alle Quantoren vor der Matrix stehen.

Definition 2.4.7 Eine Formel ist *pränex* oder in *Pränexform*, falls sie die Form $Q_1 y_1 Q_2 y_2 \ldots Q_n y_n \alpha$ mit einer quantorfreien Formel α hat. Hierbei ist für $i = 1, \ldots, n$ y_i eine Variable und $Q_i \in \{\forall, \exists\}$. Ist die Formel zusätzlich bereinigt, so sagen wir, sie ist in BPF.

Satz 2.4.8 Zu jeder Formel α läßt sich eine äquivalente Formel β in BPF angeben.

Beweis. Wir führen den Beweis durch Induktion über den Formelaufbau. Ist α atomar, so ist α bereits in BPF. Wir setzen daher $\beta = \alpha$.

Hat α die Form $\neg\gamma$, und ist $\gamma_1 = Q_1 y_1 \ldots Q_n y_n\ \gamma'$ die nach Induktionsvoraussetzung existierende zu γ äquivalente Formel, so ist $\alpha \equiv \bar{Q}_1 y_1 \ldots \bar{Q}_n y_n\ \neg\gamma'$, wobei $\bar{Q}_i = \exists$, falls $Q_i = \forall$, und $\bar{Q}_i = \forall$ falls $Q_i = \exists$. Diese Formel hat die gewünschte Form.

Hat α die Form $(\gamma \Box \delta)$ mit $\Box \in \{\vee, \wedge\}$, dann gibt es zu γ und δ äquivalente Formeln γ_1 und δ_1 in BPF. Durch gebundenes Umbenennen können wir $(\gamma_1 \Box \delta_1)$ bereinigen. Hiernach habe γ_1 die Form $Q_1 y_1 \ldots Q_k y_k\ \gamma'$ und δ_1 die Form $Q'_1 z_1 \ldots Q'_m z_m\ \delta'$ mit $Q_i, Q'_j \in \{\forall, \exists, \}$. Dann ist $\alpha \equiv Q_1 y_1 \ldots Q_k y_k\ Q'_1 z_1 \ldots Q'_m z_m\ (\gamma' \Box \delta')$. Diese Formel hat die gewünschte Form.

Hat α die Form $(\gamma \Diamond \delta)$ mit $\Diamond \in \{\rightarrow, \leftrightarrow\}$, dann ist α äquivalent zu $(\neg\gamma \vee \delta)$ bzw. $((\gamma \wedge \delta) \vee (\neg\gamma \wedge \neg\delta))$. Diese Formeln können in der eben beschriebenen Weise weiter behandelt werden.

Hat schließlich α die Form $Qx\ \gamma$ mit $Q \in \{\forall, \exists\}$, so hat die nach Induktionsvoraussetzung zu γ äquivalente Formel in BPFdie Form $Q_1 y_1 \ldots Q_n y_n\ \gamma'$. Durch gebundes Umbenennen kann die Variable x von $y_1, \ldots, y_n$ verschieden gemacht werden. Dann ist $\alpha \equiv Qx\ Q_1 y_1 \ldots Q_n y_n\ \gamma'$. ■

Ist eine Formel in BPF, so wollen wir nun untersuchen, wie wir die eventuell auftretenden Existenzquantoren ohne Informationsverlust eliminieren können. Die hiernach noch vorhandenen Allquantoren können dann wegen Lemma 2.3.9 weggelassen werden.

Definition 2.4.9 Für jede Formel α in BPF definieren wir ihre *Skolemform* als das Resultat der Anwendung des folgenden Algorithmus' auf α:

while α enthält einen Existenzquantor **do**
begin
α habe die Form
$\alpha = \forall y_1 \ldots \forall y_n \exists z\ \beta$ mit einer Formel β in BPF und $n \geq 0$;
Sei f ein neues, bisher in der Sprache $\mathcal{L}$ nicht vorkommendes n–stelliges Funktionszeichen;
$\mathcal{L} := \mathcal{L} \cup \{f\}$
$\alpha := \forall y_1 \ldots \forall y_n \beta[z/f(y_1, \ldots, y_n)]$;
(d.h. , der Existenzquantor in α wird gestrichen
und jedes Vorkommen der Variablen z in β durch $f(y_1, \ldots, y_n)$ ersetzt)
end;

Beachte, daß die Sprache $\mathcal{L}$ hier in jedem Iterationsschritt um ein Funktionszeichen bzw. — im Fall $n = 0$— eine Individuenkonstante erweitert wird. Jedes solches Zeichen heißt *Skloemfunktion*. Wir werden später nocheinmal hierauf zurückkommen.

Satz 2.4.10 Sei α eine Formel in BPF, α' ihre Skolemform und entstehe $\mathcal{L}'$ aus $\mathcal{L}$ durch Hinzunahme der bei der Bildung von α' auftretenden Skolemfunktion. Dann gilt:

1. Ist $\mathcal{A}'$ eine Struktur für $\mathcal{L}'$, und gilt α' in ihr, so gilt α in der *Beschränkung* von $\mathcal{A}$ auf $\mathcal{L}$, d.h. in der Struktur $(U_{\mathcal{A}'}, I_{\mathcal{A}'} \mid \mathcal{L})$, wobei $\mathcal{I}_{\mathcal{A}'} \mid \mathcal{L}$ die Einschränkung des Definitionsbereichs von $\mathcal{I}_{\mathcal{A}'}$ auf $\mathcal{L}$ ist.
2. Ist $\mathcal{A}$ eine Struktur für $\mathcal{L}$, in der α gilt, so gibt es eine Struktur $\mathcal{A}'$ für $\mathcal{L}'$ mit dem gleichen Grundbereich wie $\mathcal{A}$, in der α' gilt. $I_{\mathcal{A}'}$ stimmt auf $\mathcal{L}$ mit $I_{\mathcal{A}}$ überein.

Beweis. Offensichtlich reicht es, Formeln α und α' in BPF zu betrachten, derart, daß α' mittels der in einem **while**–Schleifendurchlauf durchgeführten Umformungsschritte aus α hervorgeht. Sei also $\alpha = \forall y_1 \ldots \forall y_n \exists z\ \beta$. Mit den genannten Umformungsschritten erhalten wir hieraus eine Formel der Form $\alpha' = \forall y_1 \ldots \forall y_n\ \beta[z/f(y_1, \ldots, y_n)]$.

1. Wir nehmen zuerst an, daß $\mathcal{A}'$ eine Struktur für $\mathcal{L}'$ und s eine Umgebung ist, so daß α' bezüglich s in $\mathcal{A}'$ gilt. Dann gilt $\beta[z/f(y_1, \ldots, y_n)]$ für alle $u_1, \ldots, u_n \in U_{\mathcal{A}'}$ bezüglich $s[y_1 \leftarrow u_1] \ldots [y_n \leftarrow u_n]$ in $\mathcal{A}'$. Mit dem Substituitionslemma folgt für

alle $u_1, \ldots, u_n \in U_{\mathcal{A}'}$, daß β bezüglich $s[y_1 \leftarrow u_1] \ldots [y_n \leftarrow u_n][z \leftarrow v]$ in $\mathcal{A}'$ gilt, wobei $v = I_{\mathcal{A}'}(f)(u_1, \ldots, u_n)$. Also gibt es für alle $u_1, \ldots, u_n \in U_{\mathcal{A}'}$ ein $v \in U_{\mathcal{A}'}$, so daß β bezüglich $s[y_1 \leftarrow u_1] \ldots [y_n \leftarrow u_n][z \leftarrow v]$ in $\mathcal{A}'$ gilt. Dies heißt aber nichts anderes, als daß α bezüglich s in der Beschränkung von $\mathcal{A}'$ auf $\mathcal{L}$ gilt.

2. Nehmen wir nun an, daß $\mathcal{A}$ eine Struktur für $\mathcal{L}$ und s eine Umgebung ist, so daß α bezüglich s in $\mathcal{A}$ gilt. Dann gibt es für alle $u_1, \ldots, u_n \in U_{\mathcal{A}}$ ein $v \in U_{\mathcal{A}}$, so daß β bezüglich $s[y_1 \leftarrow u_1] \ldots [y_n \leftarrow u_n][z \leftarrow v]$ in $\mathcal{A}$ gilt. Sei nun F eine n–stellige Funktion auf $U_{\mathcal{A}}$, so daß für alle $u_1, \ldots, u_n \in U_{\mathcal{A}}$ $F(u_1, \ldots, u_n)$ ein solches v ist. Die Existenz einer solchen Funktion ist durch das *Auswahlaxiom* gesichert.

   Wir definieren jetzt eine neue Struktur $\mathcal{A}'$, die eine Erweiterung von $\mathcal{A}$ ist derart, daß $\mathcal{A}'$ überall mit $\mathcal{A}$ identisch ist und das zusätzliche Funktionszeichen f in $\mathcal{A}'$ durch F interpretiert wird. Aufgrund der Wahl von F folgt, daß für alle $u_1, \ldots, u_n \in U_{\mathcal{A}'}$ β bezüglich $s[y_1 \leftarrow u_1] \ldots [y_n \leftarrow u_n][z \leftarrow F(u_1, \ldots, u_n)]$ in $\mathcal{A}'$ gilt. Mit dem Substituitionslemma erhalten wir hieraus, daß für alle $u_1, \ldots, u_n \in U_{\mathcal{A}'}$ $\beta[z/f(y_1, \ldots, y_n)]$ bezüglich $s[y_1 \leftarrow u_1] \ldots [y_n \leftarrow u_n]$ in $\mathcal{A}'$ gilt, und also, daß α' bezüglich s in $\mathcal{A}'$ gilt.

■

Korollar 2.4.11 Jede Formel in BPF ist genau dann erfüllbar, wenn ihre Skolemform erfüllbar ist.

Beachte, daß die Umformung in Skolemform keine Äquivalenzumformung in dem Sinne ist, daß die entstehende Formel äquivalent zur Ausgangsformel ist. Es liegt lediglich *Erfüllbarkeitsäquivalenz* vor: Die entstehende Formel besitzt genau dann ein Modell, wenn die Ausgangsformel ein Modell besitzt. Dies ist nicht unbedingt eine Einschränkung. Ziel der Logik ist es u.a. , eine übersicht über die allgemeingültigen Aussagen zu ermöglichen. Die überführung in Normalformen ist ein gutes Mittel hierzu. Nun ist ja eine Aussage α genau dann allgemeingültig, wenn $\neg\alpha$ unerfüllbar ist. Daher können auch erfüllbarkeitserhaltende Umformungen zur Erreichung des genannten Zieles eingesetzt werden.

2.5 Übungsaufgaben

1. Geben Sie eine induktive Definition von *substituierbar*.
2. Sei $\mathcal{L}$ eine Sprache, die mindestens eine Konstante c, ein ein-stelliges Funktionssymbol f und zwei 2-stellige Funktionssymbole g, k enthält. Sei $\mathcal{A} = (\mathbb{N}, \mathcal{I})$, so daß $\mathcal{I}(c) = 0$, $\mathcal{I}(f) = S$, $\mathcal{I}(g) = +$ und $\mathcal{I}(k) = \cdot$ (wobei S die Nachfolgerfunktion und $+$ und $\cdot$ die Addition bzw. die Multiplikation ist).
   (a) Geben Sie zwei Terme t ohne Variablen an, so daß $\widehat{\mathcal{I}}[s](t) = 5$ für jede Belegung s.
   (b) Geben Sie für jede natürliche Zahl n einen Term $\underline{n}$ an, so daß $\widehat{\mathcal{I}}[s](\underline{n}) = n$ für jede Belegung s.
3. Für geschlossene Formeln φ haben wir entweder $\mathcal{A} \models \varphi$ oder $\mathcal{A} \models \neg\varphi$. Geben Sie ein Beispiel an, daß zeigt, daß dies für nicht geschlossene Formeln nicht der Fall ist.
4. Zeigen Sie, daß

   $$\models \exists x\ (\alpha \to \forall y\ \alpha[x/y])\ .$$

   (Dies ist die sogenannte Trinkerformel, die uns auch in den nächsten Übungsaufgaben begegnen wird).

3 — Herleitungen

3.1 Einleitung

Ziel dieses Kapitels ist es, den Begriff der logischen Folgerung syntaktisch zu charakterisieren. Hierzu werden wir die Vorgehensweise beim Führen von Beweisen formalisieren und zeigen, daß eine Formel genau dann logische Folgerung aus einer gegebenen Formelmenge ist, wenn sie aus dieser Formelmenge herleitbar ist. Dieses Resultat ist keineswegs offensichtlich. Gibt uns doch der Beweis einer Aussage i.a. mehr Information als das bloße Wissen, daß sie wahr ist. Wir wollen dies an einem Beispiel verdeutlichen.

Seien in der Sprache der Arithmetik $\dot{2}$ und $\dot{4}$ Bezeichnungen für die Terme $\dot{s}(\dot{s}(\dot{0}))$ und $\dot{s}(\dot{s}(\dot{s}(\dot{s}(\dot{0}))))$. Dann ist die Aussage $\dot{2}\dot{+}\dot{2}\doteq\dot{4}$ logische Folgerung aus den Aussagen

(1) $\forall x\ x\dot{+}\dot{0} = x$

(2) $\forall x \forall y\ x\dot{+}\dot{s}(y)\doteq\dot{s}(x\dot{+}y)$

Insbesondere hat die obige Aussage über dem Standardmodell der Arithmetik als Bedeutung den Wert **w**. Der Grund hierfür ist, daß die beiden Terme $\dot{2}\dot{+}\dot{2}$ und $\dot{4}$ diegleiche natürliche Zahl bezeichnen, nämlich 4. Wie die Entwicklung der Logik, insbesondere der Modelltheorie, gezeigt hat, ist diese Information in vielen Fällen ausreichend. Aber die Vorgehensweise, insbesondere die Interpretation des Funktionszeichens $\dot{+}$ durch die Additionsfunktion, d.h. eine Menge von Paaren natürlicher Zahlen, übersieht, daß die Aussagen (1) und (2) eine algorithmische Vorschrift zur „Berechnung“ von $\dot{2}\dot{+}\dot{2}$ enthalten. Sie wird bei der Herleitung der obigen Aussage aus (1) und (2) benutzt:

$$\begin{array}{lll} \dot{2}\dot{+}\dot{2} & \doteq & \dot{s}(\dot{s}(\dot{0}))\dot{+}\dot{s}(\dot{s}(\dot{0})) \\ & \doteq & \dot{s}(\dot{s}(\dot{s}(\dot{0}))) + \dot{s}(\dot{0})) \quad (2) \\ & \doteq & \dot{s}(\dot{s}(\dot{s}(\dot{s}(0)) + \dot{0})) \quad (2) \\ & \doteq & \dot{s}(\dot{s}(\dot{s}(\dot{s}(0)))) \quad (1) \\ & \doteq & \dot{4}. \end{array}$$

Frege nennt diesen algorithmische Aspekt des Terms $\dot{2}\dot{+}\dot{2}$ seinen *Sinn* [Frege 1892]. Die beiden Terme $\dot{2}\dot{+}\dot{2}$ und $\dot{4}$ haben zwar die gleiche Bedeutung, aber unterschiedlichen Sinn. Allgemein sind der Sinn eines Namens die Angaben, die Informationen, die im Namen über das Denotat, d.i. seine Bedeutung, enthalten sind. Für die Mathematik war

bisher — vor allem seit der Entwicklung der Mengenlehre — fast nur die Bedeutung von formalen Ausdrücken interessant und nicht der Sinn. So ist es i.a. unwichtig, durch welche Zuordnungsvorschrift eine Funktion gegebenen ist, sondern möchten nur ihre Extension, d.i. die Menge der Argument-Wert-Paare, kennen. In der Informatik ist dies anders: Verschiedene Zuordnungsvorschriften sind verschiedene Algorithmen mit unterschiedlichen Komplexitäten.

3.2 Natürliches Schließen

Wir benutzen die Notation

$$\begin{array}{c}\vdots\\ \alpha\end{array}$$

zur Bezeichnung einer Herleitung von α. Eine solche Herleitung kann als endlicher Baum aufgeschrieben werden, dessen Knoten mit Formeln markiert sind. Die Wurzel hat die Markierung α. Die Markierungen der Blätter sind entweder *gebunden* oder *frei*.

Im allgemeinen sind die Formeln an den Blättern frei, d.h. sie sind wesentlicher Teil des Beweises. Sie heißen in diesem Fall *Annahme*. Ein einfacher Beweis ist durch die Regel gegeben, die uns die Bildung von Herleitungen erlaubt, die nur aus einer Formel bestehen:

$$\alpha$$

Hier ist α sowohl Blatt wie auch Wurzel: Wir leiten α aus der Annahme α her. Mithilfe von Regeln können aus Herleitungen weitere Herleitungen konstruiert werden. Haben wir zum Beispiel Herleitungen für die Formel α und $\alpha \to \beta$, so können wir hieraus mittels der Regel

$$\dfrac{\begin{array}{cc}\vdots & \vdots\\ \alpha & \alpha \to \beta\end{array}}{\beta}\ (\to \mathrm{E})$$

eine Herleitung für β bilden. Die Konstruktion von Herleitungen orientiert sich am Formelaufbau. Für fast alle logischen Verknüpfungen und die Quantoren gibt es eine *Introduktionsregel*, die uns die Konstruktion einer Herleitung für eine zusammengesetzte Formel aus Herleitungen der Teilformel erlaubt, und — sozusagen als Umkehrung dieser Regel — eine *Eliminationsregel*. Die obige Regel heißt $\to$*Elimination*. Die zugehörige Einführungsregel, die $\to$*Introduktion*, lautet wie folgt:

$$\dfrac{\begin{array}{c}[\alpha]\\ \vdots\\ \beta\end{array}}{\alpha \to \beta}\ (\to \mathrm{I})$$

Mit dieser Regel bilden wir aus einer Herleitung

$$\begin{array}{c}\alpha\\ \vdots\\ \beta\end{array}$$

in der α als Annahme auftritt, eine Herleitung von $\alpha \to \beta$, in der α *nicht mehr* als Annahme auftritt. In der Regel wird dies durch die Schreibweise $[\alpha]$ angedeutet. Wir sagen, daß das bzw. die Vorkommen von α in der Herleitung *gebunden* worden sind. Solange eine Formel α in einer Herleitung für eine Formel β als Annahme auftritt, können wir diese Herleitung zu einer Herleitung von β verlängern, in der α nicht mehr als Annahme auftritt, indem wir eine Herleitung von α einfügen:

$$\begin{array}{c} \vdots \\ \alpha \\ \vdots \\ \beta \end{array}$$

Bei einem gebundenem Vorkommen von α läßt sich diese Einsetzung nicht vornehmen. Wir geben nun die Regeln an:

- *Annahmeneinführung*: α (Ann)
- *Introduktionsregeln*:

$$\dfrac{\begin{array}{c}[\alpha] \\ \vdots \\ \beta\end{array}}{\alpha \to \beta}\,(\to \mathrm{I}) \qquad\qquad \dfrac{\begin{array}{c}\vdots \\ \alpha\end{array}}{\forall x \alpha}\,(\forall \mathrm{I})$$

  Die $\forall$–Introduktionsregel darf nur angewendet werden, wenn die Variable in keiner in der Herleitung von α freien Annahme frei vorkommt.

- *Eliminationsregeln*:

$$\dfrac{\begin{array}{c}\vdots \\ \alpha\end{array} \qquad \begin{array}{c}\vdots \\ \alpha \to \beta\end{array}}{\beta}\,(\to \mathrm{E}) \qquad\qquad \dfrac{\begin{array}{c}\vdots \\ \forall x \alpha\end{array}}{\alpha[x/t]}\,(\forall \mathrm{E})$$

  Die $\forall$–Eliminationsregel darf nur angewendet werden, wenn x in α durch t substituierbar ist.

Beispiel 3.2.1 Wir wollen nun schrittweise eine Herleitung der Aussage

$$\forall x(\alpha \to \beta) \to (\alpha \to \forall x \beta)$$

konstruieren, wobei wir annehmen, daß die Variable x in α nicht frei vorkommt.

1 *Schritt*:

$$\forall x(\alpha \to \beta)$$

2 *Schritt*:

$$\dfrac{\forall x(\alpha \to \beta)}{\alpha \to \beta}\,(\forall \mathrm{E})$$

3 *Schritt*:

$$\alpha$$

4 *Schritt*:

$$\dfrac{\alpha \qquad \dfrac{\forall x(\alpha \to \beta)}{\alpha \to \beta}\,(\forall \mathrm{E})}{\beta}\,(\to \mathrm{E})$$

5 *Schritt*:

$$\dfrac{\dfrac{\alpha \qquad \dfrac{\forall x(\alpha \to \beta)}{\alpha \to \beta}\,(\forall \mathrm{E})}{\beta}\,(\to \mathrm{E})}{\forall x\beta}\,(\forall \mathrm{I})$$

6 *Schritt*:

$$\dfrac{\dfrac{[\alpha] \qquad \dfrac{\forall x(\alpha \to \beta)}{\alpha \to \beta}\,(\forall \mathrm{E})}{\beta}\,(\to \mathrm{E})}{\forall x\beta}\,(\forall \mathrm{I})}{\alpha \to \forall x\beta}\,(\to \mathrm{I})$$

7 *Schritt*:

$$\dfrac{\dfrac{\dfrac{[\alpha] \qquad \dfrac{\forall x(\alpha \to \beta)}{\alpha \to \beta}\,(\forall \mathrm{E})}{\beta}\,(\to \mathrm{E})}{\forall x\beta}\,(\forall \mathrm{I})}{\alpha \to \forall x\beta}\,(\to \mathrm{I})}{\forall x(\alpha \to \beta) \to (\alpha \to \forall x\beta)}\,(\to \mathrm{I})$$

Es fällt auf, daß wir nur Introduktions– und Eliminationsregeln für $\to$ und $\forall$ angegeben. Nach Korollar 1.4.6 ist dies aber keine Einschränkung, zumal jede Formel der Art $\exists x\alpha$ äquivalent zu $\neg\forall x\neg\alpha$ ist. Wir betrachten eine Formel als herleitbar, wenn die äquivalente Formel eine Herleitung besitzt, die wir erhalten, indem wir $\vee$,$\wedge$,$\neg$,$\exists$ durch $\to$,$\bot$ und $\forall$ ausdrücken. Zur Erinnerung geben wir noch einmal die entsprechenden Äquivalenzen an:

$$\begin{array}{lll}
\neg\alpha & \equiv \alpha \to \bot & \\
\alpha \vee \beta & \equiv \neg\alpha \to \neg\neg\beta & \equiv (\alpha \to \bot) \to ((\beta \to \bot) \to \bot) \\
\alpha \wedge \beta & \equiv \neg(\alpha \to \neg\beta) & \equiv (\alpha \to (\beta \to \bot)) \to \bot \\
\alpha \leftrightarrow \beta & \equiv \neg((\alpha \to \beta) \to \neg(\beta \to \alpha)) & \equiv ((\alpha \to \beta) \to ((\beta \to \alpha) \to \bot)) \to \bot \\
\exists x\alpha & \equiv \neg\forall x\neg\alpha & \equiv (\forall x(\alpha \to \bot)) \to \bot
\end{array}$$

Die Logik mit dem obigen Regelsystem heißt *Minimallogik*. In ihr ist $\bot$ ein Symbol wie jedes andere. Eine der wichtigsten Forderungen an eine Schlußregel ist, daß sie die Gültigkeit der beteiligten Formeln erhält. Nach Lemma 2.3.14 haben die obigen Regeln diese Eigenschaft, und zwar unabhängig davon, welchen Wahrheitswert wir $\bot$ geben. Wir wollen aber, daß $\bot$ als Kontradiktion zu interpretieren ist. Dies erreichen wir, indem wir fordern, daß für atomare Formeln α die Formel $\neg\neg\alpha \to \alpha$ herleitbar ist (womit die Aussage auch für allgemeine Formeln bewiesen werden kann). Beachte hierzu, daß die Formel $((\alpha \to \beta) \to \beta) \to \alpha$ genau dann allgemeingültig ist, wenn β

eine Kontradiktion ist, d.h. in keinem Modell gilt. Die Formel $\neg\neg\alpha \to \alpha$ entspricht dem Vorgehen beim *Indirekten Beweis*: Führt die Annahme $\neg\alpha$ zu einem Widerspruch, so haben wir α bewiesen.

Allerdings können wir die Formel $\neg\neg\alpha \to \alpha$ *nicht* in der Minimallogik beweisen. Wir müssen also noch mehr Regeln zu unserem Herleitungsbegriff hinzufügen

IBA *Indirekter Beweis für atomare Formeln.* Für jede atomare Formel α außer $\bot$ ist

$$\neg\neg\alpha \to \alpha$$

eine Herleitung *ohne freie Annahmen.*

Ist $\mathcal{L}$ eine Sprache mit Identität, so gilt ferner:

Id *Identitätsaxiom.* Für jede Variable x der Sprache $\mathcal{L}$ ist

eine Herleitung *ohne freie Annahmen.* $x \doteq x$

GF *Gleichheitsaxiom für Funktionszeichen.*

Für jedes Funktionszeichen der Sprache $\mathcal{L}$ der Stelligkeit $n > 0$, alle Variablen y, z und alle i mit $1 \leq i \leq n$ ist

$$y \doteq z \to f(x_1, \ldots, x_n)[x_i/y] \doteq f(x_1, \ldots, x_n)[x_i/z]$$

eine Herleitung *ohne freie Annahmen.*

GR *Gleichheitsaxiom für Relationszeichen.* Für jedes Relationszeichen der Sprache $\mathcal{L}$ der Stelligkeit $n > 0$, alle Variablen y, z und jedes i mit $1 \leq i \leq n$ ist

$$y \doteq z \to (R(x_1, \ldots, x_n)[x_i/y] \to R(x_1, \ldots, x_n)[x_i/z])$$

eine Herleitung *ohne freie Annahmen.*

Sei $\hat{\alpha}$ die Formel, welche wir aus α erhalten, wenn die Verknüpfungen $\neg, \vee, \wedge$ und $\leftrightarrow$ und den Quantor $\exists$ durch $\to$, $\bot$ und $\forall$ ausdrückt. Sei ferner Γ eine Formelmenge. Dann sagen wir:

Definition 3.2.2 Bezeichne $\mathrm{FA}(\xi)$ die Menge der freien Annahmen einer Herleitung ξ. Eine Formel α ist *herleitbar* aus Γ und schreiben: $\Gamma \vdash \alpha$, wenn es eine Herleitung ξ von $\hat{\alpha}$ mit $\mathrm{FA}(\xi) \subseteq \Gamma$ gibt. Ist $\hat{\alpha}$ aus $\emptyset$ herleitbar, so nennen wir α *herleitbar* und schreiben: $\vdash \alpha$.

Lemma 3.2.3 Die folgenden Formeln sind herleitbar (sogar in Minimallogik):

1. $(\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$ (*Kettenschluß*),
2. $\alpha \to (\beta \to \alpha)$,
3. $\alpha \to \neg\neg\alpha$,
4. $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$ (*Kontraposition*),
5. $\alpha \vee \neg\alpha$ („*tertium non datur*“),

6. $(\alpha \to \beta) \to \neg\alpha \vee \beta$,
7. $\alpha \vee \beta \to \beta \vee \alpha$,
8. $\alpha \wedge \beta \to \beta \wedge \alpha$,
9. $\forall x\alpha \to \forall y\alpha[x/y]$, falls die Variable y in α nicht vorkommt.

Beweis. Um eine Herleitung von (1) zu konstruieren, ist es zweckmäßig, erst einmal einen informalen Beweis zu finden. Dies ist in diesem Fall sehr einfach. Wir wollen eine Implikation beweisen. Also nehmen wir zunächst einmal an, daß die Prämissen $\alpha \to \beta$, $\beta \to \gamma$ und α gültig sind. Zu zeigen ist γ. Aus den Annahmen α und $\alpha \to \beta$ erhalten wir β und hieraus mit $\beta \to \gamma$ schließlich γ, was zu zeigen war.

Aus diesem informalen Beweis wollen wir jetzt eine Herleitung gewinnen. Es ist

$$\dfrac{\dfrac{\dfrac{\dfrac{[\alpha] \quad [\alpha \to \beta]}{\beta} \quad [\beta \to \gamma]}{\gamma}}{\alpha \to \gamma}}{(\beta \to \gamma) \to (\alpha \to \gamma)}}{(\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))}$$

die gesuchte Herleitung von (1). (2) folgt ähnlich wie (1), ebenso (3) und (4). (5) ist ein Spezialfall von (3). Wir geben nur die Herleitungen an:

(2)

$$\dfrac{\dfrac{\dfrac{[\alpha]}{[\beta]}}{\beta \to \alpha}}{\alpha \to (\beta \to \alpha)}$$

(3)

$$\dfrac{\dfrac{\dfrac{[\alpha] \quad [\alpha \to \bot]}{\bot}}{(\alpha \to \bot) \to \bot}}{\alpha \to ((\alpha \to \bot) \to \bot)}$$

(4) ist ein Spezialfall von (1) mit $\gamma \equiv \bot$

(5) ist ein Spezialfall von (3) (angewandt auf die Formel $\neg\alpha$)

Im Fall (6) haben wir eine Herleitung von $(\alpha \to \beta) \to (\neg\neg\alpha \to \neg\neg\beta)$ zu finden. Nehmen wir also an, daß $\alpha \to \beta$ gültig ist. Mit zweimaliger Anwendung der Kontraposition erhalten wir, daß auch $\neg\neg\alpha \to \neg\neg\beta$. Seien daher ξ und ζ Herleitungen von $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$ und $(\neg\beta \to \neg\alpha) \to (\neg\neg\alpha \to \neg\neg\beta)$. Dann ist

$$\dfrac{\dfrac{\dfrac{[\alpha \to \beta] \quad \overset{\vdots\ \xi}{(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)}}{\neg\beta \to \neg\alpha} \quad \overset{\vdots\ \zeta}{(\neg\beta \to \neg\alpha) \to (\neg\neg\alpha \to \neg\neg\beta)}}{\neg\neg\alpha \to \neg\neg\beta}}{(\alpha \to \beta) \to (\neg\neg\alpha \to \neg\neg\beta)}$$

eine Herleitung von (6).
(7): Gesucht ist eine Herleitung von der (übersetzten) Formel $(\neg\alpha \to \neg\neg\beta) \to (\neg\beta \to \neg\neg\alpha)$. Wir nehmen hierzu an, daß $\neg\alpha \to \neg\neg\beta$ und $\neg\beta$ gültig sind. Zu zeigen ist dann $\neg\neg\alpha$. Nehmen wir daher weiter an, daß $\neg\alpha$ gilt. Mit der ersten Annahme folgt dann $\neg\neg\beta$, ein Widerspruch zur anderen Annahme, daß $\neg\beta$ gilt. Jetzt können wir die gesuchte Herleitung leicht angeben:

$$\dfrac{\dfrac{\dfrac{[\neg\beta] \qquad \dfrac{[\neg\alpha \to \neg\neg\beta] \qquad [\neg\alpha]}{\neg\neg\beta}}{\bot}}{\neg\neg\alpha}}{\neg\beta \to \neg\neg\alpha}}{(\neg\alpha \to \neg\neg\beta) \to (\neg\beta \to \neg\neg\alpha)}$$

ist eine Herleitung von (7).
(8): Wir haben eine Herleitung von $\neg(\alpha \to \neg\beta) \to \neg(\beta \to \neg\alpha)$ anzugeben. Offensichtlich ist

$$\dfrac{\dfrac{\dfrac{[\alpha] \qquad \dfrac{[\beta \to \neg\alpha] \qquad [\beta]}{\neg\alpha}}{\bot}}{\neg\beta}}{\alpha \to \neg\beta}}{(\beta \to \neg\alpha) \to (\alpha \to \neg\beta)}$$

eine Herleitung von $(\beta \to \neg\alpha) \to (\alpha \to \neg\beta)$. Sie werde mit ξ bezeichnet. Mittels Kontraposition folgt hieraus die herzuleitende Formel. Sei also τ eine Herleitung von $((\beta \to \neg\alpha) \to (\alpha \to \neg\beta)) \to (\neg(\alpha \to \neg\beta) \to \neg(\beta \to \neg\alpha))$. Dann ist

$$\dfrac{\xi \qquad \tau}{\neg(\alpha \to \neg\beta) \to \neg(\beta \to \neg\alpha)}$$

die gesuchte Herleitung.
(9): Wir nehmen an, daß $\forall x\alpha$ gültig ist. Zu zeigen ist $\forall y\alpha[x/y]$. Sei also y beliebig, aber fest gewählt. Spezialisieren wir jetzt unsere Annahme für dieses y, so erhalten wir $\alpha[x/y]$ und damit auch $\forall y\alpha[x/y]$, denn die Variable y kommt in $\forall x\alpha$ nicht frei vor. Nun ist es wieder einfach eine Herleitung von (9) anzugeben:

$$\dfrac{\dfrac{\dfrac{[\forall x\alpha]}{\alpha[x/y]}}{\forall y\alpha[x/y]}}{\forall x\alpha \to \forall y\alpha[x/y]}$$

ist eine solche. ■

In der Definition von „Herleitung“ haben wir festgelegt, daß für von $\bot$ verschiedene atomare Formeln α die Formeln $\neg\neg\alpha \to \alpha$ als Axiome benutzt werden können. Diese Axiome heißen auch *Stabilitätsaxiome*. Wir zeigen nun:

Lemma 3.2.4 Für jede Formel α ist $\vdash \neg\neg\alpha \to \alpha$.

Beweis. Wir führen den Beweis durch Induktion über den Formelaufbau, wobei wir nur die logische Verknüpfung $\to$ und den Allquantor zu berücksichtigen haben. Ist α atomar, so ist $\neg\neg\alpha \to \alpha$, wie wir gerade gesehen haben, ein Axiom, falls $\alpha \neq \bot$. Im Fall $\alpha = \bot$ ist aus $(\bot \to \bot) \to \bot$ die Formel $\bot$ herzuleiten. Die Prämisse $\bot \to \bot$ der Annahme $(\bot \to \bot) \to \bot$ ist aber leicht herzuleiten, d.h. wir haben $\bot$. Jetzt läßt sich die gesuchte Herleitung einfach angeben:

$$\dfrac{\dfrac{\dfrac{[\bot]}{\bot \to \bot} \qquad [\neg\neg\bot]}{\bot}}{(\neg\neg\bot) \to \bot}$$

ist eine Herleitung der Formel $\neg\neg\bot \to \bot$.

Ist α von der Form $\beta \to \gamma$, so ist γ aus $\neg\neg(\beta \to \gamma)$ und β herzuleiten. Nach Induktionsvoraussetzung gilt $\neg\neg\gamma \to \gamma$. Nehmen wir nun an, daß $\neg\gamma$. Dann ist auch $\neg(\beta \to \gamma)$. Denn aus der Annahme, daß $\beta \to \gamma$, erhalten wir mit β γ und damit einen Widerspruch zu $\neg\gamma$. Die Folgerung, daß $\neg(\beta \to \gamma)$ widerspricht aber der Voraussetzung, daß $\neg\neg(\beta \to \gamma)$. Also ist $\neg\neg\gamma$, woraus mit der Induktionsvoraussetzung γ folgt. Die gesuchte Herleitung erhalten wir nun wie folgt: Sei ξ eine nach Induktionsvoraussetzung bekannte Herleitung der Formel $\neg\neg\gamma \to \gamma$. Dann ist

$$\dfrac{\dfrac{[\neg\neg(\beta \to \gamma)] \qquad \dfrac{\dfrac{\dfrac{[\beta] \qquad [\beta \to \gamma]}{\gamma} \qquad [\neg\gamma]}{\bot}}{\neg(\beta \to \gamma)}}{\bot} \qquad \xi}{\gamma}}{\beta \to \gamma}$$
$$\neg\neg(\beta \to \gamma) \to (\beta \to \gamma)$$

eine Herleitung der Formel $\neg\neg(\beta \to \gamma) \to (\beta \to \gamma)$.

Ist α von der Form $\forall x\beta$, so ist α aus $\neg\neg\forall x\beta$ herzuleiten. Nach Induktionsvoraussetung gilt $\neg\neg\beta \to \beta$. Da x in $\forall x\beta$ nicht frei vorkommt, genügt es also $\neg\neg\beta$ herzuleiten. Gelte daher noch $\neg\beta$. Nehmen wir jetzt weiter $\forall x\beta$ an, so folgt β und wegen $\neg\beta$ ein Widerspruch. Also $\neg\forall x\beta$, im Widerspruch wiederum zu der Annahme $\neg\neg\forall x\beta$. Somit führt die Annahme $\neg\beta$ auf einen Widerspruch, d.h. , wir haben wie gewünscht $\neg\neg\beta$. Nun läßt sich die gesuchte Herleitung leicht angeben. Sei ξ eine nach Induktionsvoraussetzung bekannte Herleitung der Formel $\neg\neg\beta \to \beta$. Dann ist

$$\dfrac{\dfrac{\dfrac{[\neg\neg\forall x\beta] \qquad \dfrac{\dfrac{\dfrac{[\neg\beta] \qquad \dfrac{[\forall x\beta]}{\beta}}{\bot}}{\neg\forall x\beta}}{\bot} \qquad \xi}{\beta}}{\forall x\beta}}{\neg\neg\forall x\beta \to \forall x\beta}$$

eine Herleitung der Formel $\neg\neg\forall x\beta \to \forall x\beta$. ■

Definition 3.2.5 Ist ξ eine Herleitung von $\alpha \to \beta$ und τ eine Herleitung von α, so wollen wir mit $(\xi\tau)$ die Herleitung

$$\dfrac{\xi \qquad \tau}{\beta}$$

von β bezeichnen.

Korollar 3.2.6 Die folgenden Formeln sind herleitbar:

1. $\bot \to \alpha$ („*ex falso quod libet*“),
2. $\beta \wedge \neg\beta \to \alpha$,
3. $(\alpha \to (\neg\beta \to \gamma)) \to (\neg(\alpha \to \beta) \to \gamma)$,

Beweis. (1) Sei α eine beliebige Formel. Wir haben zu zeigen, daß $\bot \to \alpha$ herleitbar ist. Nach Lemma 3.2.3(1) und (2) und obigem Satz gibt es Herleitungen τ, ζ und ξ der Formeln $(\bot \to \neg\neg\alpha) \to ((\neg\neg\alpha \to \alpha) \to (\bot \to \alpha))$, $\bot \to ((\alpha \to \bot) \to \bot)$ und $\neg\neg\alpha \to \alpha$. Dann ist $(\xi\tau)\zeta$ eine Herleitung der Fomel $\bot \to \alpha$.

(2) Nach Lemma 3.2.3(3) gibt es Herleitungen ξ und ζ von $\beta \to \neg\neg\beta$ und $(\beta \to \neg\neg\beta) \to \neg\neg(\beta \to \neg\neg\beta)$. Dann ist es leicht ζ und ξ zu einer Herleitung von $\neg\neg(\beta \to \neg\neg\beta) \equiv (\beta \wedge \neg\beta) \to \bot$ zu kombinieren. Sei weiter τ eine Herleitung von $\bot \to \alpha$ und η eine nach Lemma 3.2.3(1) existierende Herleitung von $((\beta \wedge \neg\beta) \to \bot) \to ((\bot \to \alpha) \to ((\beta \wedge \neg\beta) \to \alpha))$. Dann ist $((\eta(\zeta\xi))\tau)$ die gesuchte Herleitung.

(3) Wir haben zu zeigen, daß γ aus $\neg(\alpha \to \beta)$ und $\alpha \to (\neg\beta \to \gamma)$ herleitbar ist. Dazu nehmen wir an, daß $\alpha \to (\neg\beta \to \gamma)$ und $\neg(\alpha \to \beta)$ gültig sind. Ferner nehmen wir an, daß $\neg\gamma$ gilt. Wir wollen zeigen, daß dann β aus α folgt. Gelte daher α und $\neg\beta$. Dann gilt nach unserer ersten Annahme, daß γ. Also war die Annahme, daß $\neg\beta$ falsch, d.h. ,wir haben β. Also haben wir $\alpha \to \beta$ gezeigt. Dies widerspricht unserer Eingangsannahme, woraus folgt, daß auch die Annahme $\neg\gamma$ falsch war. Wir erhalten somit γ, was zu zeigen war. Seien nun ξ und τ Herleitungen der Formeln $\neg\neg\beta \to \beta$ und $\neg\neg\gamma \to \gamma$. Dann ist

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\alpha \to (\neg\beta \to \gamma)] \qquad [\alpha]}{\neg\beta \to \gamma} \qquad [\neg\beta]}{\gamma} \qquad [\neg\gamma]}{\dfrac{\bot}{\neg\neg\beta}} \qquad \xi}{\beta}}{\alpha \to \beta} \qquad [\neg(\alpha \to \beta)]}{\dfrac{\dfrac{\bot}{\neg\neg\gamma} \qquad \tau}{\gamma}}}{\neg(\alpha \to \beta) \to \gamma}}{(\alpha \to (\neg\beta \to \gamma)) \to (\neg(\alpha \to \beta) \to \gamma)}$$

eine Herleitung der Formel $(\alpha \to (\neg\beta \to \gamma)) \to (\neg(\alpha \to \beta) \to \gamma)$. ■

Wir haben uns bei der Definition des Herleitungsbegriffs bemüht, mit möglichst wenig Schlußregeln auszukommen. Wegen der gewählten Regeln haben die in Herleitungen vorkommenden Formeln i.w. die Gestalt $\alpha_1 \to (\alpha_2 \to \ldots (\alpha_m \to \beta)\ldots)$. Zur Abkürzung schreiben wir hier auch $\alpha_1, \ldots, \alpha_m \to \beta$, wobei wir endliche Folgen $\alpha_1, \ldots, \alpha_m$ von Formeln manchmal auch mit $\vec{\alpha}$ bezeichnen. Für Formeln dieser Art gelten nun einige nützliche Eigenschaften.

Lemma 3.2.7 Die folgenden Formeln sind herleitbar:

1. $(\vec{\alpha} \to \beta) \to (\vec{\alpha}, \alpha \to \beta)$ (*Abschwächung*),
2. $(\vec{\alpha}, \alpha, \alpha \to \beta) \to (\vec{\alpha}, \alpha \to \beta)$ (*Kontraktion*),
3. $(\vec{\alpha}, \alpha, \vec{\beta}, \beta, \vec{\gamma} \to \delta) \to (\vec{\alpha}, \beta, \vec{\beta}, \alpha, \vec{\gamma} \to \delta)$ (*Vertauschung*).

Der Nachweis ihrer Herleitbarkeit ist sehr einfach und wird hier übergangen.

Korollar 3.2.8 Die folgenden Formeln sind herleitbar:

1. $x_2 \doteq x_1 \to x_1 \doteq x_2$,
2. $x_1 \doteq x_2 \to (x_2 \doteq x_3 \to x_1 \doteq x_3)$.

Beweis. (1) Wegen des Gleichheitsaxioms für Relationszeichen ist die Formel $x_2 \doteq x_1 \to (x_1 \doteq x_2[x_1/x_2] \to x_1 \doteq x_2[x_1/x_1])$ herleitbar. Mit Vertauschung erhalten wir hieraus, daß auch $x_2 \doteq x_2 \to (x_2 \doteq x_1 \to x_1 \doteq x_2)$ herleitbar ist, woraus aufgrund des Identitätsaxioms die Herleitung von (1) folgt. Ähnlich erhalten wir auch die Herleitbarkeit von (2). ■

Ausgehend von den gewählten Introduktions– und Eliminationsregeln lassen sich auch für die übrigen logischen Vernüpfungen und den Existenzquantor derartige Regeln herleiten.

Lemma 3.2.9 Es gilt:

- $\neg$*–Introduktion:*

$$\frac{\Gamma, \alpha \vdash \bot}{\Gamma \vdash \neg\alpha}\ (\neg\mathrm{I})$$

  $\neg$*–Elimination:*

$$\frac{\Gamma \vdash \alpha}{\Gamma, \neg\alpha \vdash \bot}(\neg\mathrm{E})$$

- $\vee$*–Introduktion:*

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta}(\vee 1\mathrm{I}),$$

$$\frac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta}(\vee 2\mathrm{I})$$

  $\vee$*–Elimination:*

$$\frac{\Gamma, \alpha \vdash \gamma \quad \Gamma, \beta \vdash \gamma}{\Gamma, \alpha \vee \beta \vdash \gamma}\ (\vee\mathrm{E})$$

- $\wedge$*–Introduktion:*

$$\frac{\Gamma \vdash \alpha \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta}\ (\wedge\mathrm{I})$$

  $\wedge$*–Elimination:*

$$\frac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \alpha}\ (\wedge 1\mathrm{E}), \qquad \frac{\Gamma \vdash \alpha \wedge \beta}{\Gamma \vdash \beta}\ (\wedge 2\mathrm{E})$$

- $\leftrightarrow$*–Introduktion:*

$$\frac{\Gamma, \alpha \vdash \beta \quad \Gamma, \beta \vdash \alpha}{\Gamma \vdash \alpha \leftrightarrow \beta} \ (\leftrightarrow \mathrm{I})$$

  $\leftrightarrow$*–Elimination:*

$$\frac{\Gamma \vdash \alpha \leftrightarrow \beta \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha} \ (\leftrightarrow 1\mathrm{E})$$

$$\frac{\Gamma \vdash \alpha \leftrightarrow \beta \quad \Gamma \vdash \alpha}{\Gamma \vdash \beta} \ (\leftrightarrow 2\mathrm{E})$$

- $\neg\neg$*–Elimination:*

$$\frac{\Gamma \vdash \neg\neg\alpha}{\Gamma \vdash \alpha} \ (\neg\neg\mathrm{E})$$

- $\exists$*–Introduktion:*

$$\frac{\Gamma \vdash \alpha[x/t]}{\Gamma \vdash \exists x \alpha} (\exists\mathrm{I}),$$

  falls die Variable x in α durch t substituierbar ist

- $\exists$*–Elimination:*

$$\frac{\Gamma \vdash \exists x \alpha \quad \Gamma, \alpha \vdash \beta}{\Gamma, \exists x \alpha \vdash \beta} \ (\exists\mathrm{E}),$$

  falls die Variable x weder in β noch in den Annahmen aus Γ frei vorkommt

Beweis. Der Beweis der $\neg$–Introduktion und –Elimination ist sehr einfach und soll hier übergangen werden. Die $\neg\neg$–Elimination folgt aus Lemma 3.2.4. Ebenso folgen $\leftrightarrow$–Introduktion und –Elimination aus den entsprechenden Regeln für $\wedge$ und $\rightarrow$. Wir beweisen nun die restlichen Regeln, wobei wir uns bei der $\vee$–Introduktion und der $\wedge$–Elimination wegen Lemma 3.2.3 auf den Nachweis einer der beiden Regeln beschränken können.
($\vee$1). Sei ξ eine Herleitung von α aus Γ. Dann ist

$$\dfrac{\dfrac{\dfrac{[\neg\alpha] \quad \xi}{\bot}}{\neg\neg\beta}[\neg\beta]}{\neg\alpha \rightarrow \neg\neg\beta}$$

eine Herleitung von $\neg\alpha \rightarrow \neg\neg\beta$, d.h. von $\alpha \vee \beta$ aus Γ.
($\vee$E). Seien ξ und ζ Herleitungen von γ aus Γ und α bzw. β. Sei ferner τ eine nach Lemma 3.2.4 existierende Herleitung von $\neg\neg\gamma \rightarrow \gamma$. Dann ist

$$\dfrac{\dfrac{\dfrac{\dfrac{[\neg\gamma] \quad [\beta]\zeta}{\bot}}{\neg\beta} \quad \dfrac{\dfrac{[\neg\gamma] \quad [\alpha]\xi}{\bot}}{\neg\alpha}}{\dfrac{\bot}{\neg\neg\gamma}} \quad \dfrac{[\neg\alpha \rightarrow \neg\neg\beta]}{\neg\neg\beta}}{\gamma} \quad \tau}{(\neg\alpha \rightarrow \neg\neg\beta) \rightarrow \gamma}$$

eine Herleitung von γ aus Γ und $\alpha \vee \beta$.
Die restlichen Regeln sind dem Leser als Übung überlassen. ■

Der in diesem Kapitel eingeführte Herleitungskalkül ist bis jetzt nur ein Kalkül zur Manipulation von Zeichenreihen. Ein solcher Kalkül ist im Rahmen der Logik nur dann sinnvoll, wenn mit ihm nur wahre, d.h. allgemeingültige Formeln herleitbar sind. Ein Herleitungskalkül mit dieser Eigenschaft heißt *korrekt*.

Satz 3.2.10 — Korrektheitssatz. Ist eine Formel α aus einer Formelmenge Γ herleitbar, so ist sie auch logische Folgerung von Γ.

Den Beweis dieses Satzes führen wir leicht durch Induktion über den Aufbau von Herleitungen, unter Benutzung von Lemma 2.3.14. In Zeichen gilt also

$$\Gamma \vdash \alpha \implies \Gamma \models \alpha \, .$$

Unser nächstes Ziel ist der Beweis der Umkehrung. Diese Eigenschaft eines Herleitungskalküls heißt seine *(semantische) Vollständigkeit*.

3.3 Vollständigkeit

Wir wollen jetzt den Gödelschen Vollständigkeitssatz beweisen. Er sagt aus, daß jede Formel α, die in allen Modellen $\mathcal{M}$ gültig ist, auch herleitbar ist. Zum Beweis verwenden wir ein Verfahren, das auf Beth, Hintikka und Schütte zurückgeht. Gegeben sei die Formel α. Wir suchen dann systematisch nach einem Gegenbeispiel zu α, also nach einem Modell $\mathcal{M}$ mit $\mathcal{M} \not\models \alpha$. Wenn diese Suche nicht zum Erfolg führt, so liefert uns das Protokoll der erfolglosen Suche eine Herleitung von α.

Genauer beweisen wir den Vollständigkeitssatz in der folgenden leicht verallgemeinerten Form. Gegeben sei eine Formel α sowie einer Formelmenge Γ, letztere in der Form einer eventuell abbrechenden Aufzählung $\alpha_0, \alpha_1, \ldots$ aller Formeln aus Γ. Wir nehmen an, daß α *aus* Γ *folgt*; also daß für jedes Modell $\mathcal{M}$ mit $\mathcal{M} \models \alpha_i$ für alle α_i in Γ gilt $\mathcal{M} \models \alpha$. Zu zeigen ist dann, daß α aus Annahmen in Γ herleitbar ist. In Zeichen wollen wir also zeigen, daß

$$\Gamma \models \alpha \implies \Gamma \vdash \alpha \ .$$

Zum Beweis gehen wir wie oben skizziert vor. Zu gegebenem α und Γ suchen wir systematisch nach einem Gegenbeispiel zu der Aussage, daß α aus Γ folgt, d.h. nach einem Modell $\mathcal{M}$ mit $\mathcal{M} \models \alpha_i$ für alle α_i in Γ, aber $\mathcal{M} \not\models \alpha$. Wenn diese Suche nicht zu einem Erfolg führt, liefert uns das Protokoll der erfolglosen Suche eine Herleitung von α aus Annahmen in Γ. Eine wichtige Eigenschaft der so gewonnenen Herleitung ist es, daß sie keine „*Umwege*“ macht im folgenden Sinn: Alle in ihr vorkommenden Formeln sind aussagenlogisch, also mit $\to$ und $\bot$ aus All– und Primformeln aufgebaut, welche Teilformeln von α oder von den α_i in Γ sind.

Für das folgende fest gegeben sei also eine Formel α sowie eine Formelmenge Γ, letzteres in der Form einer eventuell abbrechenden Aufzählung $\alpha_0, \alpha_1, \ldots$. Ohne Beschränkung der Allgemeinheit können wir annehmen, *daß* α *und* Γ *keine Variablen frei enthalten.* Wir geben uns ferner eine feste eventuell abbrechende Aufzählung $\delta_0, \delta_1, \ldots$ aller Teilformeln von α und von den α_i vor, *in der jede Allformel unendlich oft wiederholt wird.*

Definition 3.3.1 Definition des *Suchbaums* für ein Gegenbeispiel dazu, daß α aus Γ folgt. Der Suchbaum ist ein *endlich verzweigter Baum, dessen Knoten mit endlichen Listen von Formeln* beschriftet sind; diese Formeln sind eventuell negierte Teilformeln von α und den α_i. Die Wurzel wird mit der leeren Liste beschriftet. Angenommen, wir haben den Suchbaum bis zu einem Knoten k der Länge n bereits konstruiert, und es gibt noch ein δ_n. Sei S die Liste aller Formeln, die an Knoten auf dem Pfad bis einschließlich k als Elemente von Knotenbeschriftungen auftreten. Wir setzen die Konstruktion des Suchbaums wie folgt fort. Falls Γ die Formel $\bot$ oder eine Formel δ zusammen mit ihrer Negation $\neg\delta$, oder eine der Formeln $\alpha, \neg\alpha_1, \neg\alpha_2 \ldots$ enthält, so notieren wir am Knoten k „**Pfad geschlossen**“ und setzen an dieser Stelle die Konstruktion des Suchbaums nicht weiter fort. Anderenfalls unterscheiden wir entsprechend der Form von δ_n drei Fälle.

1. $\delta_n \equiv R\vec{t}$: k erhält zwei Nachfolgerknoten, die wir wie folgt beschriften:

   $$R\vec{t} \qquad \neg R\vec{t}$$

2. $\delta_n \equiv \beta \to \gamma$: k erhält drei Nachfolgerknoten, die wir wie folgt beschriften.

   $$(\beta \to \gamma), \neg\beta \qquad (\beta \to \gamma), \gamma \qquad \neg(\beta \to \gamma), \beta, \neg\gamma$$

3. $\delta_n \equiv \forall x\beta : k$ erhält zwei Nachfolgerknoten, die wir wie folgt beschriften.

   $$\forall x\beta, \beta[x/r] \qquad \neg\forall x\beta, \neg\beta[x/y]$$

   Hierbei ist r der erste Term, die auf dem Pfad bis zum Knoten k noch nicht zur Spezialisierung der Formel $\forall x\beta$ benutzt worden ist. y ist die erste Variable mit $y \notin \mathrm{FV}(S, \forall x\beta)$. Wir beziehen uns dabei auf eine fest vorgegebene Aufzählung aller Terme und Variablen.

Lemma 3.3.2 ($\Gamma \vdash \alpha$, **falls der Suchbaum geschlossen ist**). Jeder Knoten im Suchbaum habe eine Länge $\leq h$, und alle Blätter des Suchbaums seien mit „Pfad geschlossen“ beschriftet. Dann findet man eine Herleitung von α aus Annahmen in Γ mit folgender Eigenschaft: Alle in ihr vorkommenden Formeln sind aussagenlogisch aus All– und Primformeln aufgebaut, welche Teilformeln von α und den α_i in Γ sind.

Beweis. Zum Beweis konstruieren wir rekursiv für jeden Knoten k im Suchbaum eine Herleitung von $S \to \alpha$ aus Annahmen in S; S ist dabei wieder die Liste aller Fomeln, die an Knoten auf dem Pfad bis einschließlich k als Elemente von Knotenbeschriftungen auftreten. Falls in k der Pfad geschlossen wurde, ist die Behauptung offensichtlich. Anderenfalls unterscheiden wir wieder entsprechend der Form von δ_n drei Fälle.

Wir führen eine Induktion vom Blatt zur Wurzel. Der *Induktionsanfang* ist klar, da der Pfad geschlossen ist.

1. $\delta_n \equiv R\vec{t}$. Nach Induktionsvoraussetzung haben wir

   $$\Gamma \vdash S, R\vec{t} \to \alpha,$$
   $$\Gamma \vdash S, \neg R\vec{t} \to \alpha.$$

   Daraus folgt (Übung 4)

   $$\Gamma \vdash S \to \alpha.$$

2. $\delta_n \equiv \beta \to \gamma$. Nach Induktionsvoraussetzung haben wir

   $$\Gamma \vdash S, (\beta \to \gamma), \neg\beta \to \alpha\ ,$$
   $$\Gamma \vdash S, (\beta \to \gamma), \gamma \to \alpha\ .$$

   Daraus erhalten wir (Übung 4)

   $$\Gamma \vdash S, (\beta \to \gamma) \to \alpha\ .$$

   Ferner haben wir nach Induktionsvoraussetzung

   $$\Gamma \vdash S, \neg(\beta \to \gamma), \beta, \neg\gamma \to \alpha\ .$$

   Daraus erhalten wir insbesondere (Übung 4)

   $$\Gamma \vdash S, \neg(\beta \to \gamma) \to \alpha\ .$$

   Insgesamt haben wir also

   $$\Gamma \vdash S \to \alpha\ .$$

3. $\delta_n \equiv \forall x\beta$. Nach Induktionsvoraussetzung haben wir

$$\Gamma \vdash S, \forall x\beta, \beta[x/r] \to \alpha,$$
$$\Gamma \vdash S, \neg\forall x\beta, \neg\beta[x/y] \to \alpha$$

mit $\mathrm{FV}(S, \forall x\beta) \cap \{y\} = \emptyset$. Daraus folgt (wieder Übung 4)

$$\Gamma \vdash S, \forall x\beta \to \alpha,$$
$$\Gamma \vdash S, \neg\forall x\beta \to \alpha,$$

also auch

$$\Gamma \vdash S \to \alpha.$$ ■

Wir nehmen jetzt an, daß wir einen maximalen nicht-geschlossenen Pfad π im Suchbaum vorliegen haben[1]. Beachte, daß π genau dann endlich ist, wenn Γ und α keine Allformeln enthalten und Γ endlich ist. Mit $\mathcal{T}_\pi$ bezeichnen wir die Menge aller Formeln, die an irgendwelchen Knoten auf dem Pfad π als Elemenete von Knotenbeschriftungen auftreten. Aus $\mathcal{T}_\pi$ wollen wir uns jetzt ein Modell $\mathcal{M}_\pi$ konstruieren, welches ein Gegenbeispiel dafür bildet, daß α aus Γ folgt: Es soll also gelten $\mathcal{M}_\pi \models \Gamma$, aber $\mathcal{M}_\pi \not\models \alpha$. Da wir nichts anderes zur Verfügung haben, definieren wir uns die Trägermengen $\mathcal{U}_\pi$ des konstruierenden Modells aus syntaktischem Material. $\mathcal{U}_\pi$ bestehe aus allen Termen unseres vorgegebenen Termsystems. Beachte, daß jedes $\mathcal{U}_\pi$ deshalb abzählbar unendlich ist; dies wird uns später den Satz von Löwenheim-Skolem liefern.

Als letztes müssen wir noch eine Interpretation $\mathcal{I}_\pi$ angeben. Auf offensichtliche, aber eventuell verwirrende[2] Weise, bilden wir jede Konstante c auf sich selber ab. Jedes n-stellige Funktionssymbol f bilden wir ab auf die Funktion $\mathcal{I}_\pi(f)$, welche die Terme $t_1, \ldots, t_n$ auf den formalen Term $f(t_1, \ldots, t_n)$ abbildet.

Schließlich ist zur Vervollständigung unserer Definition des Modells von $\mathcal{M}_\pi$ für jedes Prädikatensymbol R der Stelligkeit n eine Teilmenge $\mathcal{I}_\pi(R)$ von $\mathcal{U}_\pi^n$ anzugeben: $R(t_1, \ldots, t_n)$ gelte genau dann, wenn die Formel $R(t_1 \ldots t_n)$ auf dem Pfad π vorkommt, d.h. wenn $R(t_1 \ldots t_n) \in T_\pi$.

Lemma 3.3.3 Sei π ein maximaler nicht geschlossener Pfad im Suchbaum. Dann gilt $\mathcal{M}_\pi \models \Gamma$, aber $\mathcal{M}_\pi \not\models \alpha$.

Beweis. Zum Beweis zeigen wir für jede *Teilformel* β von α und den α_i aus Γ

$$\mathcal{M}_\pi \models \beta \iff \beta \in T_\pi,$$

und zwar durch Induktion über die Anzahl der logischen Symbole von β. Daraus folgt die Behauptung, denn nach Konstruktion des Suchbaums ist $\Gamma \subseteq T_\pi$, aber $\alpha \notin T_\pi$. Entsprechend der Form von β unterscheiden wir drei Fälle.

1. $R\vec{t}$. Dann gilt die Äquivalenz nach Defintion von $\mathcal{M}_\pi$.

[1] Später werden wir uns überlegen, wie wir ein solches π definieren können, falls der Suchbaum nicht geschlossen ist.

[2] Man beachte, daß das unser syntaktisches Material jetzt auch auf der Modellseite auftaucht, was es schwer macht konzeptuell zwischen der syntaktischen und der semantischen Ebene zu unterscheiden.

2. $\beta \to \gamma$ „$\Rightarrow$“. Gelte $\mathcal{M}_\pi \models \beta \to \gamma$. Zu zeigen ist $\beta \to \gamma \in T_\pi$. Betrachte den zur Formel $\beta \to \gamma$ gehörigen Knoten l auf π. Falls unser Pfad π einen der ersten zwei Nachfolgerknoten von l enthält, ist nach Konstruktion des Suchbaumes $\beta \to \gamma \in T_\pi$ und wir sind fertig. Nehmen wir also jetzt an, daß rechte Nachfolgerknoten von l auf π liegt. Dann sind $\beta, \neg\gamma \in T_\pi$. Nach Induktionsvoraussetzung wissen wir also $\mathcal{M}_\pi \models \beta$. Wegen $\mathcal{M}_\pi \models \beta \to \gamma$ folgt $\mathcal{M}_\pi \models \gamma$, also wieder nach Induktionsvoraussetzung $\gamma \in T_\pi$. Mit $\neg\gamma \in T_\pi$ haben wir einen Widerspruch gegen die Voraussetzung, daß π nicht geschlossener Pfad ist. „$\Leftarrow$“ Gelte $\beta \to \gamma \in T_\pi$. Zu zeigen ist $\mathcal{M}_\pi \models \beta \to \gamma$. Nehmen wir also an, daß $\mathcal{M}_\pi \models \beta$. Nach Induktionsvoraussetzung folgt $\beta \in T_\pi$. Wir betrachten jetzt wieder den zu $\beta \to \gamma$ gehörigen Knoten auf π. Da π ein nicht geschlossener Pfad ist, kann nur der mittlere Nachfolgerknoten auf π liegen. Also ist $\gamma \in T_\pi$ und daher nach Induktionsvoraussetzung $\mathcal{M}_\pi \models \gamma$.

3. $\forall x\beta$. „$\Rightarrow$“ Gelte $\mathcal{M}_\pi \models \forall x\beta$. Zu zeigen ist $\forall x\beta \in T_\pi$. Betrachten wir den ersten zu $\forall x\beta$ gehörigen Knoten l auf π. Falls unser Pfad π den linken Nachfolgerknoten von l enthält, ist nach Konstruktion des Suchbaums $\forall x\beta \in T_\pi$ und wir sind fertig. Nehmen wir jetzt an, daß der rechte Nachfolgerknoten von l auf π liegt. Dann ist $\neg\beta[x/y] \in T_\pi$. Wegen $\mathcal{M}_\pi \models \forall x\beta$ gilt $\mathcal{M}_\pi \models \beta[x/y]$, also nach Induktionsvoraussetzung $\beta[x/y] \in T_\pi$. Mit $\neg\beta[x/y] \in T_\pi$ haben wir einen Widerspruch gegen die Voraussetzung, daß π nicht geschlossener Pfad ist. „$\Leftarrow$“ Gelte $\forall x\beta \in T_\pi$. Zu zeigen ist $\mathcal{M}_\pi \models \forall x\beta$. Sei s eine Belegung und $r = s(x)$. Zu zeigen ist dann $\mathcal{M}_\pi \models \beta[x/r]$. Wir betrachten jetzt den zu $\forall x\beta$ und dem Term r gehörigen Knoten l auf π. Da π ein nichtgeschlossener Pfad ist, muß der linke Nachfolgerknoten von l auf π liegen. Also $\beta[x/r] \in T_\pi$ und daher nach Induktionsvoraussetzung $\mathcal{M}_\pi \models \beta[x/r]$.

■

Als letzte Vorbereitung auf den Beweis des Vollständigkeitssatzes zeigen wir jetzt, daß im Fall eines unbeschränkten Suchbaums stets ein unendlicher (und damit maximaler) nicht-geschlossener Pfad definiert werden kann. Dies folgt mit dem bereits bekannten Lemma von König. Nochmal zur Erinnerung:

Lemma 3.3.4 — König. Jeder unbeschränkte endlich verzweigte Baum enthält einen unendlichen Pfad.

Jetzt können wir den folgenden Vollständigkeitssatz beweisen. $\alpha, \alpha_0, \alpha_1, \ldots$ seien abgeschlossene Formeln und $\Gamma = \{\alpha_0, \alpha_1, \ldots\}$.

Satz 3.3.5 — Gödel. Folgende Aussagen sind äquivalent

1. $\Gamma \models \alpha$
2. Es gibt eine Herleitung von α aus Annahmen in Γ mit folgender Eigenschaft: Alle in ihr vorkommenden Formeln sind aussagenlogisch aus All- und Primformlen aufgebaut, welche Teilformeln von α und den α_i sind.
3. $\Gamma \vdash \alpha$.

Beweis. $2 \Rightarrow 3$ ist trivial, und $3 \Rightarrow 1$ gilt nach dem Korrektheitssatz. Zum Beweis von $1 \Rightarrow 2$ haben wir zu zeigen, daß sich aus der Annahme, jede derartige Herleitung aus Annahmen in Γ habe eine von α verschiedene Endformel, ein Widerspruch ergibt. Wir machen also diese Annahme und betrachten den oben konstruierten Suchbaum für ein Gegenbeispiel dazu, daß α aus Γ folgt. Nach Lemma 3.3.3 kann der Suchbaum nicht geschlossen sein. Ist nun Γ endlich und sind α und Γ quantorenfrei, so ist nach

Konstruktion der Suchbaum beschränkt: seine Höhe ist die Anzahl der Teilformeln von α und den Formeln in Γ. Wir finden also einen nicht-geschlossenen maximalen Pfad π darin. Das oben aus π konstruierte Modell $\mathcal{M}_\pi$ hat nach Lemma 3.3.3 die Eigenschaft $\mathcal{M}_\pi \models S$ aber $\mathcal{M}_\pi \not\models \alpha$. Dies widerspricht unserer Voraussetzung, daß jedes Modell $\mathcal{M}$ von Γ auch Modell von α ist. Ist andererseits Γ unendlich oder α,Γ nicht quantorenfrei, so ist der Suchbaum unbeschränkt. Da er nach Konstruktion endlich verzweigt ist, können wir nach Lemma 3.3.4 einen unendlichen (also maximalen) nicht–geschlossenen Pfad π darin definieren. Wie eben erhalten wir daraus mit Lemma 3.3.3 einen Widerspruch zur Voraussetzung des Satzes. ■

Satz 3.3.6 — Löwenheim, Skolem. Besitzt eine Formelmenge Γ überhaupt ein Modell, so auch ein abzählbares.

Beweis. Wir spezialisieren die obigen Überlegungen auf den Fall $\alpha \equiv \bot$ und betrachten den Suchbaum für ein Gegenbeispiel dafür, daß $\bot$ aus Γ folgt; o.B.d.A. können wir Γ als abgeschlossen annehmen. Dieser Suchbaum kann nach Lemma 3.3.3 nicht geschlossen sein, da man sonst $\Gamma \vdash \bot$ hätte und damit wegen des Korrektheitssatzes einen Widerspruch zur Voraussetzung, daß Γ ein Modell besitzt. Wie eben beweisen wir mit Hilfe von Lemma 3.3.3, daß es dann einen maximalen nicht-geschlossenen Pfad π im Suchbaum gibt. Das durch π bestimmte Modell $\mathcal{M}_\pi$ ist nach Konstruktion abzählbar, und wegen Lemma 3.3.3 gilt $\mathcal{M}_\pi \models \Gamma$. ■

Satz 3.3.7 — Endlichkeitssatz. Ist $\Gamma \models \alpha$, so gibt es $\Gamma' \subseteq \Gamma$ mit Γ ist endlich und $\Gamma' \models \alpha$.

Beweis. Es gilt $\Gamma \models \alpha \Rightarrow_{\text{Vollständig}} \Gamma \vdash \alpha \Rightarrow$ex. Herleitung ξ von α mit $\mathrm{FA}(\xi) \subseteq \Gamma$. Sei Γ' die Menge der β mit $\beta \in \mathrm{FA}(\xi)$. Da eine Herleitung ein endlicher Pfad mit endlich vielen Formeln markierter Baum ist, ist Γ' endlich. Ferner $\Gamma' \vdash \alpha \Rightarrow_{Korr.Satz} \Gamma' \models \alpha$. ■

Satz 3.3.8 — Kompaktheitssatz von Gödel und Malcew. Besitzt jede endliche Teilmenge einer Formelmenge Γ ein Modell, so auch Γ selbst.

Beweis. Zum Beweis betrachten wir wieder den Suchbaum für ein Gegenbeispiel dafür, daß $\bot$ aus Γ folgt; oBdA können wir Γ als abgeschlossen annehmen. Der Suchbaum kann nicht geschlossen sein, denn dann hätten wir nach Lemma 3.3.3 eine Herleitung von $\bot$ aus endlichen vielen Formeln aus Γ im Widerspruch zu der Voraussetzung, daß jede endliche Teilmenge von Γ ein Modell besitzt. Es gibt also wieder einen maximalen nicht-geschlossenen Pfad π im Suchbaum, und für das durch π bestimmte Modell $\mathcal{M}_\pi$ haben wir $\mathcal{M}_\pi \models \alpha$. ■

Schließlich erhalten wir noch den ebenfalls wichtigen Satz von Herbrand.

Satz 3.3.9 — Herbrand. Gilt $\vdash \forall\vec{x}.\alpha \to \beta$ mit quantorenfreien Formeln α,β, so finden wir endlich viele Termlisten $\vec{r_1}, \ldots, \vec{r_m}$ und eine Herleitung von $\alpha_{\vec{x}}[\vec{r_1}], \ldots, \alpha_{\vec{x}}[\vec{r_m}] \to \beta$.

Beweis. Wir betrachten den aufgrund der Voraussetzung geschlossenen Suchbaum für ein Gegenbeispiel zu $\forall\vec{x}.\alpha \to \beta$; oBdA können wir $\forall\vec{x}.\alpha \to \beta$ als abgeschlossen annehmen. An jedem Knoten k, in dem $\forall\vec{x}.\alpha$ betrachtet wurde, streichen wir in dem mit $\forall\vec{x}.\alpha, \alpha_{\vec{x}}[\vec{r}]$ beschrifteten linken Nachfolgerknoten die Formel $\forall\vec{x}.\alpha$ und entfernen den mit $\neg\forall\vec{x}.\alpha, \neg\alpha_{\vec{x}}[\vec{y}]$ beschrifteten rechten Nachfolgerknoten sowie alle Fortsetzungen dieses Knotens. $\vec{r_1}, \ldots, \vec{r_m}$ seien alle Termtupel, die in dem Suchbaum zur Spezialisierung von $\forall\vec{x}.\alpha$ verwendet wurden. Wie im Beweis von Lemma 3.3.2 kann man jetzt rekursiv für jeden Knoten k in dem so modifizierten Suchbaum eine Herleitung von $\Gamma, \alpha_{\vec{x}}[\vec{r_1}], \ldots, \alpha_{\vec{x}}[\vec{r_m}] \to \beta$ konstruieren. Γ ist dabei wieder die Liste aller Formeln, die

an Knoten auf dem Pfad bis einschließlich k als Elemente von Knotenbeschriftungen auftreten. ■

3.4 Übungsaufgaben

1. Geben Sie eine Herleitung von

   $$\neg\neg(\alpha \to \beta) \to (\alpha \to \neg\neg\beta)$$

   in Minimallogik (d.h. vor Allem ohne Benutzung eines indirekten Beweis) an.

2. (a) Geben Sie eine Herleitung der Peirce'sche Formel

   $$((\alpha \to \beta) \to \alpha) \to \alpha$$

   an.

   (b) Geben Sie eine Herleitung der Trinker Formel an:

   $$\exists x\ (\alpha \to \forall y\ \alpha[x/y])\ .$$

   (Der Name kommt von der Interpretation „in jeder nichtleeren Bar gibt es eine Person, so daß, wenn diese Person betrunken ist jeder betrunken ist.“)

   Überraschenderweise sind beide Herleitungen etwas trickreich und benötigen indirekte Beweise.

3. Beweisen Sie die restlichen Fälle von Lemma 3.2.9.

4. (a) Zeigen Sie, daß $\Gamma \vdash \alpha \to \beta$ genau dann wenn $\Gamma, \alpha \vdash \beta$.

   (b) Zeigen Sie, daß wenn $\Gamma \vdash \beta \to \alpha$ und $\Gamma \vdash \neg\beta \to \alpha$ auch $\Gamma \vdash \alpha$. (Hinweis Kontraposition und indirekter Beweis[3] für α).

   (c) Zeigen Sie, daß wenn $\Gamma \vdash \beta, \gamma \to \alpha$ und $\Gamma \vdash \beta \to \gamma$ dann $\Gamma \vdash \beta \to \alpha$.

[3] Man kann hier sogar zeigen, daß es nicht ohne einen indirekten Beweis geht!

4 — Mathematische Theorien

4.1 Grundbegriffe

Ein Charakteristikum von Wissenschaft ist die Bildung von Theorien. Das sind Systeme von Aussagen, die aus gewissen Grundannahmen gefolgert oder experimentell bestätigt werden. Wir wollen in diesem Kapitel Eigenschaften mathematischer Theorien untersuchen.

Definition 4.1.1

1. Eine *Theorie erster Stufe* $\mathcal{T} = (\mathcal{L}, \Gamma)$ besteht aus einer Sprache erster Stufe $\mathcal{L}$ und einer Menge Γ von $\mathcal{L}$–Formeln derart, daß jede aus Γ herleitbare $\mathcal{L}$–Formel schon Element von Γ ist. Die Elemente von Γ heißen *Sätze* der Theorie.
2. $\mathcal{T}$ heißt *widerspruchsfrei*, wenn nicht jede $\mathcal{L}$–Formel Satz von $\mathcal{T}$ ist; anderenfalls *widerspruchsvoll*.
3. $\mathcal{T}$ heißt *vollständig*, wenn für alle $\mathcal{L}$–Aussagen α $\alpha \in \Gamma$ oder $\neg\alpha \in \Gamma$.

Beachte, daß die in Lemma 1.5.9 gegebenen Charakterisierungen der Widerspruchsfreiheit auch hier gelten. Es gibt zwei grundsätzlich verschiedene Arten, Theorien zu definieren. Bei der *modelltheoretischen* Methode geben wir eine Struktur $\mathcal{A}$ vor und nehmen als deren zugeordnete Theorie

$$\mathrm{Th}(\mathcal{A}) = (\mathcal{L}_{\mathcal{A}}, \{\, \alpha \mid \mathcal{A} \models \alpha \,\}) \ .$$

Lemma 4.1.2 Jede Theorie einer Struktur ist widerspruchsfrei und vollständig.

Beispiele solcher Theorien sind $\mathrm{Th}(\mathbb{N}, +)$ und $\mathrm{Th}(\mathbb{N}, +, *)$. Hierbei sind $\mathrm{Th}(\mathbb{N}, +)$ und $\mathrm{Th}(\mathbb{N}, +, *)$ die Strukturen mit Grundbereich $\mathbb{N}$ und fixierter Interpretation von $+$ als Additionsfunktion und $*$ als Multiplikationsfunktion. $\mathrm{Th}(\mathbb{N}, +)$ heißt *Presburger–Arithmetik* [Presburger] und $\mathrm{Th}(\mathbb{N}, +, *)$ *elementare Arithmetik*.

Bei der *axiomatischen* Methode geben wir ein *Axiomensystem*, also eine Menge Δ von Formeln einer Sprache $\mathcal{L}$, vor und definieren die zugehörige Theorie als $(\mathcal{L}, \mathrm{Cons}(\Delta))$, wobei

$$\mathrm{Cons}(\Delta) = \{\, \alpha \mid \Delta \vdash \alpha \,\} \ .$$

Statt von einem Modell des Axiomensystems sprechen wir in diesem Fall auch von einem Modell der Theorie.

Beispiel 4.1.3 Sei $\mathcal{L}_{\mathcal{A}}$ die Sprache der Arithmetik erster Stufe. Dann ist die *Peano–Arithmetik erster Stufe* die Theorie $\mathcal{S} = (\mathcal{L}_{\mathcal{A}}, \mathrm{Cons}(\{P1, \ldots, P7\}))$ mit

(P1) $\dot{0} \dot{\neq} \dot{s}(x_1)$

(P2) $\dot{s}(x_1) \doteq \dot{s}(x_2) \to x_1 \doteq x_2$

(P3) $x_1 \dot{+} \dot{0} \doteq x_1$

(P4) $x_1 \dot{+} \dot{s}(x_2) \doteq \dot{s}(x_1 \dot{+} x_2)$

(P5) $x_1 \dot{*} \dot{0} \doteq \dot{0}$

(P6) $x_1 \dot{*} \dot{s}(x_2) \doteq (x_1 \dot{*} x_2) \dot{+} x_1$

(P7) $\alpha[x/\dot{0}] \to (\forall x(\alpha \to \alpha[x/\dot{s}(x)]) \to \forall x \alpha)$ ($\alpha(x)$ eine $\mathcal{L}$–Formel).

(P7) ist kein Axiom, sondern ein Axiomenschema. Es heißt das *Induktionsschema*. Es entspricht allerdings nicht voll dem Peanoschen Induktionsaxiom. Dieses gilt für beliebige Eigenschaften, also Teilmengen von $\mathbb{N}$. Davon gibt es überabzählbar viele. In (P7) beschränken wir uns auf die abzählbar vielen in $\mathcal{L}_{\mathcal{A}}$ definierbaren Eigenschaften. Erst in der Peano-Arithmetik zweiter Stufe kann das Induktionsaxiom voll wiedergegeben werden:

$$\forall R^1(R^1(\dot{0}) \to (\forall x_1(R^1(x_1) \to R^1(\dot{s}(x_1))) \to \forall x_1 R^1(x_1))).$$

4.2 Vollständigkeit und Entscheidbarkeit

Eine Theorie $(\mathcal{L}, \Gamma)$ heißt *(endlich) axiomatisierbar*, falls es ein (endliches) Axiomensystem Δ mit $\Gamma = \mathrm{Cons}(\Delta)$ gibt. Man fordert von einem Axiomensystem i.a., daß es entscheidbar oder doch zumindest effektiv aufzählbar ist.

Definition 4.2.1

1. Eine Menge M heißt *entscheidbar*, wenn es einen Algorithmus gibt, der zu gegebener Eingabe a in endlich vielen Schritten feststellt, ob $a \in M$.
2. Sie heißt *effektiv aufzählbar*, wenn es einen Algorithmus gibt, der ihre Elemente nach und nach auflistet.
3. Eine Theorie $(\mathcal{L}, \Gamma)$ heißt *entscheidbar*, wenn Γ entscheidbar ist, und *semientscheidbar*, wenn Γ effektiv aufzählbar ist.
4. Sie heißt *effektiv axiomatisiert*, falls sie ein effektiv aufzählbares Axiomensystem hat.

Offensichtlich ist jede entscheidbare Menge auch effektiv aufzählbar. In der Berechenbarkeitstheorie wird gezeigt, daß die Umkehrung falsch ist. Da die Menge der Herleitungen effektiv aufzählbar ist, gilt:

Lemma 4.2.2 Ist Δ eine effektiv aufzählbare Menge von $\mathcal{L}$–Formeln, so ist auch $\mathrm{Cons}(\Delta)$ effektiv aufzählbar.

Daher ist jede axiomatisierte Theorie semi-entscheidbar. Darüberhinaus gilt:

Satz 4.2.3 Jede vollständige, effektiv axiomatisierte Theorie ist entscheidbar.

Beweis. Sei $\mathcal{T} = (\mathcal{L}, \Gamma)$ eine vollständige Theorie mit effektiv aufzählbarem Axiomensystem Δ. Ist $\mathcal{T}$ widerspruchsvoll, so ist jede $\mathcal{L}$–Formel logische Folgerung von Δ. Da von jeder Zeichenreihe über $\mathcal{L}$ effektiv festgestellt werden kann, ob sie eine Formel ist, ist $\mathcal{T}$ in diesem Fall entscheidbar. Ist $\mathcal{T}$ widerspruchsfrei, so ist wegen der Vollständigkeit für jede $\mathcal{L}$–Aussage α entweder $\alpha \in \mathrm{Cons}(\Delta)$ oder $\neg\alpha \in \mathrm{Cons}(\Delta)$. Wie wir gesehen haben, lassen sich die Elemente von $\mathrm{Cons}(\Delta)$ unter den obigen Vorraussetzungen durch einen Algorithmus auflisten. Hiermit können wir nun ein Entscheidungsverfahren für $\mathcal{T}$ konstruieren: Ist β eine $\mathcal{L}$–Formel, und α ihr Allabschluß, so lassen wir das Aufzählverfahren solange arbeiten, bis α oder $\neg\alpha$ aufgelistet wird. Im ersten Fall ist nach Lemma 2.3.14 $\beta \in \mathit{Cons}\,(\Delta)$. Im zweiten Fall ist $\beta \notin \mathrm{Cons}(\Delta)$. ■

An diese Ergebnisse schließen sich nun die folgenden Fragestellungen an, die in der mathematischen Logik untersucht werden:

1. Welche weiteren (effektiv axiomatisierten) Theorien sind entscheidbar?
2. Welche modelltheoretisch definierten Theorien sind axiomatisierbar?

Satz 4.2.4 — Presburger 1929. Sei $\mathcal{L}$ die Sprache, die wir aus $\mathcal{L}_{\mathcal{A}}$ erhält, indem wir das Zeichen $\dot{*}$ aus dem Alphabet entfernen. Dann ist

$$\mathrm{Th}(\mathbb{N}, +) = (\mathcal{L}, \mathrm{Cons}(\{P1, \ldots, P4, P7\})\ .$$

Daher ist $\mathrm{Th}(\mathbb{N}, +)$ entscheidbar.

Allerdings gilt

Satz 4.2.5 — Fischer und Rabin 1974. Jedes Entscheidungsverfahren für die Presburger–Arithmetik benötigt mindestens doppelt exponentielle Zeit.

Hinsichtlich eines Beweises dieser Sätze siehe [Presburger] und [Hilbert und Bernays 1934, pp. 359–366] bzw. [Fischer und Rabin (1974)] und [Ferrante und Rackoff 1979]. Wir wollen nun zeigen, daß eine große Klasse von Theorien unentscheidbar ist. Gewisse Aussagen über entscheidbare Mengen sind in dieser Theorie Sätze. Hierbei ist es üblich, sich auf entscheibare Teilmengen der natürlichen Zahlen zu beschränken. Mittels einer geeigneten Kodierung lassen sich entscheidbare Mengen über anderen Alphabeten in entscheidbare Teilmengen von $\mathbb{N}$ überführen.

Definition 4.2.6 Sei $\mathcal{T} = (\mathcal{L}, \Gamma)$ eine Theorie und enthalte $\mathcal{L}$ mindestens eine Individuenkonstante c und ein einstelliges Funktionszeichen f. Sei ferner $\hat{n} = c$, falls $n = 0$, und $\hat{n} = f(\widehat{n-1})$, falls $n > 0$. Dann heißt eine Teilmenge M von $\mathbb{N}$ *repräsentierbar* in $\mathcal{T}$, wenn es eine $\mathcal{L}$–Formel α mit höchstens einer frei vorkommenden Variablen x gibt, so daß genau dann $n \in M$, wenn $\alpha[x/\hat{n}] \in \Gamma$.

Wie in [Mendelson 1964] gezeigt wird, gilt:

Lemma 4.2.7 In der Peano-Arithmetik erster Stufe sind alle entscheidbaren Mengen repräsentierbar. Dies gilt sogar schon für die *Robinson-Arithmetik*

$$\mathcal{Q} = (\mathcal{L}_{\mathcal{A}}, \mathrm{Cons}(\{P1, \ldots, P6, R\}))$$

mit

(R) $x_1 \dot{\neq} \dot{0} \to \exists x_2(x_1 \doteq \dot{s}(x_2))$

Satz 4.2.8 — Unentscheidbarkeitstheorem (Church). Jede Theorie, in der alle entscheidbaren Teilmengen von $\mathbb{N}$ repräsentierbar sind, ist unentscheidbar.

Beweis. Der Beweis benutzt einen Diagonalabschluß, den wir zuerst erläutern wollen. Sei $(P_m)_{m\geqslant 0}$ eine Familie von Mengen natürlicher Zahlen und

$$Q = \{m \mid m \notin P_m\}.$$

Dann ist die Menge Q von allen Mengen P_m verschieden. Nehmen wir nämlich an, es wäre $Q = P_a$. Dann gilt genau dann $a \in P_a$, wenn $a \in Q$. Nach Definition von Q ist dies aber genau dann der Fall, wenn $a \notin P_a$; ein Widerspruch. Sei nun $\mathcal{T} = (\mathcal{L}, \Gamma)$ eine Theorie, in der alle entscheidbaren Teilmengen von $\mathbb{N}$ repräsentierbar sind und sei $\alpha_0, \alpha_1, \ldots$ eine effektive Aufzählung aller $\mathcal{L}$–Formeln mit höchstens einer frei vorkommenden Variablen x. Dann setzen wir

$$P_m = \{n \mid \alpha_m[x/\hat{n}] \in \Gamma\} \qquad \text{und} \qquad Q = \{m \mid \alpha_m[x/\hat{m}] \notin \Gamma\}.$$

Wie wir gerade gesehen haben, ist Q von allen P_m verschieden. Da die entscheidbaren Teilmengen von $\mathbb{N}$ in $\mathcal{T}$ repräsentierbar sind, sind diese in der Mengenfamilie (P_m) $m = 0, 1, \ldots$ enthalten. Also ist Q nicht entscheidbar. Nehmen wir nun an, $\mathcal{T}$ wäre entscheidbar, dann wäre es auch die Menge Q, im Widerspruch zum gerade bewiesenen. ■

Mit Satz 4.2.3 folgt hieraus

Satz 4.2.9 — Unvollständigkeitssatz. Jede widerspruchsfreie, effektiv axiomatisierte Theorie, in der alle entscheidbaren Teilmengen von $\mathbb{N}$ repräsentierbar sind, ist unvollständig.

Unter etwas stärkeren Voraussetzungen läßt sich sogar eine Aussage angeben, die kein Satz der Theorie und deren Nagation auch kein Satz der Theorie ist. Die Konstruktion dieser Aussage beruht i.w. auf den schon im Altertum bekannten *Lügner-Paradoxon* —Ist der Satz „Ich lüge jetzt“ (oder: „Dieser Satz ist falsch“) wahr oder falsch?—, wobei Wahrheit durch Herleitbarkeit ersetzt wird. Der erste Schritt in dieser Konstruktion besteht in der Kodierung der Formeln und Herleitungen einer vorgegebenen Theorie, und zwar so, daß wesentliche Eigenschaften dieser Kodierung entscheidbar und in einer schwachen Theorie der Arithmetik, wie etwa der Robinson–Arithmetik, beweisbar sind. Der an Detailfragen interessierte Leser sei auf [Mendelson 1964] verwiesen.

Satz 4.2.10 Sei $\mathcal{T} = (\mathcal{L}, \mathrm{Cons}(\Delta))$ eine Theorie mit entscheidbarem Axiomensystem Δ derart, daß $\mathcal{L}$ die Sprache der Arithmetik umfaßt, jedes Axiom der Robinson-Arithmetik aus Δ herleitbar ist und jede aus Δ herleitbare $\mathcal{L}_{\mathcal{A}}$–Formel in $(\mathbb{N}, +, *)$ gilt. (Wir sagen im Fall derzuletzt genannten Eigenschaft, daß $\mathcal{T}$ *korrekt* ist.) Sei ferner β eine $\mathcal{L}_{\mathcal{A}}$–Formel, in der genau die Variablen x_1 und x_2 frei vorkommen, so daß $\beta[x_1/\hat{n}][x_2/\hat{m}]$ in der Robinson-Arithmetik herleitbar ist, falls n die Codenummer einer $\mathcal{L}_{\mathcal{A}}$–Formel α mit höchstens einer frei vorkommenden Variablen x und m die Codenummer einer Herleitung der Aussage $\alpha[x/\hat{n}]$ aus Δ ist. Ist dann a die Codenummer der Aussage $\neg\exists x_2\beta$, so ist $\exists x_2\beta[x_1/\hat{a}]$ in $\mathcal{T}$ formal unentscheidbar, d.h. , es ist weder $\exists x_2\beta[x_1/\hat{a}]$ noch $\neg\exists x_2\beta[x_1/\hat{a}]$ aus Δ herleitbar.

Beweis. Nehmen wir an, es wäre $\exists x_2\beta[x_1/\hat{a}]$ aus Δ herleitbar. Dann gäbe es wegen der Korrektheit von $\mathcal{T}$ eine Herleitung von $\neg\exists x_2\beta[x_1/\hat{a}]$ aus Δ, ein Widerspruch zur Widerspruchsfreiheit von $\mathcal{T}$, die ihrerseits eine Konsequenz der Korrektheit ist. Nehmen wir nun andererseits an, es wäre $\neg\exists x_2\beta[x_1/\hat{a}]$ aus Δ herleitbar. Dann gäbe es die Codenummer m einer solchen Herleitung. Folglich wäre $\beta[x_1/\hat{a}][x_2/\hat{m}]$ in der Robinson–Arithmetik und also auch in $\mathcal{T}$ herleitbar. Dann wäre aber auch $\exists x_2\beta[x_1/\hat{a}]$ aus Δ herleitbar, im Widerspruch zur Widerspruchsfreiheit von $\mathcal{T}$. ■

Dies ist i.w. der Gödelsche Unvollständigkeitssatz. Gödel hat allerdings anstelle der Korrektheit eine rein syntaktische Bedingung an $\mathcal{T}$ gestellt. Es stellt sich nun die Frage, ob es noch andere „natürlichere“ formal unentscheidbare Aussagen gibt. Wie Gödel in seinem zweiten Unvollständigkeitssatz zeigt, ist unter ähnlichen Voraussetzungen wie im obigen Satz die Widerspruchsfreiheit der betrachteten Theorie in dieser nicht herleitbar, wegen der Korrektheit natürlich auch nicht ihre Negation. (Hinsichtlich eines Beweises siehe [Börger 1986] und [Shoenfield 1967]). Dieses Ergebnis ist von großer Bedeutung für das sogenannte Hilbertsche Programm, wonach ja die Mathematik oder Teile davon dadurch gegen das Auftreten von Paradoxien geschützt werden soll, daß sie formalisiert und die Widerspruchsfreiheit der formalisierten Theorie hergeleitet werden soll. Beachte in diesem Zusammenhang, daß jede stärkere Theorie, in dem die Widerspruchsfreiheit der betrachteten, die Voraussetzungen des Unvollständigkeitssatzes genügenden Theorie bewiesen werden soll, auch diesen Bedingungen genügt. Seit Ende der siebziger Jahre sind zahlreiche andere formal unentscheidbare Aussagen gefunden worden. So wird z.B. [Cichon 1987] die Tatsache ausgenutzt, daß zwar alle berechenbaren Funktionen über den natürlichen Zahlen durch einen Term in der Sprache der Arithmetik repräsentiert werden können, aber nicht von allen totalen unter diesen Funktionen in der Peano–Arithmetik $\mathcal{S}$ bewiesen werden kann, daß diese für jede natürliche Zahl definiert sind. Konstruieren wir nun eine berechenbare Funktion mit in $\mathcal{S}$ beweisbarer Totalität, so ist ihre Totalität in $\mathcal{P}$ nicht herleitbar und wegen der Korrektheit von $\mathcal{P}$ auch nicht die Negation dieser Aussage.

4.3 Das Entscheidbarkeitsproblem der Prädikatenlogik

In der Aussagenlogik haben wir uns mit dem Problem beschäftigt, ob es einen Algorithmus gibt, der von einer vorgelegten Formel entscheidt, ob sie erfüllbar ist. In der Prädikatenlogik interessieren wir uns für eine ähnliche Fragestellung: Gibt es zu einer gegebenen Sprache $\mathcal{L}$ einen Algorithmus, der das folgende Problem entscheidet:

Gegeben: Eine Formel α der Sprache $\mathcal{L}$

Frage: Ist α allgemeingültig ?

Dieses Problem heißt das *Entscheidungsproblem der Prädikatenlogik*. Da Strukturen auf beliebig mächtigen Mengen definiert sein können, ist es schwierig, sich einen Überblick über alle Strukturen für eine Sprache zu verschaffen. Daher ist anzunehmen, daß dieses Problem i.a. algorithmisch unlösbar ist.

Satz 4.3.1 — Church. Für eine Sprache mit mindestens einer Individuenkonstante, einem einstelligen Funktionszeichen, zwei zweistelligen Funktionszeichen und einem zweistelligen Relationszeichen ist algorithmisch nicht entscheidbar, ob eine vorgelegte Formel der Sprache allgemeingültig ist.

Beweis. Sei $\mathcal{L}_{\mathcal{A}}$ die Sprache der Arithmetik und α eine Formel dieser Sprache. Dann ist nach Lemma 2.3.14 genau dann P1, ..., P6,R $\models \alpha$, wenn P1 $\rightarrow$ (P2 $\rightarrow$ ... (P6 $\rightarrow$ (R $\rightarrow \alpha$)) ...) allgemeingültig ist. Gäbe es nun einen Algorithmus, der von einer gegebenen $\mathcal{L}$–Formel entscheidet, ob sie allgemeingültig ist, so hätten wir also auch ein Entscheidungsverfahren für die Menge der Sätze der Robinson–Arithmetik, ein Widerspruch zur Unentscheidbarkeit dieser Theorie. ■

Bemerkung 4.3.2 Satz 4.3.1 gilt auch noch unter der schwächeren Voraussetzung, daß $\mathcal{L}$ mindestens ein zweistelliges Relationszeichen enthält (siehe [Tarski, Mostowski und Robinson 1953]), allerdings nicht mehr, wenn die Sprache als nichtlogische Zeichen höchstens einstellige Relationszeichen enthält. Wir sprechen in diesem Fall von der *monadischen* Prädikatenlogik.

Satz 4.3.3 Das Entscheidungsproblem für die monadische Prädikatenlogik ist lösbar.

Beweis. Sei $\mathcal{L}$ eine Sprache erster Stufe, die als nichtlogische Zeichen höchstens einstellige Relationszeichen enthält und α eine Formel dieser Sprache. Seien ferner $R_1, \ldots, R_k$ die in dieser Formel vorkommenden Relationszeichen.

Zwischenbehauptung. *α ist genau dann allgemeingültig, wenn α in allen Strukturen gilt, deren Grundbereiche nicht mehr als 2^k Elemente haben.*

Da eine Menge mit höchstens 2^k Elementen nicht mehr als 2^{2^k} Teilmengen besitzt, gibt es höchstens $(2^{2^k})^k$ verschiedene Interpretationen der in α vorkommenden Relationszeichen. Die R_i sind einstellig, also sind nur einelementige Teilmengen interessant. Ob α in diesen Strukturen gilt, läßt sich algorithmisch feststellen. Also haben wir ein Testverfahren für die Allgemeingültigkeit von Formeln der Sprache $\mathcal{L}$. Wir beweisen nun die Zwischenbehauptung. Offensichtlich genügt es zu zeigen, daß α allgemeingültig ist, wenn α in allen Strukturen mit höchstens 2^k Elementen gilt. Werde deshalb angenommen, daß α in allen solchen Strukturen gilt, und sei $\mathcal{A}$ eine Struktur für $\mathcal{L}$. Wir definieren nun für Elemente a, b des Grundbereichs $\mathcal{A}$ eine Relation $\approx$ durch

$$a \approx b \iff \text{für alle } i = 1, \ldots, n : a \in I_{\mathcal{A}}(R_i) \iff b \in I_{\mathcal{A}}(R_i).$$

Dann ist $\approx$ eine Äquivalenzrelation, und da jede Äquivalenzrelation $[a]$ durch die k Wahrheitswerte $a \in I_{\mathcal{A}}(R_i)$ $1 \leq i \leq k$ charakterisiert ist, gibt es höchstens 2^k Äquivalenzklassen. Sei nun U die Menge dieser Äquivalenzklassen und für $i = 1, \ldots, k$

$$I(R_i) = \{[a] \mid a \in I_{\mathcal{A}}(R_i)\}.$$

Für von den R_i verschiedene Relationszeichen R aus $\mathcal{L}$ sei $I(R) = \emptyset$. Offensichtlich ist (U, I) eine Struktur für $\mathcal{L}$. Durch Induktion über den Formelaufbau läßt sich nun zeigen, daß α genau dann in (U, I) gilt, wenn α in $\mathcal{A}$ gilt. Wir haben angenommen, daß α in allen Strukturen für $\mathcal{L}$ mit höchstens 2^k Elementen gilt. Also gilt α in (U, I) und daher auch in $\mathcal{A}$. ■

4.4 Konservative Erweiterungen

Wie wir in Abschnitt 2.4 gesehen haben, müssen wir bei der Bildung der Skolemform einer Formel die Sprache, in der diese Formel gebildet wurde, durch Hinzunahme neuer Funktionszeichen bzw. Individuenkonstanten erweitern. Die Bedeutung dieser neuen Zeichen ist durch die Skolemform der Formel festgelegt.

Definition 4.4.1 Seien $\mathcal{T} = (\mathcal{L}, \Gamma)$ und $\mathcal{T}' = (\mathcal{L}', \Gamma')$ Theorien erster Stufe.

1. $\mathcal{T}'$ ist *Erweiterung* von $\mathcal{T}$, wenn $\mathcal{L}'$ Erweiterung von $\mathcal{L}$ ist und $\Gamma \supseteq \Gamma'$.
2. $\mathcal{T}'$ heißt *konservativ* über $\mathcal{T}$, wenn für jede $\mathcal{L}$–Formel α aus $\alpha \in \Gamma'$ stets $\alpha \in \Gamma$ folgt.

Sind $\mathcal{T}$ und $\mathcal{T}'$ axiomatische Theorien mit Axiomensystem Δ und Δ', so ist $\mathcal{T}'$ konservative Erweiterung von $\mathcal{T}$, wenn, bezogen auf die Sprache $\mathcal{L}$, aus Δ' nichts herleitbar ist, was nicht schon aus Δ herleitbar ist.

Lemma 4.4.2 Sei $(\mathcal{L}, \Gamma)$ eine Theorie und α eine $\mathcal{L}$–Formel. Sei α' die zugehörige Skolemform und $\mathcal{L}'$ die Erweiterung von $\mathcal{L}$, die aus $\mathcal{L}$ durch Hinzunahme der bei der Bildung von α' auftretenden Skolemfunktion hervorgeht. Dann haben $\mathcal{T} = (\mathcal{L}, \mathit{Cons}(\Gamma \cup \{\alpha\}))$ und $\mathcal{T}' = (\mathcal{L}', \mathit{Cons}(\Gamma \setminus \{\alpha\} \cup \{\alpha'\}))$ eine gemeinsame, konservative Erweiterung.

Beweis. Sei $\mathcal{T}'' = (\mathcal{L}', \mathit{Cons}(\Gamma \cup \{\alpha, \alpha'\}))$. Dann ist $\mathcal{T}''$ Erweiterung von $\mathcal{T}$ wie von $\mathcal{T}'$. Wir haben nun zu zeigen, daß die Erweiterungen konservativ sind.

Sei hierzu β eine $\mathcal{L}$–Formel mit $\Gamma, \alpha, \alpha' \models \beta$ und $\mathcal{A}$ ein Modell von $\Gamma \cup \{\alpha\}$. Wie wir in Satz 2.4.10 gesehen haben, läßt sich $\mathcal{A}$ zu einer Struktur für $\mathcal{L}'$ erweitern, die Modell von $\Gamma \cup \{\alpha, \alpha'\}$ ist. Dann gilt β in $\mathcal{A}'$. Da β eine $\mathcal{L}$–Formel ist, folgt, daß β auch in der Beschränkung von $\mathcal{A}'$ auf $\mathcal{L}$, d.h. in $\mathcal{A}$ gilt. Also ist $\mathcal{T}''$ konservative Erweiterung von $\mathcal{T}$.

Sei nun β eine $\mathcal{L}$–Formel mit $\Gamma, \alpha, \alpha' \models \beta$. Nach Satz 2.4.10 gilt α (als $\mathcal{L}$–Formel aufgefaßt) in jedem Modell von α'. Ist also $\mathcal{A}$ ein Modell von $\Gamma \cup \{\alpha'\}$, so auch von $\Gamma \cup \{\alpha, \alpha'\}$ und damit auch von β. Hieraus folgt, daß $\mathcal{T}''$ auch eine konservative Erweiterung von $\mathcal{T}'$ ist. ■

Die Überlegung, die wir hier für ein einzelnes Axiom durchgeführt haben, können wir ebenso auf ganze Axiomensysteme anwenden.

Definition 4.4.3 Sei $\mathcal{T}$ eine axiomatische Theorie mit zugehöriger Sprache $\mathcal{L}$ und Axiomensystem Δ. Sei ferner Δ^s die Menge der Skolemformen α^s der Elemente α von Δ, und zwar so, daß Δ^s zu jedem Axiom aus Δ nur eine Skolemform enthält und die zu verschiedenen dieser Axiome gehörenden Skolemfunktionen verschieden sind. Sei $\mathcal{L}^s$ die aus $\mathcal{L}$ durch Hinzunahme aller dieser Skolemfunktionen hervorgehende Erweiterung. Dann heißt die Theorie $\mathcal{T}^s = (\mathcal{L}^s, \mathit{Cons}(\Delta^s))$ *Skolemisierung* von $\mathcal{T}$.

Satz 4.4.4 Eine axiomatische Theorie $\mathcal{T}$ und ihre Skolemisierung $\mathcal{T}^s$ besitzen stets eine gemeinsame konservative Erweiterung.

Beweis. Sei Δ das Axiomensystem von $\mathcal{T}$ und $\mathcal{L}$ die zugehörige Sprache. Dann ist $\hat{\mathcal{T}} = (\mathcal{L}^s, \mathit{Cons}(\Delta \cup \Delta^s))$ Erweiterung von $\mathcal{T}$ und $\mathcal{T}^s$. Darüberhinaus folgt wie im Beweis des obigen Lemmas, daß $\hat{\mathcal{T}}$ konservativ über $\mathcal{T}^s$ ist.

Sei nun β eine aus $\Delta \cup \Delta^s$ herleitbare $\mathcal{L}$–Formel. Dann gibt es nach dem Endlichkeitssatz endlich viele Axiome $\alpha_1, \ldots, \alpha_n \in \Delta$, so daß β aus $\alpha_1, \ldots, \alpha_n, \alpha_1^s, \ldots, \alpha_n^s$ herleitbar ist. Gehe $\mathcal{L}'$ aus $\mathcal{L}$ durch Hinzunahme der in den α_i^s vorkommenden Skolemfunktionen hervor. Da diese Funktionszeichen alle verschieden sind, folgt mittels n–facher

Anwendung des obigen Lemmas, daß die Theorie $(\mathcal{L}', Cons(\{\alpha_1, \ldots, \alpha_n, \alpha_1^s, \ldots, \alpha_n^s\}))$ konservativ über $\mathcal{T}$ ist. Also β auch aus Δ herleitbar, womit gezeigt ist, daß $\hat{\mathcal{T}}$ auch konservativ über $\mathcal{T}$ ist. ■

Korollar 4.4.5 Jede $\mathcal{L}$–Formel ist genau dann Satz von $\mathcal{T}^s$, wenn sie auch Satz von $\mathcal{T}$ ist.

Was ist nun der Vorteil der Skolemisierung ?

Definition 4.4.6 Seien $\mathcal{A}$ und $\mathcal{A}'$ Strukturen für die Sprache $\mathcal{L}$. Dann heißt $\mathcal{A}'$ *Unterstruktur* von $\mathcal{A}$, wenn $U_{\mathcal{A}'} \subseteq U_{\mathcal{A}}$ und

- für jede Individuenkonstante c von $\mathcal{L}$ $I_{\mathcal{A}'}(c) = I_{\mathcal{A}}(c) \in U_{\mathcal{A}'}$,
- für jedes n–stelliges Funktionszeichen f von $\mathcal{L}$ $I_{\mathcal{A}'}(f) = I_{\mathcal{A}}(f) \mid_{U^n_{\mathcal{A}'}}$ und
- für jedes n–stellige Relationszeichen R von $\mathcal{L}$ $I_{\mathcal{A}'}(R) = I_{\mathcal{A}}(R) \cap U^n_{\mathcal{A}'}$.

Mittels Induktion über den Formelaufbau läßt sich zeigen:

Satz 4.4.7 Gilt eine quantorfreie $\mathcal{L}$–Formel in einer Struktur für $\mathcal{L}$, so auch in jeder ihrer Unterstrukturen.

Wir sehen also, daß die Klasse der Modelle der Skolemisierung einer Theorie gegen Unterstrukturen abgeschlossen ist.

5 — Mengenlehre

5.1 Einleitung

Alles ist Menge!

5.2 Die Axiome von ZFC

Die Zermelo-Fraenkel'sche Mengenlehre ist die Theorie bestehend aus der Sprache $\mathcal{L}$ mit Identität, welche sonst nur das zweistellige Relationszeichen $\in$ enthält (wie üblich in Infix-Notation geschrieben) und den in Kürze folgenden Axiomen.

Vorher wollen wir aber noch kurz ein paar abkürzende Schreibweisen einführen.

Schreibweise 5.2.1

- $\forall y \in x\ \varphi$ für $\forall y\ (y \in x \to \varphi)$
- $x \subset y$ für $\forall z \in x\ z \in y$
- $\exists! x\ \varphi$ für $\exists x\ (\varphi \wedge \forall y\ \varphi[x/y] \to x = y)$

Definition 5.2.1 Die Axiome bzw. Axiomenschema von ZF sind:

ZF0 Existenz: Es gibt eine Menge.

$$\exists x\ x = x\ .$$

ZF1 Extensionalität: Mengen, die dieselben Elemente enthalten, sind gleich.

$$\forall x\ \forall y\ \forall x\ (z \in x \leftrightarrow y \in x) \to y = x\ .$$

ZF2 Fundierung.

$$\forall x\ (\exists y\ y \in x) \to (\exists y \in x\ (\neg \exists z\ z \in y \wedge z \in x))$$

ZF3 Aussonderungsschema (Comprehension). Ist $\mathrm{FV}\,\varphi \subset x, z, w_1, \ldots, w_n$ (also insbesondere ist y nicht frei in φ), so gilt

$$\forall z\ \forall w_1, \ldots, w_n\ \exists y\ \forall x\ (x \in y \leftrightarrow (x \in z \wedge \varphi))$$

ZF4 Paarmengenaxiom.

$$\forall x\ \forall y\ \exists z\ x \in z \wedge y \in z$$

ZF5 Vereinigungsmengenaxiom

$$\forall A\ \exists B\ \forall C\ \forall x \in C\ (C \in A \to x \in B)$$

ZF6 Replacement: Ist $\mathrm{FV}\,\varphi \subset x, y, A, w_1, \ldots, w_n$ (also insbesondere ist B nicht frei in φ), so gilt

$$\forall A\ \forall w_1, \ldots, w_n\ \forall x \in A\ \exists! y\ \varphi \to (\exists B\ \forall x \in A\ \exists y\ {\in Y}\varphi)$$

ZF7 Unendlichkeit:

$$\exists x\ (\emptyset \in x \wedge (\forall y \in x\ (y \cup \{y\} \in x)))$$

ZF8 Potenzmengenaxiom

$$\forall x\ \exists y\ \forall z\ (z \subset x \to z \in y)$$

Einige Bemerkungen zu diesen Axiomen.

- Unendlichkeit macht erst in ein paar Zeilen Sinn, da $\cup$ und $\{\}$ noch undefiniert sind.
- Extensionalität: Die Rückrichtung ist herleitbar; muss also nicht extra gefordert werden.
- Die Menge deren Existenz in dem Aussonderungsaxiom gefordert wird ist eindeutig. Für sie wollen wir

  $$\{\, x \in y \mid \varphi \,\}$$

  schreiben.
- Das Fundierungsaxiom stellt sicher, daß es keine Menge x geben kann mit $x \in x$; ausserdem stellt es sicher, daß es keine unendliche Kette $x_1 \ni x_2 \ni x_3 \ldots$. Siehe Übung 1
- Aus dem Paarmengenaxiom und dem Aussonderungsschema folgt

  $$\forall x\ \forall y\ \exists! z\ x \in z \wedge y \in z \wedge \forall u \in z\ z = x \vee z = y$$

  Diese eindeutig bestimmte Menge z wollen wir von nun an mit

  $$\{x, y\}$$

  bezeichnen. Des Weiteren sei $\{x\} = \{x, x\}$.
- Ähnlich können wir auch eine eindeutige Menge wie B im Vereinigungsaxiom finden. Diese bezeichnen wir mit $\bigcup A$. Ausserdem sei $x \cup y = \bigcup \{x, y\}$.
- Und nochmals ähnlich sei $\mathcal{P}(x)$ die Potenzmenge des Potenzmengenaxioms definiert.
- Die leere Menge $\emptyset$ erhalten wir durch das Aussonderungsschema mit $\varphi \equiv x \neq x$ aus irgendeiner Menge (Axiom 0 stellt ja die Existenz von Mengen sicher). Sie hat genau die Eigenschaft, die man erwartet, nämlich $\forall x\ \neg(x \in \emptyset)$.

5.3 Klassen und die Russel'sche Antinomie

Definition 5.3.1 Eine Zusammenfassung von Mengen heißt *Klasse*. Klassen, die keine Mengen sind heißen *echte Klassen*. Formal fassen wir Klassen als Zeichenfolgen des Typs $\{ x \mid \varphi \}$ auf.

Vielleicht ist man voreilig zu der Meinung verleitet, daß wegen dem Aussonderungsschema alles vom Typ $\{ x \mid \varphi \}$ auch eine Menge sein muss. In der Tat ist dies keine dumme Vermutung, denn immerhin war der Unterschied auch Größen der Mathematik wie Frege Russel zunächst unbekannt.

Allerdings gilt

Satz 5.3.2 — Russel'sche Antinomie. $\{ x \mid x \notin x \}$ ist keine Menge. Oder formal:

$$\exists x \, \forall y \, (y \in x \leftrightarrow y \notin y)$$

steht im Widerspruch zu den Axiomen von ZF.

Beweis. Sei x wie oben. Dann gilt für $y = x$, daß $x \in x \leftrightarrow x \notin x$; ein Widerspruch. ■

Korollar 5.3.3 Es gibt keine Menge die alle Mengen enthält.

Beweis. Sonst könnte man mit dem Aussonderungsschema die Menge aus dem vorherigen Satz bilden. ■

Korollar 5.3.4 Es gibt echte Klassen.

Klassen sind eigentlich nur wichtig, um auf der Meta-ebene über gewisse Konstrukte zu reden. Für die Entwicklung der Mengenlehre aufbauend auf Axiomen sind sie aus technischer Sicht unwichtig.

5.4 Mehr Definitionen

- Für Durchschnitte benötigen wir kein extra Axiom, das Aussonderungsschema reicht schon aus: Die Menge $x \cap y = \{ z \in x \mid z \in y \}$
- Auch für eine nicht-leere Familie von Mengen F können wir analog den Durchschnitt definieren: Ist $x \in F$, so ist

$$\bigcap F = \{ z \in x \mid \forall y \in F \; z \in y \} \; .$$

Definition 5.4.1 Sind x, y Mengen, so heißt die Menge $\{\{x\}, \{x, y\}\}$ das geordnete Paar. In Zeichen schreiben wir $\langle x, y \rangle$.

Diese Definition geht auf den polnischen Mathematiker Kuratowski zurück. Es gibt auch alternative Möglichkeiten geordnete Paare zu definieren. Siehe Übung 2.

Satz 5.4.2 Für x, x', y, y' gilt, daß

$$\langle x, y \rangle = \langle x', y' \rangle \iff x = x' \wedge y = y' \; .$$

Beweis. Die Rückrichtung ist trivial, es reicht also die Richtung $\Longrightarrow$ zu beweisen. Wir unterscheiden zwei Fälle:

- $x = y$. Dann ist $\langle x, y \rangle = \{\{x\}\} = \langle x', y' \rangle = \{\{x'\}, \{x', y'\}\}$. Also ist $x' \in \{x\}$, und damit $x' = x$. Genauso folgt auch $y' = x$.

- $x \neq y$. Dann muss auch $x' \neq y'$ sein. Ausserdem muss gelten, daß $\{x'\} = \{x\}$ (der Fall $\{x'\} = \{x, y\}$ kann ausgeschlossen werden, da dann $x = x' = y$). Also ist $x = x'$ und damit auch einfach $y = y'$. ■

Wie üblich würden wir gerne das Produkt $A \times B$ als Menge von geordneten Paaren definieren; d.h. $\{ z \mid \exists a \in A, b \in B \; z = \langle a, b \rangle \}$. Um allerdings das Aussonderungsaxiom anzuwenden, müssen wir zuerst eine Menge finden, die mindestens alle Paare $\langle a, b \rangle$ mit $a \in A$ und $b \in B$ als Elemente besitzt; also eine Menge aus der wir die Elemente, welche wir wollen, aussondern können. Da $a, b \in A \cup B$ und damit $\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$ und damit wiederum $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$, haben wir eine passende Menge gefunden.

Definition 5.4.3

1. Eine *Relation* ist eine Menge, deren Elemente geordnete Paare sind.
2. Der *Definitionsbereich* (domain) von R ist
$$\operatorname{dom} R = \{ x \in \bigcup\bigcup R \mid \exists y\ss \langle x, y \rangle \in R \} .$$
3. Der *Bildbereich* von R ist
$$\operatorname{rge} R = \{ y \in \bigcup\bigcup R \mid \exists x \; \langle x, y \rangle \in R \} .$$
4. Die Umkehrrelation von R ist
$$R^{-1} = \{ \langle y, x \rangle \mid \langle x, y \rangle \in R \} .$$

Definition 5.4.4 Eine Menge f ist eine Funktion genau dann, wenn f eine Relation ist, so daß

$$\forall x \in \operatorname{dom} f \; \exists! y \; \langle x, y \rangle \in f .$$

Wie üblich schreiben wir in diesem Fall $f : A \to B$, falls f eine Funktion mit $\operatorname{dom}(f) = A$ und $\operatorname{rge} f \subset B$ ist.
Ausserdem schreiben wir $f(x)$ für das eindeutige Element y mit $\langle x, y \rangle \in f$.

Definition 5.4.5 Surjektiv, injektiv und bijektiv sind definiert wie üblich.

5.5 Wohlordnungen und Ordinalzahlen

Definition 5.5.1 Eine *lineare Ordnung* (auch *totale Ordnung*) ist ein Paar $\langle A, R \rangle$, so daß R die Menge A *linear ordnet*; d.h.

1. $\forall x, y, z \in A \; (xRy \wedge yRz \to xRz)$ (Transitivität)
2. $\forall x \in A \; \neg (xRx)$ (Irreflixivität)
3. $\forall x, y \in A \; xRy \vee x = y \vee yRx$ (Trichotomie)

Die Standardbeispiele für lineare Ordnungen sind $\langle \mathbb{Z}, < \rangle$ und $\langle \mathbb{R}, < \rangle$.

Definition 5.5.2 Zwei lineare Ordnungen[1] $\langle A, R \rangle$ und $\langle B, S \rangle$ heißen isomorph, falls es eine bijektive Funktion $f : A \to B$ gibt, so daß

$$\forall a, a' \in A \; \big(aRa' \leftrightarrow f(a) S f(a') \big) .$$

In Zeichen schreiben wir dann $\langle A, R \rangle \cong \langle B, S \rangle$.

[1] Diese Definition funktioniert natürlich für beliebige zwei-stellige Relationen.

Definition 5.5.3 Eine lineare Ordnung $\langle A, R\rangle$ heißt *Wohlordung* bzw. die Menge A *durch* R *wohlgeordnet*, falls jede nicht-leere Teilmenge ein R-minimales Element hat; d.h. wenn $M \subset A$ eine nicht-leere Teilmenge ist, so gibt es $m \in M$ so daß für alle $x \in M$ gilt $\neg(xRm)$.

Da A linear geordnet ist dies äquivalent zu der Existenz eines kleinsten Elements, d.h. für alle $x \in M$ gilt $x = m \vee mRx$.

Das Standardbeispiel für Wohlordnungen ist $\langle \mathbb{N}, <\rangle$. Gegenbeispiele sind $\langle \mathbb{Z}, <\rangle$, $\langle \mathbb{Q}, <\rangle$ und $\langle \mathbb{R}, <\rangle$.[2]

Definition 5.5.4 Für ein Paar $\langle A, R\rangle$ und $x \in A$ sei $\mathrm{pred}(A, x, R)$ definiert durch

$$\mathrm{pred}(A, x, R) = \{\, y \in A \mid yRx \,\} \ .$$

Satz 5.5.5 — Der Trichotomiesatz für Wohlordnungen. Sind $\langle A, R\rangle$ und $\langle B, S\rangle$ Wohlordnungen, so ist entweder

- $\langle A, R\rangle \cong \langle B, S\rangle$ oder
- es gibt $x \in A$ mit $\langle \mathrm{pred}(A, x, R), R\rangle \cong \langle B, S\rangle$ oder
- es gibt $y \in B$ mit $\langle A, R\rangle \cong \langle \mathrm{pred}(B, y, S), S\rangle$.

Beweis. Ausgelassen. ■

Definition 5.5.6 Eine Menge x heißt *transitiv*,[3] genau dann, wenn

$$\forall y \in x\ \forall z \in y\ (z \in x) \ .$$

Beispiele für transitive Mengen sind

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset, \{\emptyset\}\}\}$$

Nicht transitiv hingegen ist $\{\{\emptyset\}\}$

Definition 5.5.7 Eine Menge x heißt *Ordinalzahl*, genau dann wenn x transitiv ist und $\langle x, \in\rangle$ Wohlordnung ist.

Satz 5.5.8

1. Ist x Ordinalzahl und $y \in x$, so ist auch y Ordinalzahl.
2. Sind x, y Ordinalzahlen und $\langle x, \in\rangle \cong \langle y, \in\rangle$, so ist $x = y$.
3. Sind x, y Ordinalzahlen, so ist entweder $x = y$, $x \in y$ oder $y \in x$.
4. Sind x, y und z Ordinalzahlen und ist $x \in y$ und $y \in z$, so auch $x \in z$
5. Wenn C eine nicht-leere Menge von Ordinalzahlen ist, dann gibt es ein $x \in C$, so daß $\forall y \in x\ y \notin C$.

Beweis. 1. Wir müssen zeigen, daß y transitiv und $\langle y, \in\rangle$ Wohlordnung ist. Sei also $u \in v$ und $v \in y$. Da x transitiv ist ist dann auch $v \in x$ und damit wiederum $u \in x$. Nun ist $\langle x, \in\rangle$ Wohlordnung und damit insbesondere transitiv (im Ordnungssinn), also $u \in y$.

Sei nun $C \subset y$ eine nicht-leere Teilmenge dann ist, für alle $z \in C$, wegen $y \in x$ und der Transitivität von x auch $z \in X$. Also $C \subset x$, und damit existiert ein $\in$-minimales Element.

[2] Diese Mengen haben wir natürlich noch nicht formal definiert.
[3] nicht zu verwechseln mit der Transitivität von Ordnungen

2. Sei $f : A \to B$ bijektiv mit

$$\forall a, a' \in A \left(a \in a' \leftrightarrow f(a) \in f(a')\right) .$$

Betrachten wir nun die Menge $M = \{ x \in A \mid f(x) \neq x \}$. Wir wollen den Fall ausschliessen, daß M nicht-leer ist. Dann gäbe es aber, wegen der Wohlordnung von A ein minimales Element $m \in M$. Für alle $p \in m$ gilt aber, da m minimal ist, daß $f(p) = p$ ist. Damit ist $m \subset f(m)$. Umgekehrt gibt es wegen der Surjektivität für $q \in f(m)$ ein r mit $f(r) = q$. Aber aus $f(r) \in f(m)$ folgt wegen der Isomorphieeigenschaft, daß $r \in m$. Wiederum muss aber wegen der Minimalität von m gelten, daß $f(r) = r$. Also ist $q = f(r) = r \in m$; d.h. $f(m) \subset m$. Wegen des Extensionalitätsaxioms gilt also $f(m) = m$. Ein Widerspruch und damit ist M leer, oder anderst ausgedrückt $f = \mathrm{id}$. Damit sieht man leicht, daß $x = y$.

3. Dies folgt aus dem Trichotomiesatz für Wohlordnungen und dem vorherigen Punkt.

4. Dies folgt aus der Transitivität von z.

5. Sei $z \in C$. Entweder $z \cap C = \emptyset$, in welchem Falle wir einfach $x = z$ verwenden können, oder $z \cap C$ ist nicht leer. Im zweiten Falle können wir das minimale Element von $z \cap C$ wählen (z ist ja wohlgeordnet als Ordinalzahl), welches die gesuchten Eigenschaften hat.

■

Satz 5.5.9 — Die Antinomie von Burali-Forti 1897. Die Klasse aller Ordinalzahlen ist echt.

Beweis. Sonst wäre

$$u = \{ x \mid x \text{ ist Ordinalzahl} \}$$

wegen des obigen Lemmas selbst Ordinalzahl; also $u \in u$, was dem Fundierungsaxiom widerspricht (vgl. Übung 1) ■

Satz 5.5.10 Zu jeder Wohlordnung $\langle A, R \rangle$ gibt es genau eine Ordinalzahl x, so daß

$$\langle A, R \rangle \cong \langle x, \in \rangle .$$

Beweis. ■

5.6 Ordinalzahl Arithmetik

Wir wollen nun dazu übergehen Ordinalzahlen weniger als Mengen und mehr als Zahlen aufzufassen. Dazu schreiben wir $\alpha < \beta$ für $\alpha \in \beta$ und $\alpha \leqslant \beta$ für $\alpha \in \beta \vee \alpha = \beta$.

Lemma 5.6.1 1. $\alpha \leqslant \beta \iff \alpha \subset \beta$.

2. Ist C eine Menge von Ordinalzahlen, so ist das Supremum, d.h. die kleinste obere Schranke, gegeben durch

$$\sup C = \bigcup C .$$

3. Ist x eine nicht-leere Menge von Ordinalzahlen, so ist das Minimum, d.h. die kleinste untere Schranke, gegeben durch

$$\min C = \bigcap C .$$

Man beachte, daß $\sup C$ nicht unbedingt Element von C sein muss. Allerdings ist immer $\bigcap C \in C$.

Beweis. 1. Sei $\alpha \leqslant \beta$ und $x \in \alpha$. Entweder $\alpha = \beta$ und damit $x \in \beta$, oder $\alpha \in \beta$. Aber in letzterem Falle ist, wegen der Transitivität von β auch $x \in \beta$. Umgekehrt sei $\alpha \subset \beta$. Wegen der Trichotomie der Ordinalzahlen müssen wir nur den Fall $\beta \in \alpha$ ausschliessen. Da in diesem Fall aber $\beta \in \beta$ wäre sind wir wegen des Fundierungsaxioms fertig.

2.

■

Definition 5.6.2 Für eine Ordinalzahl α definieren wir $S(\alpha)$, bzw. $\alpha + 1$ als

$$\alpha + 1 = \alpha \cup \{\alpha\} .$$

Satz 5.6.3

1. $\alpha + 1$ ist eine Ordinalzahl.
2. $\alpha < \alpha + 1$.
3. $\forall \beta\ \beta < \alpha + 1 \to \beta \leqslant \alpha$.

Definition 5.6.4 $0 = \emptyset$, $1 = S(0)$, $2 = S(1)$, ... Dies sind die sogenannten von Neumannn'schen natürlichen Zahlen.

Definition 5.6.5 α heißt *Nachfolgerordinalzahl* falls es eine Ordinalzahl β mit $\alpha = \beta + 1$ gibt. Eine Zahl $\alpha \neq 0$ heißt *Limesordinalzahl* falls sie keine Nachfolgerordinalzahl ist.

Satz 5.6.6 — Transfinite Induktion / Ordinalzahlinduktion.
Sei φ eine Eigenschaft, so daß

1. $\varphi[x/0]$
2. $\varphi[x/\alpha] \to \varphi[x/\alpha + 1]$ für alle Ordinalzahlen α und
3. $(\forall \alpha < \beta\ \varphi[x/\alpha]) \to \varphi[x/\beta]$,

dann gilt $\varphi[x/\alpha]$ für alle Ordinalzahlen α.

Beweis. Nehmen wir an, es gibt α mit $\neg\varphi[x/\alpha]$. Wir können annehmen (Fundierungsaxiom[4].), daß α minimal ist. Dann ist aber α als Ordinalzahl entweder 0, eine Nachfolgerordinalzahl, oder eine Limesordinalzahl. In allen drei Fällen können wir ein kleineres Element finden, für das φ nicht gilt. ■

Die Transfinite Induktion erlaubt uns die folgende Definition eindeutig zu machen:

Definition 5.6.7 Seien α, β Ordinalzahlen. Die *ordinale Addition* ist rekursiv definiert über

1. $\alpha + 0 = \alpha$
2. Wenn β Nachfolgerordinalzahl ist, also $\beta = \gamma + 1$, so ist $\alpha + \beta = (\alpha + \gamma) + 1$.
3. Ist β Limesordinalzahl, so ist

$$\alpha + \beta = \bigcup_{\gamma < \beta} (\alpha + \gamma) .$$

[4]Hier ist das erste mal, daß wir das volle Fundierungsaxiom verwenden, und nicht nur $\neg(x \in x)$

Bemerkung 5.6.8 Mit dieser Definition ist $\alpha + 1$ zwar doppeldeutig, beide Definitionen führen aber zur gleichen Ordinalzahl.

5.7 Das Auswahlaxiom

Das Auswahlaxiom (AC) besagt

$$\forall A\ (\forall x \in A\ (\exists y\ y \in x) \to \exists f : A \to \cup A\ (\forall x \in A\ f(x) \in x))$$

D.h. wenn für eine Menge von Mengen A jede Menge $x \in A$ nicht leer ist, dann existiert eine *Funktion* f, die jeder Menge $x \in A$ ein Element in A zuordnet.

Auch wenn das Auswahlaxiom harmlos aussieht, so hat es doch recht fragwürdige Konsequenzen, wie z.B. das Banach-Tarski Paradox.

Hier wollen wir zeigen, daß das Auswahlaxiom in ZF äquivalent ist zu den folgenden Aussagen:[5]

> [Das Lemma von Zorn] Sei $\langle P, R\rangle$ eine Halbordnung.[6] Hat jede Kette (total geordnete Teilmenge) eine obere Schranke in P, so hat P mindestens ein maximales Element.
>
> [Der Wohlordnungssatz] Jede Menge kann wohlgeordnet werden. D.h. ist P eine Menge, so existiert eine zweistellige Relation R, so daß $\langle P, R\rangle$ Wohlordnung ist.

Beweis.

- Zeigen wir zunächst, daß das Lemma von Zorn aus dem Auswahlaxiom folgt.
  Nehmen wir hierzu an, daß das Lemma von Zorn falsch ist. Dann können wir für jede total geordnete Teilmenge T von P ein Element $b(T)$ finden, daß echt größer als eine obere Schranke ist. Das Auswahlaxiom stellt sicher, daß b eine *Funktion* ist.

  Sei jetzt $A_0 \in T$ beliebig. Für eine Nachfolgerordinalzahl $\alpha = \beta + 1$ sei $A_{\beta+1} = A_\beta \cup \{b(A_\beta)\}$ und für eine Limesordinalzahl α sein $A_\alpha = \bigcup_{\beta<\alpha} A_\beta \cup \{b(A_\beta)\}$. Diese Mengen sind so konstruiert, daß für $\alpha < \gamma$ die Menge A_α eine echte Teilmenge von A_γ ist. Alle diese Menge sind aber Teilmengen von P, also erhalten wir einen Widerspruch, da wir auf diese Weise die Klasse der Ordinalzahlen in die Menge P injektiv einbetten können.

- Wollen wir als nächstes den Wohlordnungssatz aus dem Lemma von Zorn beweisen. Sei dazu P eine Menge. Betrachten wir nun die Menge

  $$M = \{\, \langle A, R\rangle \mid A \subset P \wedge \langle A, R\rangle \text{ ist eine Wohlordnung} \,\} .$$

  Auf M selber können wir eine Halbordnung definieren durch $\langle E, R\rangle \leqslant \langle F, S\rangle$ genau dann wenn $E \subset F$ ist und S auf E genau R entspricht; d.h. für alle $x, y \in E$ ist $xRy \iff xSy$. Diese Halbordnung erfüllt die Voraussetzung des Lemma von Zorns: Sei K eine nach dieser Halbordnung total geordnete Kette, dann ist

  $$\left\langle \bigcup \{\, E \mid \exists R\ \langle E, R\rangle \in K \,\}, \bigcup \{\, R \mid \exists E\ \langle E, R\rangle \in K \,\} \right\rangle$$

[5] Es gibt ein ganzes Buch über Äquivalenzen des Auswahlaxioms!
[6] D.h. R ist eine reflexive, transitive, und antisymmetrische Relation.

eine obere Schranke. Also hat M ein maximales Element $\langle E_m, R_m\rangle$. Jetzt muss aber $E_m = A$ sein, denn sonst gäbe es $x \in A \setminus E_m$; aber dann könnten wir R_m zu R'_m auf $E_m \cup \{x\}$ ausweiten, so daß $\langle E_m, R_m\rangle \leqslant \langle E_m \cup \{x\}, R'_m\rangle$, was ein Widerspruch zur Maximalität wäre.

- Zeigen wir als letztes, daß das Auswahlaxiom aus dem Wohlordnungssatz folgt. Sei hierzu A eine Menge von nicht-leeren Mengen. Definiere nun $X = \bigcup A$. Dann kann, nach dem Wohlordnungssatz, X wohlgeordnet werden; d.h. es gibt R so daß $\langle X, R\rangle$ eine Wohlordnung ist. Für jedes $x \in A$, und also $x \subset X$, gibt es jetzt ein eindeutiges R-minimales Element in x. Auf diese Weise können wir also eine Funktion definieren, die jedem x dieses minimale Element zuordnet.

■

5.8 Übungsaufgaben

1. Zeigen Sie, daß aus den ZF-Axiomen folgt, daß es keine Menge x gibt, so daß $x \in x$.
2. Wieners Vorschlag um geordnete Paare zu definieren war

   $$\langle x, y\rangle = \{\{\{x, y\}\}, \{\{y\}\}\} \ .$$

   Zeigen Sie, daß auch für diese Definition gilt, daß für x, x', y, y' gilt, daß

   $$\langle x, y\rangle = \langle x', y'\rangle \iff x = x' \wedge y = y' \ .$$

Literaturverzeichnis

[Schöning 1987] Schöning, U. (1987). *Logik für Informatiker*. Wissenschaftsverlag, Mannheim.

[Lloyd 1987] Lloyd, J. W. (1987). *Foundations of Logic Programming*. 2. Auflage, Springer, Berlin.

[Börger 1986] Börger, E. (1986). *Berechenbarkeit, Komplexität, Logik*. 2. berichtigte Auflage, Vieweg, Braunschweig.

[Gallier 1986] Gallier, J. H. (1986). *Logic for Computer Science*. Harper & Row, New York.

[Richter 1978] Richter, M. M. (1978). *Logikkalküle*. Teubner, Stuttgart.

[Nerode und Shore] Nerode, A. und Shore, R. A. (1989). *Logic and Logic Programming*. Vorlesungsscript. Cornwell University, Ithaca, N. Y. .

[Presburger] Presburger, M. (1929). Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in in welcher die Addition als einzige Operation hervortritt. *C. R. I. Congrès des Math des Pays Slaves* , Warschau, pp. 192–201,395.

[Fischer und Rabin (1974)] Fischer, M. J. und Rabin, M. O. (1974). Super-exponential complexity of Presburger arithmetic. *S/AM-AMS Proc., Vol.7, Complexity of Computation (Korp, R. M. , Hrsg.)*

[Ferrante und Rackoff 1979] Ferrante,J. und Rackoff, Ch. W. (1979). *The Computational Complexity of Logic Theories*. Lec. Nots Math. 718. Springer, Berlin.

[Hilbert und Bernays 1934] Hilbert, D. und Bernays, P. (1934). *Grundlagen der Mathematik*, Bd.I. Springer, Berlin.

[Mendelson 1964] Mendelson, E. (1964) *Introduction to Mathematical Logic*. Van Nostrand, New York.

[Tarski, Mostowski und Robinson 1953] Tarski, A. , Mostowski, A. und Robinson, R. (1953). *Undecidable Theories*. North–Holland, Amsterdam.

[Cichon 1987] Cichon, E. A. (1983). A short proof of recently discovered independence results using recursiontheoretic methods. *Proc AMS 87, pp.704–706*.

[Shoenfield 1967] Shoenfield,J. R. (1967) *Mathematical Logic*. Addison-Wesley, Reading, Mass

[Frege 1892] Frege, G. (1892) Über Sinn und Bedeutung. *Zeitschr. für Philos. und philos. Kritik*, NF 100, pp.25–50.

[Gerard, Lafont und Taylor 1989] Gerard,J. Y. , Lafont, Y. und Taylor, P. (1989). *Proofs and Types*. Cambridge University Press, Cambridge.