Logische Grundlagen der Informatik

Skript zur Vorlesung

Prof. Peter H. Starke
Lehrstuhl für Automaten- und Systemtheorie

27. Oktober 1994

Inhaltsverzeichnis

Kapitel 0

Einleitung

Die Vorlesung „Logische Grundlagen der Informatik“ gibt eine Einführung in grundlegende Begriffe und Methoden der Mathematik und der darauf basierenden Informatik. Zu diesen grundlegenden Begriffen gehören sicher der Mengenbegriff und der Kalkülbegriff. Ersterer demonstriert, wie die Abstraktion in der Mathematik funktioniert, letzterer die Bildung von Theorien, d. h. die Bildung mathematischer Modelle. Der Dualismus zwischen Modell und Wirklichkeit spiegelt sich dabei in der Beziehung zwischen Syntax und Semantik eines Kalküls wider. Dabei betrachten wir es als Hauptaufgabe der Logik, semantische (d. h. inhaltliche) Beziehungen und Begriffe syntaktisch zu charakterisieren, insbesondere algorithmisch zu erfassen. Deshalb wird bei der Untersuchung der Prädikatenlogik ein Ausflug in die Algorithmentheorie notwendig sein.

Kapitel 1

Mengen

1.1 Mengenbegriff und Elementbeziehung

In diesem Abschnitt verfolgen wir das Ziel, den Mengenbegriff zu definieren. Dazu müssen wir uns zunächst Rechenschaft darüber geben, was wir unter einer Definition verstehen wollen.

1.1.1 Arten von Definitionen

1. *explizite* Definitionen
   Das zu definierende Objekt kommt im definierenden Ausdruck nicht vor.

   (a) Definition durch Aufzählung
   Beispiel

   - Die Menge der Ziffern besteht aus den Elementen $0, 1, \ldots, 9$

   (b) Definition durch Angabe einer charakteristischen Eigenschaft
   Beispiel x ist Quadratzahl:

   - x ist ganze Zahl und es gibt ein y mit: $y \cdot y = x$

   Nachteile:

   - Aufzählung ist unmöglich bei unendlichen Mengen
   - charakteristische Eigenschaft setzt andere Begriffe voraus

2. *implizite* Definitionen
   Das zu definierende Objekt kommt im definierenden Ausdruck vor.

   (a) rekursive (induktive) Definition
   Beispiel Die Folge $(a_i)_{i=0,1,\ldots}$ von natürlichen Zahlen wird definiert durch

   - $a_0 = 0$
   - $a_{i+1} = a_i + 2i + 1 = a_i + i + i + 1$

   $\Rightarrow$ eine induktive Definition beschreibt den Aufbau aus (elementaren) Objekten mittels (elementarer) Operationen.

   (b) Axiomatische Charakterisierung
   Angabe eines Systems von Aussagen, welche die zu charakterisierenden Grundbegriffe in Beziehung setzen.

Definitionen sind nicht wahr oder falsch (höchstens unzweckmäßig), bedürfen aber einer Rechtfertigung hinsichtlich der Frage, ob wenigstens ein Objekt der definierten Art überhaupt existiert.

Bei expliziten Definitionen ist dies i. a. klar; wenn die Elemente $0, 1, \ldots, 9$ existieren, so existiert die Menge der Ziffern. Ganz offen ist dieses Problem bei der axiomatischen Charakterisierung; hierbei geht es doch um die Frage, ob es ein Modell des Axiomensystems gibt, d. h. Objekte, bei denen alle Aussagen dieses Systems wahr sind. (Dann nennt man dieses System widerspruchsfrei.)

1.1.2 Die CANTORschen „Definitionen"

Der Mengenbegriff gilt als der Grundbegriff der Mathematik in dem Sinne, daß sich alle übrigen mathematischen Begriffe auf der Basis der Begriffe der Menge und der Elementbeziehung exakt begründen lassen. Dementsprechend ist eine *explizite* Definition des Begriffs „Menge" nicht möglich, denn eine explizite Definition eines Begriffes bedeutet immer, daß dieser Begriff auf andere (grundlegendere) Begriffe zurückgeführt wird.

Die Mengenbildung hat zwei Aspekte:

- operativ-praktischer Aspekt: Äpfel in den Korb legen, Perlen auffädeln $\Rightarrow$ Zusammenfassen
- Abstraktionsaspekt: Schaffung eines neuen Objektes, Absehen von der Individualität der Elemente, gemeinsame Eigenschaft.

Erklärung 1 (G. CANTOR) Eine Menge M ist eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche Elemente der Menge M genannt werden, zu einem ganzen.

Wenn wir den Abstraktionsaspekt stärker betonen wollen, können wir diese Erklärung wie folgt präzisieren:

Erklärung 2 Zu jeder Eigenschaft H der wohlunterschiedenen Objekte unserer Anschauung und unseres Denkens existiert eine Menge M derart, daß für jedes Objekt x gilt:

$$\underbrace{x \text{ ist Element von } M}_{x\in M} \text{ genau dann, wenn } \underbrace{x \text{ die Eigenschaft } H \text{ hat}}_{H(x)}$$

Als abkürzende Schreibweisen benutzen wir künftig:

1. $x \in M$ für „x ist ein Element von M"
2. $x \notin M$ für „x ist kein Element von M"
3. $H(x)$ für „x hat die Eigenschaft H"
4. $\{x|H(x)\}$ für „die Menge aller x mit $H(x)$"

Die geschweiften Klammern werden zur Bezeichnung von Mengen reserviert.

Wenn wir die Erklärung 2 (oder 1) zur Grundlage eines Aufbaus der Mengenlehre (bzw. der Mathematik) verwenden wollen, müssen wir uns nach der Widerspruchsfreiheit dieser Erklärung (dieses Axioms) fragen. RUSSEL zeigte uns um die Jahrhundertwende, mit folgender Überlegung, daß es damit schlecht bestellt ist.

Wir betrachten die Eigenschaft H^*, die durch die Formel $x \notin x$ bestimmt ist, d. h. ein Objekt unserer Anschauung oder unseres Denkens hat die Eigenschaft M^* genau dann, wenn es *nicht* Element von x ist. Nach der Erklärung 2 existiert dann die Menge $M^* \equiv \{x|x \notin x\}$.

Nun ist M^* selbst ein Objekt unseres Denkens, wir können also fragen, ob $M^* \in M^*$ ist. Es ist $M^* \in M^*$ genau dann, wenn M^* die Eigenschaft H^* hat, also genau dann, wenn $M^* \notin M^*$ ist. Das ist ein (logischer) Widerspruch, die sogenannte RUSSELsche Antinomie.

Wir haben gesehen, daß die Erklärungen 1 und 2 zum Aufbau der Mengenlehre nicht brauchbar sind, andererseits kommen die Erklärungen unserem anschaulichen Vorstellungen von der Mengenbildung entgegen. Was haben wir also bei der Präzisierung bzw. Formulierung unserer Vorstellungen vergessen? Es ist anschaulich klar, daß eine Menge gegenüber den Elementen eine neue Qualität darstellt, etwas durch Abstraktion gewonnenes, das nicht ohne weiteres mit seinen Elementen auf die gleiche Stufe gestellt werden darf.

Eine Lösung (es gibt andere Möglichkeiten), die Mengenbildung soweit einzuschränken, daß keine Mengen mehr gebildet werden können, die zu Antinomien führen (die RUSSELsche Antinomie ist nur *ein* Beispiel), besteht darin, Mengen verschiedener Stufen $(0., 1., \ldots)$ zu betrachten und die Mengenbildung nur von Stufe zu Stufe zuzulassen. Wir legen einen Objektbereich E von Elementen, auch Mengen *Nullter Stufe* genannt, zugrunde, durch Zusammenfassung von Elementen bilden wir die Mengen erster Stufe, solche Mengen bilden die Elemente von Mengen zweiter Stufe und so fort.

Wir bezeichnen im Folgenden:

- Elemente von E (Mengen nullter Stufe) durch kleine lateinische Buchstaben $a, b, c, \ldots$
- Mengen von Elementen von E (Mengen erster Stufe) durch große lateinische Buchstaben $A, B, \ldots, M, \ldots$
- Mengen zweiter Stufe (Mengensysteme) durch große deutsche Buchstaben $\mathfrak{M}, \mathfrak{N}, \ldots$
- allgemein: Mengen n-ter Stufe $(n = 0, 1, \ldots)$ durch große lateinische Buchstaben mit dem oberen Index $n : M^{(n)}, N^{(n)}, \ldots$

Axiom 1.1.3 (Mengenbildungsaxiome)
Zu jeder Eigenschaft H von Mengen n-ter Stufe $(n = 0, 1, 2, \ldots)$ gibt es eine Menge $M^{(n+1)}$ $n+1$-ter Stufe derart, daß für alle Mengen $N^{(n)}$ n-ter Stufe gilt:

$$N^{(n)} \in M^{(n+1)} \text{genau dann, wenn } H\left(N^{(n)}\right).$$

Aus diesem Mengenbildungsprinzip kann die RUSSELsche Antinomie nicht hergeleitet werden, weil da die Eigenschaft H^*, d. h. $x \notin x$, keine zur Mengenbildung zugelassene Eigenschaft ist.

Zum Aufbau der Mengenlehre reichen die Axiome 1.1.3 allein nicht aus, wie wir sofort sehen, wenn wir uns mit der Frage beschäftigen, wann Mengen gleich sind, wobei wir voraussetzen, daß uns das für Elemente von E bekannt ist, handelt es sich doch gemäß unserer Anschauung dabei um „wohlunterschiedene" Objekte. Zwei unterschiedliche Definitionen der Gleichheit bieten sich an:

Definition 1.1.4 (Umfangsgleichheit, extensionale Gleichheit)
Mengen $M^{(n+1)}$, $N^{(n+1)}$ $(n+1)$-ter Stufe heißen umfangsgleich ($M^{(n+1)} =_u N^{(n+1)}$), wenn sie dieselben Elemente haben.

Definition 1.1.5 (Eigenschaftsgleichheit)
Mengen $M^{(n+1)}$, $N^{(n+1)}$ $(n+1)$-ter Stufe heißen eigenschaftsgleich ($M^{(n+1)} =_e N^{(n+1)}$), wenn sie dieselben (mengentheoretischen) Eigenschaften haben, d. h. für jede Eigenschaft H von Mengen ($(n+1)$-ter Stufe gilt

$$H\left(M^{(n+1)}\right) \text{ genau dann, wenn } H\left(N^{(n+1)}\right)$$

Mit der Definition der Umfangsgleichheit präsentieren wir unsere Vorstellung, daß eine Menge durch ihre Elemente bereits eindeutig bestimmt ist, während die Eigenschaftsgleichheit besagt, daß Gleichheit die Gemeinsamkeit in allen Eigenschaften impliziert. Naheliegend ist es daher, nach der Beziehung zwischen diesen beiden Begriffen zu fragen.

Satz 1.1.6
Wenn $M^{(n+1)} =_e N^{(n+1)}$, so $M^{(n+1)} =_u N^{(n+1)}$ $(n = 0, 1, \ldots)$.

Beweis Wir haben zu zeigen, daß (unter der Voraussetzung $M^{(n+1)} =_e N^{(n+1)}$) für alle Mengen $X^{(n)}$ n-ter Stufe gilt

$$X^{(n)} \in M^{(n+1)} \text{genau dann ,wenn } X^{(n)} \in N^{(n+1)},$$

Denn dann und nur dann, wenn 1.1.2 gilt, haben $M^{(n+1)}$ und $N^{(n+1)}$ dieselben Elemente.

Es sei nun $X^{(n)}$ eine beliebige Menge n-ter Stufe. Wir betrachten die Eigenschaft $H^{X^{(n)}}$ von Mengen $(n+1)$-ter Stufe, mit:

$$H^{X^{(n)}}\left(Y^{(n+1)}\right) \text{ genau dann, wenn } X^{(n)} \in Y^{(n+1)}.$$

weil $M^{(n+1)} =_e N^{(n+1)}$ ist, gilt

$$\begin{array}{rlll} X^{(n)} \in M^{(n+1)} & \text{gdw.} & H^{X^{(n)}}(M^{(n+1)}) & (\text{nach Def. von } H^{X^{(n)}}) \\ & \text{gdw.} & H^{X^{(n)}}(N^{(n+1)}) & (\text{wegen } M^{(n+1)} =_e N^{(n+1)}) \\ & \text{gdw.} & X^{(n)} \in N^{(n+1)} & (\text{nach Def. von } H^{X^{(n)}}), \end{array}$$

also gilt 1.1.2 und der Satz 1.1.6 ist bewiesen.

Die Umkehrung des Satzes 1.1.6, d. h. die Aussage:

$$\text{Wenn } M^{(n+1)} =_u N^{(n+1)}, \text{ so } M^{(n+1)} =_e N^{(n+1)}$$

kann dagegen aus den Mengenbildungsaxiomen nicht abgeleitet werden. Wir fordern daher die

Axiom 1.1.7 (Extensionalitätsaxiome)
Wenn Mengen $(n+1)$-ter Stufe umfangsgleich (extensional gleich) sind, so sind sie eigenschaftsgleich.

Nach dieser Forderung sind Umfangsgleichheit und Eigenschaftsgleichheit identisch, wir sprechen daher nur noch von Gleichheit schlechthin und schreiben $M = N$, wenn Mengen M, N gleich sind.

Um genügend „Material“ für die Mengenbildung zu haben, fordern wir ferner das

Axiom 1.1.8 (Unendlichkeitsaxiom)
Es gibt eine unendliche Menge erster Stufe.

Anschaulich bedeutet das, daß unser Objektbereich E unendlich viele Elemente hat, was aber „unendlich“ im Sinne der Mengenlehre bedeutet, kann an dieser Stelle noch nicht präzisiert werden. Ein weiteres Axiomenschema, das aus den bereits angegebenen Axiomen nicht bewiesen werden kann (von diesen unabhängig ist), bilden die sogenannten

Axiom 1.1.9 (Auswahlaxiome)
Zu jeder nichtleeren Menge $M^{(n+2)}$ $(n+2)$-ter Stufe (zu jedem Mengensystem) mit paarweise disjunkten nichtleeren Mengen $N^{(n+1)}$ als Elementen gibt es eine Auswahlmenge $A^{(n+1)}$, die mit jedem $N^{(n+1)}$ aus $M^{(n+2)}$ genau ein Element $X^{(n)}$ gemeinsam hat.

Dabei heißt eine Menge *nichtleer*, wenn sie (wenigstens) ein Element besitzt und Mengen (gleicher Stufe) heißen *disjunkt*, wenn sie kein Element gemeinsam haben.

Mit den bisher angegebenen Axiomen kommt man nun tatsächlich beim Aufbau der Mengenlehre aus. Dabei muß an dieser Stelle die Rolle der Auswahlaxiome unklar bleiben; ihre Bedeutung kann erst eine ihrer Anwendungen beim Beweis tiefliegender Sätze der Mengenlehre klar machen.

Bevor wir uns im nächsten Abschnitt mit dem Rechnen mit Mengen (der sogenannten Mengenalgebra) beschäftigen, wollen wir noch zwei wichtige spezielle Mengen definieren und benennen.

Betrachten wir die durch $x \neq x$ gegebene Eigenschaft $H^{\neq}$ von Mengen 0-ter Stufe (Elementen). Nach 1.1.3 gibt es eine Menge M_0 mit

$$x \in M_0 \text{ gdw. } x \neq x$$

für alle Elemente x aus dem Objektbereich E. Weil jedes Element x zu sich selbst gleich ist, enthält M_0 *kein* Element. Ist andererseits M' eine Menge erster Stufe, die kein Element enthällt, so enthällt M' offenbar dieselben Elemente wie M_0 (nämlich keine), nach dem Extensionalitätsaxiom gilt also $M' = M_0$.

Dieselbe Überlegung für höhere Stufen $n = 1, 2, \ldots$ beweist den

Satz 1.1.10
Zu jeder Stufe $n+1$ gibt es genau eine Menge M_0 $(n+1)$-ter Stufe derart, daß für alle Mengen N n-ter Stufe gilt $N \notin M_0$.

Nachdem wir gezeigt haben, daß es eine aber auch nur eine solche Menge gibt dürfen wir von *der* Menge M_0 $(n+1)$-ter Stufe sprechen.

Definition 1.1.11
Die nach Satz 1.1.10 bestimmte Menge $M_0^{(n+1)} = \left\{N^{(n)} | N^{(n)} \neq N^{(n)}\right\}$ heißt *die leere Menge* $(n+1)$-ter Stufe und wird durch $\emptyset^{(n+1)}$ notiert. Für $\emptyset^{(1)}$ schreiben wir auch $\emptyset$.

In analoger Weise zeigt man mittels der Eigenschaft $x = x$, daß es zu jeder Stufe $(n+1)$ $(n = 0, 1, \ldots)$ genau eine *Allmenge* $E^{(n+1)}$ $(n+1)$-ter Stufe gibt, die genau die Mengen n-ter Stufe als Elemente hat. Dabei ist $E^{(1)}$ gerade der Objektbereich E, d. h. $E^{(1)} = E$. Die Allmenge $E^{(2)}$ zweiter Stufe bezeichnen wir mit $\mathfrak{E}$.

Zu jedem Element $a \in E$ existiert nach dem Mengenbildungsaxiom die Menge M für die gilt:

- $a \in M$
- Für jedes b gilt: Wenn $b \in M$, so $b = a$.

Wir schreiben M als $\{a\}$.

Für Elemente a, b ist dementsprechend $\{a, b\}$ die Menge M, für die gilt:

- $a \in M$, $b \in M$
- Für jedes c gilt: Wenn $c \in M$, so $c = a$ oder $c = b$.

Ist dabei $a \neq b$, so wird $\{a, b\}$ als Zweiermenge bezeichnet.

1.2 Mengenalgebra

In diesem Abschnitt beschäftigen wir uns mit den wichtigsten Beziehungen und Operationen zwischen Mengen. Da es sich dabei (bis auf die Potenzmengenbildung) um Beziehungen und Operationen für Mengen gleicher Stufe handelt, lassen wir die Stufenindizes weg bzw. definieren die Beziehungen und Operationen für Mengen erster Stufe.

Definition 1.2.1 (Inklusion, Teilmengenbeziehung)
Die Menge M heißt *Teilmenge der Menge* N (oder *in* N *enthalten*), (notiert durch $M \subseteq N$), wenn für alle Elemente x gilt:

$$\text{wenn } x \in M, \text{ so } x \in N$$

Die grundlegenden Eigenschaften der Inklusion vermittelt der

Satz 1.2.2
Für beliebige Mengen M, N, L gilt:

1. $M \subseteq M$ (Reflexivität)
   (d. h. die Inklusion ist ein *reflexive Relation*)
2. Wenn $M \subseteq N$ und $N \subseteq L$, so $M \subseteq L$ (Transitivität)
   (d. h. die Inklusion ist eine *transitive* Relation)
3. Wenn $M \subseteq N$ und $N \subseteq M$, so $M = N$ (Antisymetrie)
   (d. h. die Inklusion ist eine antisymetrische Relation).

Den *Beweis* von Satz 1.2.2 führt man durch Rückgang auf die Definition der Inklusion, d. h. man macht diese Definition rückgängig und nimmt logische Umformungen vor. Als Beispiel führen wir den Beweis für Aussage 2 vor.

Aus der Voraussetzung $M \subseteq N$ und $N \subseteq L$ ist $M \subseteq L$ zu beweisen. Wenn wir vereinbaren daß x ein beliebiges Element ist, so ergibt sich nach Einsetzen der Definition der Inklusion, daß folgendes zu beweisen ist:

$$\begin{array}{ll|l} \text{Wenn:} & \text{wenn } x \in M, \text{ so } x \in N & \text{(a)} \\ \text{und} & \text{wenn } x \in N, \text{ so } x \in L & \text{(b)} \\ \hline \text{so:} & \text{wenn } x \in M, \text{ so } x \in L. & \text{(c)} \end{array}$$

Es sei nun $x \in M$. Dann haben wir

$$x \in M \text{und (wenn } x \in M, \text{ so } \in N),$$

folglich haben wir $x \in N$, zusammen mit (b) folgt $x \in L$; wir haben

$$\text{wenn } x \in M, \text{ so } x \in L,$$

d. h. (c). Die Aussage 2 ist damit bewiesen.

Zur Übung beweise man 1 und 3 sowie

Satz 1.2.3
Für alle Mengen M gilt $\emptyset \subseteq M$.

Definition 1.2.4 (echte Inklusion, echte Teilmenge)
Die Menge M wird *echte Teilmenge von* N (oder *in* N *echt enthalten*) (notiert durch $M \subset N$) genannt, wenn $M \subseteq N$ und $M \neq N$ ist.

Man zeigt nun

Satz 1.2.5
Für beliebige Mengen M, N, L gilt

1. $M \not\subset M$ (Irreflexivität)
2. Wenn $M \subset N$ und $N \subset L$, so $M \subset L$ (Transitivität)
3. Wenn $M \subset N$, so $N \not\subset M$ (Asymetrie)

und etwas schärfer

Satz 1.2.6
Für beliebige Mengen M, N, L gilt

1. Wenn $M \subset N$, so $M \subseteq N$
2. $M \subseteq N$ genau dann, wenn $M = N$ oder $M \subset N$
3. Wenn $M \subseteq N$ und $N \subset L$, so $M \subset L$
4. Wenn $M \subseteq N$, so $N \not\subset M$.

Neben den Beweisen der Sätze 1.2.5 und 1.2.6 formuliere man als *Übung* eine Definition der echten Inklusion, in der die Relationen $\subseteq, \neq$ (für Mengen) nicht verwendet werden, d. h. in der nur die Elementbeziehung vorkommt.

Definition 1.2.7 (Durchschnitt, Vereinigung und Komplement)
Es seien M, N beliebige Mengen. Dann ist

1. der *Durchschnitt* $M \cap N$ von M und N die Menge

$$M \cap N =_{\mathrm{Def}} \{x | x \in M \text{ und } x \in N\}$$

2. die *Vereinigung* $M \cup N$ von M und N die Menge

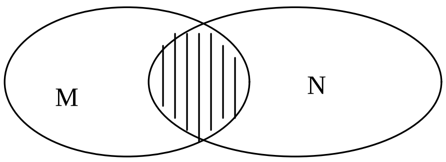
$$M \cup N =_{\mathrm{Def}} \{x | x \in M \text{ oder } x \in N\}$$

3. Das *Komplement* $\overline{M}$ von M die Menge

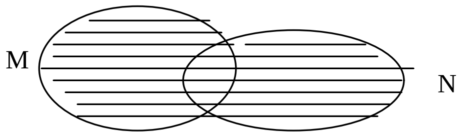
$$\overline{M} =_{\mathrm{Def}} \{x | x \notin M\}\,.$$

In der Definition der Vereinigung ($=_{\mathrm{Def}}$ bedeutet, daß die Mengen nach Definition gleich sind) ist das „oder“ im nicht ausschließenden Sinn zu verstehen (d. h. nicht als „entweder-oder“); zur Vereinigung von M und N gehören also auch die Elemente x, die in beiden Mengen Element sind. Zur Veranschaulichung der Wirkungsweise der Operatoren $\cup$, $\cap$ und $^{-}$ beschaut man sich oft Zeichnungen der folgenden Art:

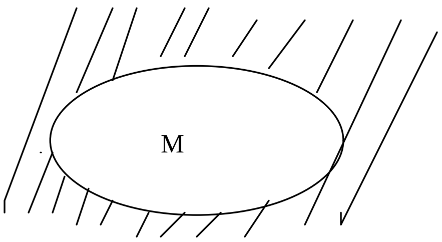
Wenn M die Menge der Punkte innerhalb des mit M bezeichneten Kreises ist und N entsprechend die Menge der Punkte innerhalb des mit N bezeichneten Kreises ist, so gibt die schraffierte Fläche gerade den Durchschnitt $M \cap N$ wieder.



Das entsprechende Bild der Vereinigung sieht so aus:



Und des Komplements so:



Wir formulieren nun eine Reihe von Sätzen über das Rechnen mit den in 1.2.7 definierten sogenannten BOOLEschen Operationen, deren Beweis wir abermals dem Leser überlassen.

Satz 1.2.8
Für beliebige Mengen M, N, L gilt:

1. $M \cap N = N \cap M$, $\quad M \cup N = N \cup M$ (Kommutativität)
2. $(M \cap N) \cap L = (M \cap N) \cap L$, $\quad (M \cup N) \cup L = (M \cup N) \cup L$ (Assoziativität)
3. $M \cap (M \cup N) = M$, $\quad M \cup (M \cap N) = M$ (Absorptionsgesetze)

Bemerkung Eine Menge V, in der zweistellige Operationen $\sqcap$ und $\sqcup$ definiert sind, die beide kommutativ und assoziativ sind und die Absorptionsgesetze erfüllen, wird *Verband* genannt, d. h. wir definieren

Definition 1.2.9
$\mathfrak{V} = [V, \sqcap, \sqcup]$ heißt Verband, wenn V eine Menge ist und:

1. $\sqcap, \sqcup$ zweistellige Operationen über V sind; $\sqcap$ und $\sqcup$ ordnen also jedem $a, b \in V$ je (genau) ein Element $a \sqcap b$, $a \sqcup b \in V$ zu;
2. $\sqcap, \sqcup$ sind kommutativ
3. $\sqcap, \sqcup$ sind assoziativ
4. $\sqcap, \sqcup$ erfüllen die Absorptionsgesetze, d. h. für alle $a, b, \in V$ gilt
$$a \sqcap (a \sqcup b) = a \text{ und } a \sqcup (a \sqcap b) = a.$$

Bezeichnen wir mit $\mathfrak{E}$ das System aller Mengen erster Stufe, so gilt also

Folgerung 1.2.10
$[\mathfrak{E}, \cap, \cup]$ ist ein Verband.

Der Verbandsbegriff ist ein wichtiger algebraischer Grundbegriff. Sein wesentlicher Inhalt besteht in einer Verallgemeinerung der Struktur des Rechnens mit Mengen auf andere Bereiche. Wir werden z. B. sehen, daß auch die Menge der Äquivalenzrelationen (über einer gegebenen Menge) einen Verband bildet, so daß man gewisse Rechnungen mit Äquivalenzklassen so durchführen kann (d. h. nach den gleichen Rechenregeln durchführen kann) als hätte man Mengen vor sich.

Satz 1.2.8 (Fortsetzung)

4. $\begin{array}{rcl} (M \cap N) \cup L & = & (M \cup L) \cap (M \cup L) \\ (M \cup N) \cap L & = & (M \cap L) \cup (M \cap L) \end{array}$ (Rechtsdistributivität)

5. $\emptyset \cap M = \emptyset$ $\quad \emptyset \cup M = M$ ($\emptyset$ ist Nullelement)

6. $E \cap M = M$ $\quad E \cup M = E$ (E ist Einselement)

7. $M \cap \overline{M} = \emptyset$ $\quad M \cup \overline{M} = E$

Bemerkung Aus der Kommutativität und der Rechtsdistributivität folgt unmittelbar die Linksdistributivität, d. h. es gilt

$$\begin{array}{rcl} L \cup (M \cap N) & = & (M \cup L) \cap (M \cup L) \\ L \cap (M \cup N) & = & (M \cap L) \cup (M \cap L) \end{array}$$

Wir sprechen daher künftig nur von der Distributivität. Ein Verband $\mathfrak{V} = [V, \sqcap, \sqcup]$, bei dem die Operationen $\sqcap$ und $\sqcup$ die distributiven Gesetze erfüllen, wird *distributiver Verband* genannt; $[\mathfrak{E}, \cap, \cup]$ ist also ein distributiver Verband.

Die Bezeichnung „Nullelement" bzw. „Einselement" werden klar, wenn man eine Analogie zwischen dem Durchschnitt von Mengen und der Addition von Zahlen herstellt. Diese Analogie geht aber nicht so weit, daß etwa die Menge der natürlichen Zahlen $\mathbb{N}$ mit Multiplikation und Addition einen Verband bildet, offenbar sind die Absorptionsgesetze nicht erfüllt (jedoch ist $[\mathbb{N}, \min, \max]$ ein Verband).

Ein Verband $[V, \sqcap, \sqcup]$, in dem es Elemente $0, 1 \in V$ gibt, so daß (1.2.8.5) und (1.2.8.6) erfüllt sind, wird Verband mit Null und Eins genannt. In jedem Verband gibt es höchstens ein Nullelement und höchstens ein Einselement, so daß bei einem Verband mit Null und Eins von *dem* Nullelement und *dem* Einselement gesprochen werden kann. Man beweist die Einzigkeit des Nullelements wie folgt (analog führt man den Beweis für das Einselement):

Es seien $0, 0' \in V$ mit (5) $0 \sqcap a = 0$ und ($5'$) $0' \sqcap a = 0'$ für alle $a \in V$. Dann gilt:

$$\begin{array}{rcll} 0 & = & 0 \sqcap 0' & \text{(wegen (5) und } a = 0' \in V) \\ & = & 0' \sqcap 0 & \text{(wegen der Kommutativität von } \sqcap) \\ & = & 0' & \text{(wegen (}5'\text{) und } a = 0 \in V) \end{array}$$

also ist $0 = 0'$, was zu zeigen war. Ein Verband $\mathfrak{V} = [V, \sqcap, \sqcup, 0, 1]$ in dem eine dritte einstellige Operation $^-$ definiert ist, die jedem $a \in V$ ein solches Element $\overline{a} \in V$ zuordnet, daß stets $a \sqcap \overline{a} = 0$, $a \sqcup \overline{a} = 1$ heißt *komplementärer Verband.* Ein distributiver komplementärer Verband (mit Null und Eins) wird BOOLEsche Algebra genannt.

Folgerung 1.2.11
$[\mathfrak{C}, \cap, \cup, ^-, \emptyset, E]$ ist eine BOOLEsche Algebra.

Wir können bereits an dieser Stelle eine Folgerung aus unseren verbandstheoretischen Überlegungen ziehen. Aus dem Beweis der Einzigkeit des Nullelements ergibt sich nämlich:

Folgerung 1.2.12
Ist M_0 eine Menge derart, daß für alle Mengen N gilt $M_0 \cap N = \emptyset$, dann ist $M_0 = \emptyset$.

Übung: Wie lautet das Analogon dieser Aussage für die Allmenge E ?

Sieht man sich die Form der bisher aufgeführten Rechenregeln an, so fällt auf, daß man aus jeden Gleichungen durch Vertauschen von $\cap$ und $\cup$ wieder gültige Gleichungen erhällt. In der Tat gilt

Satz 1.2.13 (Dualitätstheorem)
Es sei G eine gültige Gleichung, in der nur Variablen für Mengen, Klammern und die Zeichen $\cap$, $\cup$ vorkommen und G' entsteht aus G, indem an allen Stellen gleichzeitig das Zeichen $\cap$ durch das Zeichen $\cup$ und das Zeichen $\cup$ durch das Zeichen $\cap$ ersetzt wird. Dann ist G' eine gültige Geichung.

Der Beweis für das Dualitätstheorem führen wir im Kapitel 2 mit den dort entwickelten Hilfsmitteln.

Satz 1.2.14
Für beliebige Mengen M, N, L gilt:

1. $M \subseteq N$ gdw. $M \cup N = N$; $M \subseteq N$ gdw. $M \cap N = M$
2. $M \cap M = M$, $M \cup M = M$
3. $M \cap N \subseteq M$, $M \subseteq M \cup N$
4. $M \subseteq N$ und $M \subseteq K$ gdw. $M \subseteq N \cap K$, $M \subseteq K$ und $N \subseteq K$ gdw. $M \cap N \subseteq K$
5. Wenn $M \subseteq N$, so $M \cap L \subseteq N \cap L$ und $M \cup L \subseteq N \cup L$ (Monotonie)
6. Wenn $M \supseteq K$, so $M \cap (n \cup K) = (M \cap N) \cup K$
Wenn $M \subseteq K$, so $M \cup (n \cap K) = (M \cup N) \cap K$ (Modularität)
7. $\overline{\overline{M}} = M$
8. $\overline{M \cap N} = \overline{M} \cup \overline{N}$
$\overline{M \cup N} = \overline{M} \cap \overline{N}$ (DE MORGANsche Formeln)
9. $M \subseteq N$ gdw. $M \cap \overline{N} = \emptyset$ $M \subseteq N$ gdw. $\overline{M} \cup N = E$

Beweis: Die Aussage (1.2.14.1) beweist man durch Rückgang auf die Definitionen, alle übrigen Aussagen gelten in beliebigen BOOLEschen Algebren (sofern dort durch Verwendung von (1.2.14.1) als Definition eine „Inklusion“ zwischen den Verbandselementen definiert ist.

Einige dieser Bewesie geben wir im folgenden an.

Die Aussage (1.2.14.2) ergibt sich aus (1.2.8.3) wie folgt

$$\begin{array}{rcll} M \cap M & = & M \cap [M \cup (M \cap N)] & (\text{wegen } M = M \cup (M \cap N)\,,\ (1.2.8.3)) \\ & = & M \cap [M \cup K] & (\text{für} K = M \cap N\ ) \\ & = & M & (\text{wegen } (1.2.8.3)) \end{array}$$

Zu (1.2.14.3): Es ist

$$\begin{array}{lll} M \cap N \subseteq M \quad \text{gdw.} & (M \cap N) \cup M = M & (\text{wegen } (1.2.14.1)) \\ \qquad\qquad\quad\ \text{gdw} & M \cup (M \cap N) = M & (\text{wegen } (1.2.8.3)) \end{array}$$

und $M = M \cup (M \cap N)$ ist nach (1.2.8.3) wahr.

Zum Beweis von (1.2.14.4) zeigen wir zuerst:

$$\text{wenn } M \subseteq N \text{ und } M \subseteq K, \text{ so } M \subseteq N \cap K.$$

Aus $M \subseteq N$, $M \subseteq K$ ergibt sich mit (1.2.14.1)

$$M \cap N = M \quad \text{und} \quad M \cap K = M,$$

Woraus nach (1.2.14.2) folgt

$$\begin{array}{rcll} M = M \cap M & = & (M \cap N) \cap (M \cap K) & \\ & = & (M \cap M) \cap (N \cap K) & (\text{wegen } (1.2.8.3), (1.2.8.2)) \\ & = & M \cap (N \cap K) & (\text{wegen } (1.2.14.2)) \end{array}$$

also gilt nach (1.2.14.1) auch $M \subseteq N \cap K$.

Ist umgekehrt $M \subseteq N \cap K$, d. h. $M = M \cap (N \cap K)$, so gilt nach (1.2.14.3) und (1.2.8.2)

$$M = (M \cap N) \cap K \subseteq M \cap N$$

Andererseits ist $M \cap N \subseteq M$ (1.2.14.3), folglich gilt bei $L = M \cap N$

$$L \subseteq M \quad \text{und} \quad M \subseteq L.$$

Aus (1.2.14.1) ergibt sich nun mit (1.2.8.3) $L = L \cap M = M \cap L = M$ d. h. $M = M \cap N$, folglich $M \supseteq N$. Analog zeigt man $M \subseteq K$.

Die Beweise für die Aussagen (1.2.14.5) und (1.2.14.6) übergehen wir und beweisen nun (1.2.14.7).

Wegen (1.2.8.7) gilt

$$\overline{M} \cap \overline{\overline{M}} = \emptyset$$

folglich ist $M = M \cup \emptyset = M \cup \left(\overline{M} \cap \overline{\overline{M}}\right)$ nach (1.2.8.5)

Mit (1.2.8.4) erhalten wir

$$M = (M \cup \overline{M}) \cap \left(\overline{M} \cap \overline{\overline{M}}\right)$$

d. h. über (1.2.8.6)

$$M = E \cap \left(M \cup \overline{\overline{M}}\right) = M \cup \overline{\overline{M}}$$

Auf die gleiche Weise leitet man aus $\overline{M} \cap \overline{\overline{M}} = E$ her, daß

$$M = M \cap \overline{\overline{M}}$$

ist, woraus

$$\overline{\overline{M}} = \overline{\overline{M}} \cup \left(\overline{\overline{M}} \cap M\right) = \overline{\overline{M}} \cup M = M,$$

d. h. (1.2.14.7) folgt.

Übung: Man führe die übrigen Beweise von Satz 1.2.14

Definition 1.2.15 (Differenz und symetrische Differenz)
Die Differenz $M \setminus N$ der Mengen M, N ist die Menge

$$M \setminus N =_{\text{Def}} \{x | x \in M \text{ und } x \notin N\}$$

Die symetrische Differenz $M \triangle N$ der Mengen M, N ist die Menge

$$M \triangle N =_{\text{Def}} \{x | \text{ entweder } x \in M \text{ oder } x \in N\}$$

Einige Regeln für das Rechnen mit Differenz bzw. symetrischer Differenz geben die beiden folgenden Sätze wider, deren Beweis wir dem Leser überlassen.

Satz 1.2.16
Für beliebige Mengen M, N gilt

1. $M \setminus N = M \cap \overline{N}$
2. $E \setminus M = \overline{M}$
3. $M \setminus \emptyset = M$
4. $M \subseteq N$ gdw. $M \setminus N = \emptyset$
5. Wenn $M \cap N = \emptyset$, so $M \setminus N = M$ und $N \setminus M = N$.

Satz 1.2.17
Für beliebige Mengen M, N gilt:

1. $M \triangle N = \left(M \cap \overline{N}\right) \cup \left(\overline{M} \cap N\right)$
2. $M \triangle N = (M \cup N) \cap \overline{(M \cap N)} = (M \cup N) \setminus (M \cap N)$
3. $M \triangle N = N \triangle M$ (Kommutativität)
4. $(M \triangle N) \triangle K = N \triangle (M \triangle K)$ (Assoziativität)
5. $M \triangle \emptyset = M$ ($\emptyset$ ist Nullelement)
6. $M \triangle N = \emptyset$ gdw. $M = N$
7. $M \cap (M \triangle K) = (M \cap N) \triangle (M \cap K)$

Bemerkung: Ist in einer Menge G eine zweistellige assoziative Operation $\square$ definiert, so nennt man $[G, \square]$ eine *Halbgruppe*. Die Aussage (1.2.17.4) besagt also, daß $[\mathfrak{E}, \triangle]$ eine Halbgruppe ist, wegen (1.2.17.3) handelt es sich sogar um eine *kommutative Halbgruppe*. In dieser Halbgruppe ist $\emptyset$ das Nullelement. Eine kommutative Halbgruppe $[G, \square, 0]$ mit Null wird ABELsche (oder *kommutative*) *Gruppe* genannt, wenn zu jedem $g \in G$ (genau) ein $g' \in G$ mit $g \square g' = 0$ existiert. Wegen (1.2.17.6) ist also $[\mathfrak{E}, \triangle, \emptyset]$ eine ABELsche Gruppe. Ebenso wie der Verbandbegriff spielt der Gruppenbegriff eine bedeutende Rolle in der Mathematik und ihren Anwendungen.

Definition 1.2.18 (Allgemeiner Durchschnitt, Allgemeine Vereinigung)
Es sei $\mathfrak{M} \in \mathfrak{E}$ ein beliebiges Mengensystem. Der allgemeine Durchschnit von $\mathfrak{M}$ ist die Menge

$$\bigcap \mathfrak{M} =_{\text{Def}} \{x|\text{ für alle } M \in \mathfrak{M} \text{ ist } x \in M\}\,.$$

Die allgemeine Vereinigung von $\mathfrak{M}$ ist die Menge

$$\bigcup \mathfrak{M} =_{\text{Def}} \{x|\text{ es gibt ein } M \in \mathfrak{M} \text{ mit } x \in M\}\,.$$

Die Operationen „allgemeiner Durchschnitt“ und „ allgemeine Vereinigung“ führen also von Mengensystemen zu Mengen, verringern also die Stufe.

Satz 1.2.19
Es sei $\mathfrak{M}, \mathfrak{N} \subseteq \mathfrak{E}$

1. $\bigcap \emptyset^{(2)} = E$
2. $\bigcup \emptyset^{(2)} = \emptyset$
3. $(\bigcup \mathfrak{M}) \cap N = \bigcup \{M \cap N | M \in \mathfrak{M}\}$
4. $(\bigcap \mathfrak{M}) \cup N = \bigcap \{M \cup N | M \in \mathfrak{M}\}$
5. $\bigcap \mathfrak{M} \cap \bigcap \mathfrak{N} = \bigcap \{\mathfrak{M} \cup \mathfrak{N}\}$
6. $\bigcup \mathfrak{M} \cap \bigcup \mathfrak{N} = \bigcup \{\mathfrak{M} \cup \mathfrak{N}\}$
7. $\overline{\bigcap \mathfrak{M}} = \bigcup \{\overline{M} | M \in \mathfrak{M}\}$

Definition 1.2.20 (Potenzmenge)
Die Potenzmenge $\mathfrak{P}(M)$ der Menge M ist das System aller Teilmengen von M, d. h.

$$\mathfrak{P}(M) =_{\text{Def}} \{N | N \subseteq M\}$$

Die Potenzmengenbildung führt also von einer Menge zu einem Mengensystem, sie hebt die Stufe an. Es gilt der

Satz 1.2.21
Für beliebige Mengen M, N gilt:

1. $\mathfrak{P}(\emptyset) = \{\emptyset\}$
2. $\mathfrak{P}(E) = \mathfrak{E}$
3. $M \subseteq N$ gdw. $\mathfrak{P}(M) \subseteq \mathfrak{P}(N)$
4. $\mathfrak{P}(M \cup N) \supseteq \mathfrak{P}(M) \cup \mathfrak{P}(N)$
5. $\mathfrak{P}(M \cap N) = \mathfrak{P}(M) \cap \mathfrak{P}(N)$
6. $\mathfrak{P}(\overline{M}) \subseteq \{\emptyset\} \cup \overline{\mathfrak{P}(M)}$

1.3 Korrespondenzen, Relationen, Abbildungen

Unser nächstes Ziel besteht darin, den Begriff der Zuordnung mathematisch, d. h. mengentheoretisch, zu präsentieren. Wenn wir davon gesprochen haben, daß eine zweistellige Operation $\Box$ je zwei Elementen a, b einer Menge G ein Element $a \Box b$ aus G eindeutig zuordnet, so haben wir dabei an die Anschauung appelliert, aber nicht gesagt, was Zuordnen eigentlich ist.

Der einfachste Fall einer Zuordnung liegt vor, wenn einem einzigen Element a ein Element b zugeordnet ist, was man z. B. durch $[a, b]$ notieren kann. Die erste Komponente dieses sogenannten *geordneten Paares*, das Element a, wird in einen Zusammenhang gesetzt mit der zweiten Komponente, dem Element b; dem a wird das b zugeordnet und nicht umgekehrt — es kommt also auf die Reihenfolge der Komponenten (Elemente) an. Für geordnete Paare $[a, b]$, $[c, d]$ muß also gelten

$$[a, b] = [c, d] \text{ gdw. } a = c \text{ und } b = d$$

Diese Eigenschaft ist die grundlegende Eigenschaft geordneter Paar, sie kann zur axiomatischen Charakterisierung dieses Begriffs verwendet werden. Wir können aber diesen Begriff mengentheoretisch wie folgt definieren:

Definition 1.3.1
Es seien a, b beliebige Elemente. Dann ist das geordnete Paar $[a, b]$ das Mengensystem

$$[a, b] =_{\text{Def}} \{\{a\}, \{a, b\}\}.$$

Man kann nun beweisen

Satz 1.3.2
Für beliebige Elemente a, b, c, d gilt

$$[a, b] = [c, d] \text{ gdw. } a = c \text{ und } b = d.$$

Durch wiederholte Paarbildung kann man nun den Begriff des geordneten Tripels, Quadrupels, ...(allgemein:) den des n-Tupels einführen. Dazu überträgt man die Definition 1.3.1 von Elementen a, b auf beliebige Mengen a, b gleicher Stufe und definiert dann:

Definition 1.3.3
Es seien $a, b, c, d, a_1, a_2, \cdots$ beliebige Elemente.

- $[a, b, c] =_{\text{Def}} [[a, b], \{\{c\}\}]$ (Tripel)
- $[a, b, c, d] =_{\text{Def}} [[a, b, c], \{\{\{\{c\}\}\}\}]$ (Quadrupel)

  $\vdots$ $\vdots$
- $[a_1, \ldots, a_n] =_{\text{Def}} [[a_1, \ldots, a_n], \underbrace{\{\cdots\{}_{2(n-2)} a_n \underbrace{\}\cdots\}}_{2(n-2)}]$ (n-Tupel)

Man zeigt durch Induktion über $n \geq 2$:

Satz 1.3.4
$[a_1, \ldots, a_n] = [b_1, \ldots, b_n]$ gdw. $a_1 = b_1$ und ...und $a_n = b_n$.

Einfachste Zuordnungen der Form „a geht über in b“ können wir also durch das geordnete Paar $[a, b]$ beschreiben, kompliziertere Zuordnungen werden wir durch Mengen geordneter Paare beschreiben.

Definition 1.3.5
Es seien $M_1, M_2, \ldots, M_n$ Mengen (gleicher Stufe). Das CARTESische Produkt (direktes Produkt, Kreuzprodukt) von $M_1, \ldots, M_n$ in dieser Reihenfolgen) ist die Menge

$$M_1 \times M_2 =_{\text{Def}} \{[a,b]\,|a \in M_1 \text{ und } b \in M_2\}\,.$$

bzw.

$$M_1 \times \cdots \times M_n =_{\text{Def}} \{[a,\ldots,a_n]\,|a \in M_1 \text{ und } \ldots \text{und } a_n \in M_n\}\,.$$

Nach dieser Definition kann das CARTESische Produkt nur zwischen Mengen gleicher Stufe gebildet werden. Man braucht aber auch Produkte zwischen Mengen verschiedener Stufen, z. B. wenn man eine Zuordnung beschreiben will, die jedem Element eine gewisse Menge zuordnet. Eine Definition läßt sich ebenfalls angeben, wir verzichten hier darauf und gehen im folgenden davon aus, daß für beliebige Mengen N, K das Kreuzprodukt definiert ist. Wichtige Eigenschaften des Produkts formulieren wir als

Satz 1.3.6

1. $M \times N = \emptyset$ gdw. $M = \emptyset$ oder $N = \emptyset$
2. Wenn $M \subseteq N$, so $M \times K \subseteq N \times K$ und $K \times M \subseteq K \times N$.
3. $M \times (N \cup K) = (M \times N) \cup (M \times K)$
4. $M \times (N \cap K) = (M \times N) \cap (M \times K)$

Wir sind nun in der Lage, den Begriff der Zuordnung, wir sagen „Korrespondenz“ mengentheoretisch zu definieren:

Definition 1.3.7
Es seien M, N Mengen. Dann wird K eine Korrespondenz aus M in N (bzw. zwischen M und N) genannt, wenn $K \subseteq M \times N$ ist.

Beispiele

1. Es sei $M = N = \mathbb{N}$ (die Menge der natürlichen Zahlen) und
$$\leq \;=\; \{[a,b]\,|a,b \in \mathbb{N} \text{ und } a \text{ kleiner oder gleich } b\} \subseteq \mathbb{N} \times \mathbb{N}$$
2. Es sei $M = \mathbb{N}$, $N = \{\text{wahr}, \text{falsch}\}$ (die Menge der Wahrheitswerte) und
$$\begin{aligned} P_2 \;=\; & \{[a,\alpha]\,|a \in \mathbb{N} \text{ und entweder } [a \text{ ist keine Primzahl und } \alpha = \text{falsch}] \\ & \text{oder } [\alpha \text{ ist Primzahl und } \alpha = \text{wahr}]\} \end{aligned}$$
3. Es sei $M = \{1,\ldots,99\}$, N die Menge aller Straßennamen in Berlin und
$$\begin{aligned} F \;=\; & \{[a,x]\,|a \in M \text{ und } x \in N \text{ und die Straßenbahnlinie Nr.} a \text{ führt} \\ & \text{durch die Straße } x\} \end{aligned}$$

Ist K eine Korrespondenz, so schreiben wir für $[a,b] \in K$ auch aKb und sagen dafür „a steht zu b in Korrespondenz K“ oder „b ist ein K-Bild von a“ oder „a ist ein K-Urbild von b“. Unser Beispiel 1 zeigt, daß ein Element im allgemeinen mehrere Bilder oder Urbilder haben kann; Beispiel 3 zeigt, daß ein Element kein Bild bzw. Urbild haben muß.

Definition 1.3.8
Es sei $K \subseteq M \times N$ eine Korrespondenz zwischen M und N.

1. Der Definitionsbereich (Argumentenbereich, Vorbereich) von K ist die Menge D_K der Elemente von M, die K-Urbilder eines Elementes von N sind, d. h.
$$D_K =_{\text{Def}} \{a | \text{ Es gibt ein } b \text{ mit } [a,b] \in K\}$$
2. Der Bildbereich (Wertebereich, Nachbereich) von K ist die Menge B_K der Elemente von N, die K-Bild eines Elementes von M sind, d. h.
$$B_K =_{\text{Def}} \{b | \text{ Es gibt ein } a \text{ mit } [a,b] \in K\}$$
3. K heißt Korrespondenz *von* M in N, wenn $D_K = M$ ist
4. K heißt Korrespondenz aus M *auf* N, wenn $B_K = M$ ist
5. K heißt Korrespondenz *von* M *auf* N, wenn $D_K = M$ ist und $B_K = N$ ist.
6. Die Korrespondenz K wird eindeutig genannt, wenn zu jedem $a \in M$ höchstens ein $b \in M$ (eventuell keines) mit $[a,b] \in K$ existiert.
7. Die Korrespondenz K wird eindeutig umkehrbar genannt, wenn es zu jedem $b \in N$ höchstens ein $a \in M$ mit $[a,b] \in K$ gibt

Die Korrespondenzen $\leq$ und P_2 sind Korrespondenzen *von–auf*, bei F ist das nicht der Fall; ferner ist P_2 eindeutig, aber nicht eindeutig umkehrbar.

Definition 1.3.9
Es seien K und L Korrespondenzen, $K \subseteq A \times B$, $L \subseteq C \times D$.

1. Die Verkettung $K \circ L$ von K mit L ist die Menge
$$K \circ L =_{\text{Def}} \{[a,d] \mid \text{Es gibt ein } b \text{ mit } [a,b] \in K \text{ und } [b,d] \in L\}$$
2. Die Inversion K^{-1} von K ist die Menge
$$K^{-1} =_{\text{Def}} \{[b,a] \mid [a,b] \in K\}$$

Die Identität über dem Objektbereich E bezeichnen wir mit I_E, d. h.
$$I_E =_{\text{Def}} \{[a,a] \,|a \in E\}$$

Man zeigt nun:

Satz 1.3.10
Es seien $K \subseteq A \times B$, $L \subseteq C \times D$ Korrespondenzen.

1. $K \circ L$ ist eine Korrespondenz zwischen A und D
2. Die Verkettung ist eine assoziative Operation
3. I_E ist neutrales Element, d. h. $K \circ I_E = I_E \circ K = K$
4. $K \circ L = \emptyset$ genau dann, wenn $B_K \cap D_L = \emptyset$.
5. K^{-1} ist eine Korrespondenz zwischen B und A

6. $\left(K^{-1}\right)^{-1} = K$
7. $(K \circ L)^{-1} = L^{-1} \circ K^{-1}$.

Korrespondenzen aus einer Menge A in diese Menge selbst, werden als Relationen bezeichnet:

Definition 1.3.11
R wird binäre (zweistellige) Relation in A genannt, wenn $R \subseteq A \times A$ ist. Ist dabei $D_R \cup B_R = A$, so heißt R Relation *über* A.

Es ist also $\leq$ eine Relation über $\mathbb{N}$, ferner I_E eine Relation über E, die leere Menge $\emptyset^{(3)}$ dritter Stufe ist eine Relation in jeder Menge erster Stufe und $A \times A$ ist eine Relation über A (die Allrelation über A).

Wie wir später sehen werden, spielen reflexive und transitive Relationen in der Mathematik eine große Rolle — Äquivalenzrelationen und reflexive Ordnungsrelationen haben diese Eigenschaften. Deshalb interessiert eine Operation, die (ausgehend von einer Relation ohne diese Eigenschaften) die bezüglich $\subseteq$ kleinste reflexive und transitive Relation R' mit $R \subseteq R'$ als Resultat liefert.

Definition 1.3.12 (reflexiv-transitive Hülle)
Es sei R eine Relation *über* A. Wir setzen

- $R^0 = I_A$
- $R^{i+1} = R^i \circ R$
- $\langle R \rangle =_{\text{Def}} \bigcup \{R^0, R^1, \ldots\} = \bigcup_{i \in \mathbb{N}} R^i$

Die Menge $\langle R \rangle$ wird als reflexiv-transitive Hülle von R bezeichnet.

Man überlegt sich sofort

Satz 1.3.13
Es sei R Relation über A

1. $\langle R \rangle$ ist eine Relation über A
2. $\langle R \rangle$ ist reflexiv über A, d. h. für alle $a \in A$ gilt $a \langle R \rangle a$
3. $\langle R \rangle$ ist transitiv über A, d. h. für alle $a, b, c \in A$ gilt wenn $a \langle R \rangle b$, $b \langle R \rangle c$, so $a \langle R \rangle c$.

Beweis Für (1.3.13.1) ist zu zeigen $\langle R \rangle \subseteq A \times A$ und $D_{\langle R \rangle} = A$, woraus $D_{\langle R \rangle} \cup B_{\langle R \rangle} = A$ folgt. Offensichtlich gilt (1.3.13.2), weil $I_A \subseteq \langle R \rangle$ ist. Wir beweisen nun (1.3.13.3). Wegen $a \langle R \rangle b$, $b \langle R \rangle c$ gibt es Zahlen $i, j \geq 0$ mit $aR^i b$, $bR^j c$. Bei $i = 0$ folgt $a = b$, also $aR^j c$, d. h. $a \langle R \rangle c$. Analog schließt man bei $j = 0$. Sei $i > 0$. Man überlegt sich (durch Induktion über i) daß in diesem Fall Elemente $a_1, \ldots, a_{i+1} \in A$ existieren mit $a_1 = a$, $a_{i+1} = b$ und $a_l R a_{l+1}$ für $l = 1, \ldots, a_{i+1}$. Analog existieren Elemente $b_1, \ldots, b_{j+1}$ mit $b_1 = b$, $b_{j+1} = c$ und $b_k R b_{k+1}$ für $k = 1, \ldots, j$. Daraus folgt $[a, c] \in R^{i+j} \subseteq \langle R \rangle$, d. h. $a \langle R \rangle c$.

Der Gebrauch der Bezeichnung „Hülle“ ist in der Mathemetik für solche Operatonen reserviert, die die sogenannten Hülleneigenschaften haben:

Satz 1.3.14
Die Operation $\langle \rangle$ hat die Hülleneigenschaften, d. h. es gilt

1. $R \subseteq \langle R \rangle$ (Satz der Einbettung)
2. Wenn $R_1 \subseteq R_2$, so $\langle R_1 \rangle \subseteq \langle R_2 \rangle$ (Satz der Monotonie)
3. $\langle \langle R \rangle \rangle = \langle R \rangle$ (Satz der Abgeschlossenheit)

Überdies erfüllt die Operation $\langle \rangle$ den Endlichkeitssatz:

4. Wenn $[a, b] \in \langle R \rangle$, so existiert eine endliche Teilmenge $R' \subseteq R$ mit $[a, b] \in \langle R' \rangle$.

Den Beweis überlassen wir dem Leser als Übung. Ferner gilt der bereits oben erwähnte

Satz 1.3.15
Es sei R eine Relation über A. Dann ist $\langle R \rangle$ die bezüglich $\subseteq$ kleinste reflexive und transitive Relation R' mit $R \subseteq R'$, d. h. für alle Relationen R' über A gilt: Wenn $R \subseteq R'$ und R' ist reflexiv und transitiv, so ist $\langle R \rangle \subseteq R'$.

Beweis Daß $\langle R \rangle$ reflexiv und transitiv ist, sagt Satz 1.3.13. Aus (1.3.14.1) haben wir $R \subseteq \langle R \rangle$. Ist $R \subseteq R'$, so ist $\langle R \rangle \subseteq \langle R' \rangle$ wegen der Monotonie. Für reflexive und transitive Relationen R' gilt aber $R' = \langle R' \rangle$, denn aus der Reflexivität von R' über A folgt
$R^0 = I_A \subseteq R'$ und aus der Transitivität von R' folgt $R' \circ R' = R'$, d. h. $(R')^i \subseteq R'$. Also ist $\langle R \rangle \subseteq \langle R' \rangle = R'$.

In analoger Weise wie zweistellige Korrespondenzen definiert man n-stellige Korrespondenzen zwischen Mengen $M_1, \ldots, M_n$ und n-stellige Relationen R in A als

$$R \subseteq A \times \cdots \times A = \bigtimes_n A.$$

Wir wenden uns nun dem Begriff der *Abbildung* zu.

Definition 1.3.16
Es seien A, B Mengen

1. f heißt Abbildung von A in B, wenn
   (a) F eine Korrespondenz von A in B und
   (b) F eindeutig ist.
2. Eine Abbildung F wird *surjektiv* genannt (oder Abbildung *auf* B), wenn $B_f = B$ ist.
3. Eine Abbildung F heißt *injektiv* (oder umkehrbar eindeutig), wenn F eindeutig umkehrbar ist.
4. Eine Abbildung F heißt *bijektiv*, wenn F surjektiv und injektiv ist.

Die oben angegebene Korrespondenz P_2 ist also eine surjektive Abbildung von $\mathbb{N}$ auf $\{$wahr, falsch$\}$.

Die Aussage „f ist eine Abbildung von A in B“ notieren wir künftig durch „$f : A \rightarrow B$“ und statt „$[a, b] \in F$“ schreiben wir „$b = f(a)$“.

Zum Abschluß dieses Paragraphen machen wir eine Bemerkung über die *Beschreibung von Korrespondenzen durch Abbildungen*. Dabei verwenden wir, daß das Kreuzprodukt auch zwischen Mengen unterschiedlicher Stufen definiert ist.

Es sei $K \subseteq A \times B$ eine Korrespondenz zwischen A und B. Die zu K gehörige Abbildung f_K ist definiert durch

$$F_K : A \rightarrow \mathfrak{P}(B)$$

mit

$$f_K(a) =_{\mathrm{Def}} \{b | [a,b] \in K\}$$

für alle $a \in A$.

Offenbar kann K aus einer Kenntnis von f_K gewonnen werden (ist durch f_K eindeutig bestimmt), denn es gilt:

$$K = \bigcup_{a \in A} \{a\} \times f_k(a) = \bigcup \{\{a\} \times f_K(a) | a \in A\}$$

Da die Beziehung zwischen K undf_K also eineindeutig ist, kann man wirklich von einer *Beschreibung* sprechen; Beschreibung (f_K) und Beschriebenes (K) entsprechen einander eineindeutig.

1.4 Äquivalenzrelationen

Definition 1.4.1
Eine Relation $R \subseteq A \times A$ in A heißt Äquivalenzrelation über A, wenn

1. R eine reflexive Relation über A ist
2. R symetrisch ist, d. h. $[a,b] \in R$ stets $[b,a] \in R$ impliziert (m.a.W $R = R^{-1}$ ist)
3. R transitiv ist.

Bemerkung: Von der Forderung (1.4.1.1) ist nur wesentlich, daß R eine Relation über A ist, denn aus der Symmetrie folgt $D_R = B_R$, d. h. wir haben $A = D_R \cup B_R = D_R = B_R$. Ist nun $a \in A$, so gibt es ein $b \in A$ mit $[a,b] \in R$ (wegen $a \in D_R$) und $[b,a] \in R$ (wegen (1.4.1.2)) woraus mit der Transitivität $[a,a] \in R$ folgt, d. h. R ist reflexiv.

Für jede Menge A ist offenbar I_A eine Äquivalenzrelation über A, und zwar ist I_A in dem Sinne die schärfste (bzw. feinste) Äquivalenzrelation über A, daß I_A die meisten Unterschiede zwischen Elementen von A macht. Im allgemeinen nennt man ja Elemente äquivalent bzw. gleichwertig in gewisser Hinsicht, wenn sie sich in dieser Hinsicht nicht unterscheiden, z. B. gleich verhalten. Wenn es z. B. auf Zeit, Kosten, Bequemlichkeit usw. bei einer beabsichtigten Reise nicht ankommt, sondern nur auf den Ortswechsel, so ist es gleichwertig, äquivalent, ob dazu das Flugzeug oder die Bahn benutzt wird. Objekte in Äquivalenz zu setzen, bedeutet also, von gewissen ihrer Eigenschaften abzusehen (zu abstrahieren) und andere gemeinsame Eigenschaften hervorzuheben. Aus dieser Rolle bei der Abstraktion, der Bildung neuer Begriffe, leitet sich die Bedeutung des Begriffs der Äquivalenzrelation ab.

Wir betrachten nun die oben definierte Abbildung f_R für den Fall, daß R eine Äquivalenzrelation über A ist. Man zeigt leicht:

Satz 1.4.2
Es sei R eine Äquivalenzrelation über A und $a, b \in A$. Dann gilt:

1. $a \in f_R(a) \neq \emptyset$
2. $a \in f_R(b)$ genau dann, wenn $b \in f_R(a)$
3. Wenn $f_R(a) \cap f_R(b) \neq \emptyset$, so $f_R(a) = f_R(b)$.

Definition 1.4.3
Es sei A eine Menge, $A \neq \emptyset$, $\mathfrak{M} \subseteq \mathfrak{P}(A)$. $\mathfrak{M}$ heißt Zerlegung von A (Klasseneinteilung von A), wenn gilt

1. $\emptyset \notin \mathfrak{M}$
2. $A = \bigcup \mathfrak{M}$
3. $\mathfrak{M}$ ist disjunkt, d. h. für alle $M, M' \in \mathfrak{M}$ gilt: wenn $M \cap M' \neq \emptyset$, so $M = M'$.

Mit Hilfe des Begriffes der Zerlegung können wir den Satz 1.4.2 wie folgt formulieren.

Satz 1.4.2′
Ist R eine Äquivalenzrelation über $A \neq \emptyset$, so ist

$$\mathfrak{M}_R =_{\mathrm{Def}} \{f_R(a) \mid a \in A\} = B_{f_R}$$

eine Zerlegung von A.

Wir wissen bereits, daß wir eine Relation R durch die Abbildung f_R beschreiben können. Es stellt sich die Frage, ob bei Äquivalenzrelationen R dazu bereits $\mathfrak{M}_R = B_{f_R}$ genügt. Es zeigt sich zunächst:

Satz 1.4.4
Ist R eine Äquivalenzrelation über A, so gilt für $a, b \in A$: aRb genau dann, wenn es ein $M \in \mathfrak{M}_R$ mit $a, b \in M$ gibt.

Diese Aussage weist den Weg, wie zu einer Zerlegung $\mathfrak{M}$ eine Äquivalenzrelation $R_{\mathfrak{M}}$ zu definieren ist; wir setzen für $a, b \in A = \bigcup \mathfrak{M}$

$$aR_{\mathfrak{M}}b \text{ gdw. es ein } M \in \mathfrak{M} \text{ mit } a, b \in M \text{ gibt.}$$

Man zeigt ohne Schwierigkeiten:

Satz 1.4.5
Ist $\mathfrak{M}$ eine Zerlegung von A, so ist $R_{\mathfrak{M}}$ Äquivalenzrelation über A.

Die Bildung von $R_{\mathfrak{M}}$ zu einer Zerlegung $\mathfrak{M}$ erweist sich nun gerade als Umkehrung der Bildung der Zerlegung $\mathfrak{M}_R$ zu einer Äquivalenzrelation R.

Satz 1.4.6
Es sei $A \neq \emptyset$

1. Ist R eine Äquivalezrelation über A, so ist
$$R = R_{(\mathfrak{M}_R)}$$
2. Ist $\mathfrak{M}$ eine Zerlegung von A, so ist
$$\mathfrak{M} = \mathfrak{M}_{(R_{\mathfrak{M}})}$$

Äquivalenzrelationen und Zerlegungen sind einander auf diese Weise eindeutig zugeordnet. Man bezeichnet

$f_R(a)$ als die Äquivalenzklasse nach R, in der a liegt (die Äquivalenzklasse von a)

und notiert $\mathfrak{M}_R$ auch als A/R (A zerlegt nach R, A faktorisiert nach R). Wichtig ist der Fall, daß in der Menge A neben der der Äquivalenzrelation R noch weitere Relationen und Operationen, d. h. Abbildungen definiert sind, die mit R „verträglich" sind. Man nennt dann R eine Kongruenzrelation bzgl. diesen Operationen und Relationen. Wichtig ist dieser Fall deshalb, weil sich dann Relationen bzw. Operationen auf A auf dem einfacheren Bereich A/R nachbilden lassen. Wir führen das genauer aus für den Fall einer n-stelligen Operation über A.

Definition 1.4.7
Es sei A eine nichtleere Menge , $n \geq 1$.

1. $\circ$ heißt n-stellige Operation über A, wenn
$$\circ : \bigtimes_n A \rightarrow A$$
2. Eine Äquivalenzrelation R über A heißt verträglich (invariant) bzgl. der n-stelligen Operation $\circ$ über A (oder Kongruenzrelation bzgl. $\circ$), wenn für alle $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ gilt: Wenn $a_1 R b_1$ und ... und $a_n R b_n$, so $\circ(a_1, \ldots, a_n)\, R \circ (b_1, \ldots, b_n)$.

Ist nun R eine Kongruenzrelation über A bzgl. $\circ$, so können wir für $M_1, \ldots, M_n \in A/R$ definieren

$$\circ'(M_1, \cdots M_n) =_{\mathrm{Def}} f_R(\circ(a_1, \ldots, a_n))$$

für beliebiges $a_1, \ldots a_n$ mit $a_1 \in M_1$ und ...und $a_n \in M_n$.

Diese Definition muß gerechtfertigt werden, d. h. es ist zu zeigen: Wenn $[a_1, \ldots, a_n] \in M_1 \times \cdots \times M_n$ und $[b_1, \ldots b_n] \in M_1 \times \cdots \times M_n$, so

$$f_R(\circ(a_1, \ldots, a_n)) = f_R(\circ(b_1, \ldots, b_n))\,.$$

Das ergibt sich daraus, das R Kongruenz bzgl. $\circ$ ist, denn aus $a_i, b_i \in M_i \in A/R$ folgt $a_i R b_i$, also $\circ(a_1, \ldots a_n)\, R \circ (b_1, \ldots, b_n)$, folglich $f_R(\circ(a_1, \ldots, a_n)) = f_R(\circ(b_1, \ldots, b_n))$. Es ergibt sich also, daß folgendes Diagramm „kommutativ" ist

$$\begin{array}{ccccc} A & \times\cdots\times & A & \stackrel{\circ}{\rightarrow} & A \\ {\scriptstyle f_R}\downarrow & & {\scriptstyle f_R}\downarrow & & {\scriptstyle f_R}\downarrow \\ (A/R) & \times\cdots\times & (A/R) & \stackrel{\circ'}{\rightarrow} & A/R \end{array}$$

„kommutativ" bedeutet, daß man ausgehend von einer Element $[a_1, \ldots, a_n] \in \bigtimes_n A$ das gleiche Element von A/R erhält, unabhängig davon, ob man zuerst mittels $\circ$ das Element $\circ(a_1, \ldots, a_n]$ bildet und dann f_R anwendet oder zuerst mittels f_R das Element $[f_R(a_1), \ldots, f_R(a_n)] \in \bigtimes_n (A/R)$ bildet und dann $\circ'$ anwendet. Die „Abstrahierende" Abbildung f_R einer Kongruenz R liefert also zugleich eine Vereinfachung A/R des Bereichs A (z. B. kann A/R endlich sein während A unendlich ist) und eine Vereinfachung der Operation $\circ$.

1.5 Natürliche Zahlen

In diesem Abschnitt beschäftigen wir uns mit der mengentheoretischen Begründung der natürlichen Zahlen. Wir haben diesen Begriff bisher im wesentlichen nur in Beispielen benutzen können (nicht z. B. in Definitionen), denn wir haben ihn bisher nicht definiert. Insbesondere ist noch nicht klar, ob die Menge der natürlichen Zahlen überhaupt existiert, oder ob sie vielleicht sogar zu einer Antinomie führt.

Wir geben zunächst (als weiteres Beispiel einer axiomatische Charakterisierung) eine axiomatische Charakterisierung der natürlichen Zahlen, genauer der Grundbegriffe „Null", „Menge aller natürlichen Zahlen" und „die natürliche Zahl b ist unmittelbarer Nachfolger der natürlichen Zahl a" an, die wir formal durch x_0, X, $a\mathrm{Nf}b$ notieren wollen. Das PEANOsche Axiomensytem hat die folgende Gestalt:

1. $x_0 \in X$ (lies: Null ist eine natürliche Zahl)
2. Zu jedem $a \in X$ gibt es genau ein $b \in X$ mit $a\mathrm{Nf}b$
3. Es gibt kein $a \in X$ mit $a\mathrm{Nf}x_0$
4. Für alle $a, b, c \in X$ gilt: Wenn $a\mathrm{Nf}c$ und $b\mathrm{Nf}c$, so $a = b$
5. Für alle $M \subseteq X$ gilt: Wenn $x_0 \in M$ und (für alle $a \in M$ und jedes b mit $a\mathrm{Nf}b$ gilt $b \in M$), so ist $X \subseteq M$.

Ein Modell dieses Axiomensystems P ist ein Tripel $[\alpha, A, R]$, bestehend aus einem konkreten mathematischen Objekt α, einer Menge N von Objekten und einer Relation R über N, derart daß diese fünf Axiome erfüllt sind. Das Tripel $[0, \mathbb{N}, R^\star]$ mit $aR^\star b$ gdw. $b = a+1$ erfüllt offenbar das PEANOsche Axiomensystem; man kann sogar zeigen, daß jedes Modell von P zu diesem Tripel isomorph ist.

Wenn wir gesagt haben, daß $[0, \mathbb{N}, R^\star]$ P erfüllt, so setzt daß natürlich voraus, daß sich die in diesem Tripel vorkommenden Objekte 0, $\mathbb{N}$, $R^\star$ mathematisch (mengentheoretisch) als existent begründen lassen.

Den Zugang zur Einführung des Zahlenbegriffs bildet der Begriff der Gleichzahligkeit, der Gleichmächtigkeit. Das Gemeinsame einer Menge von drei Äpfeln mit einer Menge von drei Stühlen oder drei Flaschen, so daß man sagen kann die Drei, das ist das Mengensystem, in dem genau alle Mengen mit genau drei Elementen vorkommen. Nun kann man aber von einer Menge schwer feststellen, ob sie genau drei Elemente hat, ohne die drei Elemente zu zählen, es sei denn, es ist einem schon eine Menge bekannt, die genau drei Elemente enthält. Dann ist es auch anschaulich klar, daß zwei Mengen dann und nur dann gleich viele Elemente besitzen, wenn es eine Bijektion (eine eineindeutige Abbildung *von-auf*) zwischen diesen Mengen gibt.

Definition 1.5.1
Mengen A, B heißen gleichmächtig (oder äquivalent, notiert durch $A \sim B$), wenn es eine Bijektion $\Phi : A \to B$ gibt.

Man überlegt sich leicht:

Satz 1.5.2
$\sim$ ist eine Äquivalenzrelation über $\mathfrak{C}$

Definition 1.5.3
Die Äquivalenzklassen von $\mathfrak{C}$ nach $\sim$, d. h. die Elemente von $\mathfrak{C}/\sim$ heißen Kardinalzahlen (von Mengen erster Stufe). Es ist für $M \in \mathfrak{C}$

$$\mathrm{card}\,(M) = \{N | N \in \mathfrak{C} \text{ und } N \sim M\}$$

Eine Kardinalzahl ist also ein nichtleeres Mengensystem, das alle Mengen enthält, die zu einer Menge dieses Systems gleichmächtig sind. Unserer Anschauung entspricht es, die natürlichen Zahlen als Kardinalzahlen der endlichen Mengen einzuführen. Wir müssen also dazu den Begriff der endlichen Menge klären, ohne dabei den Zahlenbegriff zu benutzen. Die Erklärung „M ist genau dann endlich, wenn es Elemente $a_1, a_2, \ldots, a_n$ so gibt, daß $M = \{a_1, \ldots, a_n\}$ ist“, ist also als Endlichkeitsdefinition nicht brauchbar.

Definition 1.5.4 (Russel)

1. Das System $\mathfrak{M}_{\text{fin}}$ der endlichen Mengen ist das kleinste Mengensystem $\mathfrak{M}$ mit
   (a) $\emptyset \in \mathfrak{M}$ (Anfangsschritt)
   (b) Ist $M \in \mathfrak{M}$ und $a \in E$, so $(M \cup \{a\}) \in \mathfrak{M}$ (Induktionschritt)
2. M heißt endlich, wenn $M \in \mathfrak{M}_{\text{fin}}$ ist (unendlich sonst)

Das *Unendlichkeitsaxiom* sagt also: $E \notin \mathfrak{M}_{\text{fin}}$.

Eine weitere Endlichkeits- bzw. Unendlichkeitsdefinition wurde von Dedekind angegeben.

Definition 1.5.5 (Dedekind)

1. Eine Menge M heißt „endlich“, wenn sie nicht „unendlich“ ist.
2. Eine Menge M heißt „unendlich“, wenn es eine echte Teilmenge $M' \subset M$ mit $M' \sim M$ gibt.

Diese Definition beruht auf der Beobachtung, daß nur unendliche Mengen zu einer ihrer echten Teilmengen äquivalent sind. So ist z. B. Die Menge $\mathbb{N}$ ist äquivalent mit der Menge der geraden natürlichen Zahlen, eine Bijektion $\Phi : \mathbb{N} \to \{0, 2, 4, \ldots\}$ ist gegeben durch die Gleichung $\Phi(x) = 2x$. Wir beweisen, daß beide Definitionen gleichwertig sind.

Satz 1.5.6
Eine Menge M ist endlich genau dann, wenn sie „endlich“ ist.

Beweis

1. Jede endliche Menge ist „endlich“, d. h. Wenn $M \in \mathfrak{M}_{\text{fin}}$, so gilt für jede echte Teilmenge $M' \subset M$: $M' \not\sim M$. Wir beweisen diese Behauptung durch Induktion über M

   Anfangsschritt $M = \emptyset$: Die Behauptung ist trivial, weil die leere Menge keine echten Teilmengen besitzt.

   Induktionsschritt:

   Vor.: Für jede echte Teilmenge M' von M ist $M' \not\sim M$

   Beh.: Für jede echte Teilmenge N' von $M \cup \{a\}$ ist $N' \not\sim M \cup \{a\}$

Wenn $a \in M$ ist, so gilt $M \cup \{a\} = M$, die Behauptung ist mit der Voraussetzung identisch. Es sei also $a \notin M$.

Wir schließen indirekt, und nehmen an, daß

$$N' \subset M \cup \{a\} \ , \ N' \sim M \cup \{a\} .$$

Es sei $\Phi : N' \to M \cup \{a\}$ bijektiv. Wir setzen

$$N'' =_{\mathrm{Def}} N' \setminus \left\{\Phi^{-1}(a)\right\} \ , \ \Phi' =_{\mathrm{Def}} \Phi \setminus \left\{\left[\Phi^{-1}(a), a\right]\right\}$$

und erhalten

$$\Phi' : N'' \to M \text{ ist bijektiv}$$

also $N'' \sim M$.

Fall 1: Ist nun $a \notin N''$, so gilt wegen

$$N'' = N' \setminus \left\{\Phi^{-1}(a)\right\} \subset N' \subset M \cup \{a\} ,$$

die Inklusion $N'' \subseteq M$, aus $N'' \sim M$ folgt nach Induktionsvoraussetzung $N'' = M$, folglich $\Phi^{-1}(a) = a$, d. h. $N' = M \cup \{a\}$ im Widerspruch zu $N' \subset M \cup \{a\}$.

Fall 2: Betrachten wir nun den Fall $a \in N''$. Es sei $b =_{\mathrm{Def}} \Phi'(a) \in M$ und $c =_{\mathrm{Def}} \Phi^{-1}(a)$, sowie

$$\Psi(x) =_{\mathrm{Def}} \begin{cases} a & \text{für} \quad x = a \\ b & \text{für} \quad x = c \\ \Phi(x) & \text{für} \quad x \in N' \setminus \{a, c\} \end{cases}$$

ferner $N''' = (N'' \setminus \{a\} \cup \{c\})$. Dabei ist $N''' \sim N'' \sim M$ und $a \notin N''' \subset N' \subset M \cup \{a\}$, also $N''' \subseteq M$, woraus nach Induktionsvoraussetzung $N''' = M$ folgt. Wegen $N' = N''' \cup \{a\} = M \cup \{a\}$ erghalten wir abermals einem Widerspruch zu $N' \subset M \cup \{a\}$. Damit ist die Aussage 1 bewiesen.

2. Jede „endliche“ Menge M ist endlich, d. h. $M \in \mathfrak{M}_{\mathrm{fin}}$.

   Wir führen den Beweis indirekt und nehmen an, daß M_0 eine Menge ist, mit

   (a) Wenn $M' \subset M_0$, so $M' \not\sim M$

   (b) $M_0 \notin \mathfrak{M}_{\mathrm{fin}}$.

   Dann gibt es zu jedem $N \in \mathfrak{M}_{\mathrm{fin}}$ mit $N \subseteq M_0$ ein $a \in M_0$ mit $a \notin N$, d. h. $M_0 \setminus N \neq \emptyset$ für alle $N \in \mathfrak{M}_{\mathrm{fin}}$ mit $N \subseteq M_0$. Wir setzen

   $$\mathfrak{M}^\star =_{\mathrm{Def}} \{M_0 \setminus N | N \subseteq M_0 \text{und } N \in \mathfrak{M}_{\mathrm{fin}}\}$$

   Es ist $\emptyset \notin \mathfrak{M}^\star$ weil $M \notin \mathfrak{M}_{\mathrm{fin}}$ und $\mathfrak{M}^\star \neq \emptyset$ weil $M_0 = M_0 \setminus \emptyset \in \mathfrak{M}^\star$.

   Eine gleichwertige Formulierung des Auswahlaxioms lautet:

   > Zu jedem nichtleeren Mengensystem $\mathfrak{M}$ nichtleerer Mengen existiert eine Auswahlfunktion, d. h. eine Abbildung $\rho : \mathfrak{M} \to \bigcup \mathfrak{M}$ mit $\rho(M) \in M$ für alle $M \in \mathfrak{M}$.

Es sei ρ eine Auswahlfunktion für $\mathfrak{M}^\star$, wir setzen

$$\begin{aligned} a_0 &= \rho(M_0) \\ a_{i+1} &= \rho(M_0 \setminus \{a_0, a_1, \ldots, a_i\}) \quad i = 0, 1, 2, \ldots \end{aligned}$$

Offenbar ist $\{a_0, \ldots, a_i\} \in \mathfrak{M}_{\text{fin}}$, also $M_0 \setminus \{a_0, \ldots a_i\} \in \mathfrak{M}^\star$. Dabei sind für jedes i die Elemente $a_0, \ldots a_i$ offenbar paarweise verschieden. Es sei schließlich

$$\begin{aligned} M^\star &= \{a_0, a_1, \ldots\} \\ M^{\star\star} &= \{a_1, a_2, \ldots\} \end{aligned}$$

Offenbar ist $M^\star \sim M^{\star\star}$. Ferner ist $M_0 = M^\star \cup (M_0 \setminus M^\star)$ und für $M' =_{\text{Def}} M^{\star\star} \cup (M_0 \setminus M^\star)$ gilt $M' \subset M_0$, aber es ist $M' \sim M_0$, wie man leicht sieht. Das ist ein Widerspruch zur Voraussetzung 1.

Folgerung 1.5.7
Eine Menge ist „unendlich" genau dann, wenn sie unendlich ist.

Definition 1.5.8

1. n ist eine natürliche Zahl. wenn n die Kardinalzahl einer endlichen Menge ist.
2. $0 = \text{card}(\emptyset) = \{\emptyset\}$
3. $\mathbb{N} := \mathfrak{M}_{\text{fin}}/\sim$
4. Für natürliche Zahlen n, m definieren wir die Nachfolgerelation Nf

   $n\text{Nf}m :\leftrightarrow$ Es gibt ein $N \in n$ und $a \in E$ mit $a \notin N$ und $N \cup \{a\} \in m$.

Satz 1.5.9
Das Tripel $[0, \mathbb{N}, \text{Nf}]$ ist ein Modell des Peanoschen Axiomensystems.

Wir führen den Beweis nicht aus, merken lediglich an, daß man zum Nachweis der Existenz des Nachfolgers einer natürlichen Zahl (vgl Axiom 2) das Unendlichkeitaxiom braucht.

Ist nämlich $n \in \mathbb{N}$, etwa $n = \text{card}(N)$ wobei $N \in \mathfrak{M}_{\text{fin}}$, so ist zu zeigen, daß ein $a \in E$ mit $a \notin N$ existiert.

Gäbe es ein solches a nicht, so hätte man $E \subseteq N$, also $E = M$, d. h. $E = N \in \mathfrak{M}_{\text{fin}}$, im Widerspruch zum Unendlichkeitsaxiom.

Definition 1.5.10
Es seien m, n beliebige Kardinalzahlen. Wir setzen $m \leq n$ gdw. es Mengen $M \in n$, $N \in n$ und eine Injektion $\Phi : M \rightarrow N$gibt.

Satz 1.5.11
$[\mathfrak{C}/\sim, \leq]$ ist eine reflexive Ordnung, d. h. für beliebige Kardinalzahlen m, n, k gilt:

1. $m \leq m$
2. Wenn $m \leq n$ und $n \leq k$, so $m \leq k$
3. Wenn $m \leq n$ und $n \leq m$, so $m = n$
4. $m \leq n$ oder $n \leq m$

Die Behauptungen 1 und 2 sind leicht einzusehen. Wir beweisen hier nur die Antisymetrie von $\leq$ in Form des Bernsteinschen Äquivalenzsatzes:

Sind M, N Mengen und ist $\Phi : M \to N$ injektiv, sowie $\Psi : N \to M$ injektiv, so ist $M \sim N$.

Zur Vorbereitung zeigen wir:

Lemma 1.5.12
Es sei M eine beliebige Menge und $f : \mathfrak{P}(M) \to \mathfrak{P}(M)$ mit: Wenn $A, B \subseteq M$ und $A \subseteq B$, so $f(A) \subseteq f(B)$. Dann hat F einen Fixpunkt C, d. h. es gibt eine Menge $C \subseteq M$ mit

$$f(C) = C$$

Beweis Es sei

$$\begin{aligned} \mathfrak{A} &=_{\text{Def}} \{A \mid A \subseteq M \text{und } A \subseteq f(A)\} \\ C &=_{\text{Def}} \bigcup \mathfrak{A}. \end{aligned}$$

Zum Beweis von $C = f(C)$ zeigen wir zuerst

$$C \subseteq f(C).$$

Es sei $x \in C$ beliebig. Dann gibt es ein $A \in \mathfrak{A}$ mit $x \in A$. Wegen $A \subseteq f(A)$ ist $x \in f(A)$, ferner ist $A \subseteq C$. Aus der Monotonie von F ergibt sich $X \in f(A) \subseteq f(C)$, also $x \in f(C)$.

Aus $C \subseteq f(C)$ folgt $f(C) \subseteq f(f(C))$, also ist $f(C) \in \mathfrak{A}$, d. h. $f(C) \subseteq \bigcup \mathfrak{N} = C$. Damit ist das Lemma 1.5.12 bewiesen.

Es seien nun M, N, Φ, Ψ mit den angegebenen Eigenschaften gegeben. Wir betrachten die Abbildung $f : \mathfrak{P}(M) \to \mathfrak{P}(M)$ mit:

$$f(X) =_{\text{Def}} M \setminus \overline{\Psi}\left(N \setminus \overline{\Phi}(X)\right)$$

für $X \subseteq M$, wobei

$$\begin{aligned} \overline{\Phi}(X) &= \{\Phi(x) \mid x \in X\} \quad \text{für} \quad X \subseteq M \\ \overline{\Psi}(Y) &= \{\Psi(y) \mid y \in Y\} \quad \text{für} \quad Y \subseteq N \end{aligned}$$

gesetzt ist.

Wir zeigen zunächst, daß F monoton ist. Ist $A \subseteq B \subseteq M$, so $\overline{\Phi}(A) \subseteq \overline{\Phi}(B) \subseteq \overline{\Phi}(M) \subseteq N$, folglich $N \setminus \overline{\Phi}(A) \supseteq N \setminus \overline{\Phi}(B)$ und also

$$M \supseteq \overline{\Psi}\left(N \setminus \overline{\Phi}(A)\right) \supseteq \overline{\Psi}\left(N \setminus \overline{\Phi}(B)\right),$$

so daß

$$f(A) = M \setminus \overline{\Psi}\left(N \setminus \overline{\Phi}(A)\right) \subseteq M \setminus \overline{\Psi}\left(N \setminus \overline{\Phi}(B)\right) = f(B)$$

folgt.

Nach Lemma 1.5.12 besitzt F einen Fixpunkt C. Wir setzen nun für $x \in M$

$$\tau(x) =_{\text{Def}} \begin{cases} \Phi(x), & \text{falls } x \in C \\ \Psi^{-1}(x), & \text{falls } x \notin C \end{cases}$$

und zeigen, daß $\tau : M \to N$ bijektiv ist.

1. τ ist injektiv (eineindeutig)

   Die Eindeutigkeit von τ ist offensichtlich, es genügt also zu zeigen:

   $$\text{Wenn } \tau(x_1) = \tau(x_2), \text{ so } x_1 = x_2$$

   In den Fällen, daß $x_1, x_2 \in C$ oder $x_1, x_2 \in M \setminus C$ ist, folgt das unmittelbar aus der Eineindeutigkeit von Φ bzw. Ψ^{-1} Es sei o.B.d.A. $x_1 \in C$, $x_2 \notin C$. Dann ist

   $$y =_{\text{Def}} \tau(x_1) = \Phi(x_1) \in N \text{und } y = \tau(x_2) = \Psi^{-1}(x_2)$$

   Wegen $x_1 \in C$ ist $y = \Phi(x_1) \in \overline{\Phi}(C)$. Andererseits ist $\Psi(y) = x_2 \notin C$, also $x_2 \notin f(C) = M \setminus \overline{\Psi}\left(N \setminus \overline{\Phi}(C)\right)$, folglich $x_2 \in \overline{\Psi}\left(N \setminus \overline{\Phi}(C)\right)$ wegen $x_2 \in M$.

   Es gibt also ein $y' \in N \setminus \overline{\Phi}(C)$ mit $x_2 = \Psi(y')$. Weil Ψ eineindeutig ist, folgt aus $\Psi(y) = x_2 = \Psi(y')$, daß $y = y'$ ist. Das steht im Widerspruch zu $y \in \overline{\Phi}(C)$, $y' \notin \overline{\Phi}(C)$. Der Fall $x_1 \in C$, $x_2 \notin C$ kann also nicht eintreten.

2. τ ist Abbildung auf N.

   Es sei $y \in N$ beliebig. Wenn $x =_{\text{Def}} \Psi(y) \notin C$, so ist $\tau(x) = \Psi^{-1}(x) = y$, es ist also y ein Wert von τ. Andernfalls ist $x \in C = f(C) = M \setminus \overline{\Psi}\left(N \setminus \overline{\Phi}(C)\right)$. Folglich ist $x \in M$ und $x \notin \overline{\Psi}\left(N \setminus \overline{\Phi}(C)\right)$. Wir zeigen, daß in diesem Fall $y \in \overline{\Phi}(C)$ ist. Sonst währe nämlich $y \in N \setminus \overline{\Phi}(C)$, also $x = \Psi(y) \in \overline{\Psi}\left(N \setminus \overline{\Phi}(C)\right)$. Widerspruch. Aus $y \in \overline{\Phi}(C)$ ergibt sich die Existenz eines $x' \in C$ mit $y = \Phi(x')$. Nun ist wegen $x' \in C$

   $$\tau(x') = \Phi(x') = y,$$

   also triff y auch in diesem Fall als Wert von τ auf. Damit ist der BERNSTEINsche Äquivalenzsatz bewiesen.

Man kann zeigen:

Satz 1.5.13
Für beliebige Kardinalzahlen m, n gilt: $m \leq n$ genau dann, wenn es Mengen $M \in \mathfrak{M}$, $N \in \mathfrak{N}$ und eine surjektive Abbildung $\Phi : N \to M$ gibt.

Definition 1.5.14
Eine Menge M heißt abzählbar unendlich, wenn sie gleichmächtig mit $\mathbb{N}$ ist. Ist M unendlich und $M \not\sim \mathbb{N}$, so wird M überabzählbar genannt.

Die Kardinalzahl der Menge $\mathbb{N}$ wird mit $\aleph_0$ (Aleph Null) bezeichnet, dies ist die kleinste unendliche Kardinalzahl. Überabzählbar ist z. B. die Menge aller Folgen von Nullen und Einsen, d. h. die Menge $M_1 = \{\Phi | \Phi : \mathbb{N} \to \{0, 1\}\}$, diese Menge hat die gleiche Mächtigkeit wie die Menge der reellen Zahlen im Intervall $[0, 1]$ bzw. wie die Menge aller reellen Zahlen. Die Kardinalzahl dieser Menge wird mit $\aleph$ (Aleph) bezeichnet, es ist also $\aleph_0 < \aleph$.

Definition 1.5.15
Für Kardinalzahlen m, n sei

$$m + n =_{\text{Def}} \text{card}\,(M \cup \mathbb{N})$$

für beliebiges $M \in n, N \in n$ mit $M \cap N = \emptyset$ und

$$m \cdot n =_{\text{Def}} \text{card}\,(M \times N)$$

für beliebiges $M \in m, N \in n$.

Man zeigt ohne Schwierigkeiten, daß diese Definitionen vom Repräsentanten unabhängig sind, d. h. daß gilt:

1. Wenn $M \sim M'$, $N \sim N'$, $M \cap N = \emptyset$, $M' \cap N' = \emptyset$, so $\operatorname{card}(M \cup N) = \operatorname{card}(M' \cup N')$.
2. Wenn $M \sim M'$, $N \sim N'$, so $\operatorname{card}(M \times N) = \operatorname{card}(M' \times N')$.

Für natürliche Zahlen gelten dabei natürlich die üblichen Rechenregeln, das ist bei unendlichen Kardinalzahlen nicht der Fall, man verifiziert z. B. leicht, daß $\aleph_0 + \aleph_0 = \aleph_0$ ist. Es gilt aber z. B.

Satz 1.5.16
Es ist für beliebige Kardinalzahlen m, n: $m \leq n$ genau dann, wenn es eine Kardinalzahl k mit $m + k = n$ gibt.

Übungsaufgaben

1. Man führe die in diesem Manuskript offen gebliebenen Beweise.
2. $A \cup (B \setminus C) = ((A \cap B) \setminus C) \cup (A \cap C)$
3. $A \cap B = A \setminus (A \setminus B)$
4. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$
5. $(A \times B) \setminus (C \times D) = ((A \setminus C) \times B) \cup (A \times (B \setminus D))$
6. Es sei $f : R_1 \times R_2 \to R_1 \times R_2$ (R_1 = die Menge der reellen Zahlen) mit $f(x, y) = [x + y, x - y]$. Man untersuche, ob f surjektiv, injektiv bzw. bijektiv ist.
7. Es seien $f : X \to Y$, $g_1, g_2 : Y \to X$ mit
$$f \circ g_1 = f \circ g_2 = I_Y \,, \, g_1 \circ f = I_X \,.$$
man beweise: $g_1 = g_2$.
8. Es sei $\mathcal{Z}$ die Menge der ganzen Zahlen und
$$R = \{[[a, b]\,, [c, d]] \,|a, b, c, d \in \mathcal{Z}, \;\; b, d \neq 0, ad = bc\}$$
Man zeige, daß R eine Äquivalenzrelation ist und charakterisiere die Äquivalenzklassen.

1.6 Wörter

In diesem Abschnitt beschäftigen wir uns mit einer Verallgemeinerung der natürlichen Zahlen — den Wörtern. Wörter spielen in der Informatik eine große Rolle, sie bilden die Grundlage für den Begriff der Sprache, also für den Kalkülbegriff einerseits und für Programmiersprachen andererseits. Die rechentechnische Realisierung erfolgt je nach Anwendungsbereich durch die Datentypen String (Zeichenkette) als ARRAY OF CHARACTER oder durch den Datentyp Liste (wenn die Länge der betrachteten Ketten unbeschränkt ist). Wörter werden als endliche Folgen von Buchstaben (= Elementen eines endlichen Alphabets) verstanden.

Definition 1.6.1

1. Ein Alphabet X ist eine endliche, nichtleere Menge (die Elemente nennt man Buchstaben).
2. p ist ein Wort über X, wenn p eine endliche Folge von Elementen von X ist, d. h. es gibt eine natürliche Zahl n, so daß $p : \{0, \ldots, n-1\} \to X$.
3. Das Wort $e : \emptyset \to X$ heißt das leere Wort.
4. Die Zahl n wird als Länge $l(p)$ des Wortes p bezeichnet.
5. $W(X)$ bezeichnet die Menge aller Wörter über X.

Wir haben $l : W(X) \to \mathbb{N}$. Die Abbildung l ist nicht umkehrbar, falls $\operatorname{card}(X) \geq 2$.

Um die Menge $W(X)$ zu einer Algebra zu machen, definieren wir eine Operation auf $W(X)$:

Definition 1.6.2 (Verkettung)
Es sei $p : \{0, \ldots, n-1\} \to X$, $q : \{0, \ldots, m-1\} \to X$. Dann ist die Verkettung von p mit q die Abbildung $p^\frown q : \{0, \ldots, m+n-1\} \to X$ mit

$$p^\frown q(i) := \begin{cases} p(i), & i \leq n-1 \\ q(i-n), & n \leq i \leq m+n-1. \end{cases}$$

Was hat diese Operation für Eigenschaften?

Satz 1.6.3
$[W(X), ^\frown, e]$ ist eine Halbgruppe mit dem Einselement e.

Beweis: Man rechnet leicht nach:

1. $p^\frown(q^\frown r) = (p^\frown q)^\frown r$
2. $p^\frown e = p = e^\frown p$ für jedes $p \in W(X)$.

Übungsaufgabe Wir kennen bereits folgende Halbgruppe: $[\mathbb{N}, +, 0]$. Frage: Haben beide etwas Gemeinsames? Sind beide homomorph? (Standardfrage in der Mathematik in solchem Fall)

Definition 1.6.4
f ist Homomorphismus von der Halbgruppe $[M, \circ, 1]$ in $[N, \cdot, 1]$ wenn gilt:

1. $f : M \to N$
2. $f(1_M) = 1_N$
3. $f(m_1 \circ m_2) = f(m_1) \cdot f(m_2)$

Ist f überdies bijektiv, so heißt f Isomorphismus.

Folgerung 1.6.5
l ist ein Homomorphismus von $[W(X), ^\frown, e]$ auf $[\mathbb{N}, +, 0]$.

Bemerkung: Wenn $\operatorname{card}(X) = 1$, so ist l umkehrbar eindeutig, (folglich bijektiv). Mit anderen Worten, die Halbgruppen $[\mathbb{N}, +, 0]$ und $[W(\{a\}), ^\frown, e]$ sind isomorph.

Wir werden die Schreibweise vereinfachen, indem wir Struktureigenschaften benutzen (z. B. Erzeugendes Element)

Definition 1.6.6
E ist Erzeugendensystem für $[W(X), ^\frown, e]$, wenn:

1. $e \notin E \subseteq W(X)$
2. Zu jedem $p \in W(X) \backslash \{e\}$ gibt es Elemente $r_1, \ldots, r_k \in E$ mit $p = r_1^\frown r_2^\frown \ldots ^\frown r_k$.

Man sucht natürlich einfache Elemente als erzeugende Elemente. Hierfür bieten sich Buchstaben an (sie sind keine Wörter! Deshalb:) Für $x \in X$ sei $\underline{x} =_{\text{Def}} \{[0, x]\}$ — Wort der Länge 1.

Damit haben wir die Buchstaben auf das Nivau Wort gebracht. Später werden wir $\underline{x}$ und x identifizieren.

Satz 1.6.7
$\underline{X} =_{\text{Def}} \{\underline{x} | x \in X\}$ ist ein Erzeugendensystem für $[W(X), ^\frown, e]$.

Beweis $p \in W(X); p : \{0, \ldots, n-1\} \to X$. Offenbar ist $p = \underline{p(0)}^\frown \underline{p(1)}^\frown \ldots ^\frown \underline{p(n-1)}$, da $p(i) \in X$.

Beispiel:

1. $[\mathbb{N}^+, \cdot, 1]$ ist eine Halbgruppe. Erzeugendensystem ist Pz – die Menge der Primzahlen, z. B. $6 = 2 \cdot 3 = 3 \cdot 2$
2. $[\mathbb{N}, +, 0]$ ist Halbgruppe. Erzeugendensystem ist $\{1\}$, z. B. $3 = 1 + 1 + 1$.

Unterschied zwischen beiden Halbgruppen ist, daß die Elemente in 1 in mehreren Weisen erzeugbar und in 2 nur auf einer Weise. Die Erzeugung von 2 ist frei von nichttrivalen Gleichungen.

Definition 1.6.8
$G = [M, \cdot, 1, E]$ sei eine Halbgruppe mit Erzeugendensystem E. G heißt frei erzeugt (frei von nichttrivialen Gleichungen), wenn aus $m_1 \cdot m_2 \cdot \cdots \cdot m_k = m'_1 \cdot m'_2 \cdots m'_n$ stets $k = n$ und $m_1 = m'_1, \ldots, m_k = m'_k$ folgt (für $m_i, m'_i \in E$).

Folgerung 1.6.9
$[W(X), ^\frown, e, \underline{X}]$ ist freie Halbgruppe.

Satz 1.6.10
Alle freien Halbgruppen mit derselben Zahl von erzeugenden Elementen sind isomorph.

Beweis: Idee: Erzeugende Elemente sind nicht zerlegbar. Erzeugende aufeinander abbilden. Seien $[M_1, \circ_1, 1, E_1]$, $[M_2, \circ_2, \underline{1}, E_2]$ Halbgruppen, $\text{card}(E_1) = \text{card}(E_2)$.

Es sei $f : E_1 \to E_2$ bijektiv. Weiter definiert man den Homomorphismus folgendermaßen: $f(1) = \underline{1}$. Sei $m \in M_1$. m besitzt genau eine Darstellung $m = r_1 \circ_1 r_2 \circ_1 \cdots \circ_1 r_k$ $(r_i \in E_1)$. Dann sei $f(m) := f(r_1) \circ_2 f(r_2) \circ_2 \cdots \circ_2 f(r_k)$. Daß f ein Homomorphismus ist, ist klar.

Es bleibt zu zeigen, daß f bijektiv ist, d. h. daß f eine umkehrbare Abbildung auf M_2 ist.

Es sei $m' \in M_2$. Wenn $m' = \underline{1}$, so besitzt m' das Urbild $\underline{1} \in M_1$ wegen $f(\underline{1}) = \underline{1}$. Für $m \in M_1 \setminus \{\underline{1}\}$ ist $f(m) \neq \underline{1} \in M_2$, weil anderenfalls aus der Darstellung

$$m = r_1 \circ_1 r_2 \circ_1 \cdots \circ_1 r_k \quad (r_i \in E_1)$$

von m in M_1 eine Darstellung

$$1 = f(m) = f(r_1) \circ_2 \cdots \circ_2 f(r_k) \quad (f(r_i) \in E_2) \tag{1.6.1}$$

des Einselements in M_2 gewonnen würde im Widerspruch dazu, daß $[M_2, \circ_2, 1, E_2]$ frei ist (3.6.2 wäre eine nichttriviale Gleichung). Also ist $1 \in M_1$ das einzige Urbild von $\underline{1} \in M_2$.

Ist $m' \in M_2 \setminus \{\underline{1}\}$, dann sei

$$m' = r_1' \circ_2 \cdots \circ_2 r_k' \quad (r_i' \in E_2)$$

die Darstellung von m' aus Erzeugenden. Da f bijektiv von E_1 auf E_2 ist, gibt es eindeutig bestimmte $r_i \in E_1$ mit $f(r_i) = r_i'$ und

$$m = r_1 \circ_1 \cdots \circ_1 r_k$$

ist ein Element von M_1 mit $f(m) = m'$. Man überlegt sich wie oben, daß m eindeutig bestimmt ist.

Merke: Eine Abbildung $f : X \to Y$ induziert immer einen Homomorphismus von $[W(X), \circ, e]$ auf $[W(Y), ^\frown, e]$ Allgemein kann man sogar schreiben $f : X \to W(Y)$.

Folgerung 1.6.11
Jede freie Halbgruppe mit endlichen Erzeugendensystem ist isomorph zu einer Worthalbgruppe.

$[\mathbb{N}, +, 0, \{1\}]$ ist eine Halbgruppe mit genau einem Erzeugenden und ist isomorph zu $\left[W(\{/\}), ^\frown, e, \left\{\underline{/}\right\}\right]$. $[\mathbb{N}, +, 0, \{1\}]$ ist kommutativ, also $\left[W(\{/\}), 1, e, \left\{\underline{/}\right\}\right]$ auch; folglich ist jede freie Halbgruppe mit genau einem Erzeugenden kommutativ.

Es ist bekannt, daß man bei der Übermittlung von Nachrichten mit 2 Zeichen auskommen kann (z. B. Computer: $0, 1$). Frage, warum nicht mit einem Zeichen? Der Grund liegt in der Kommutativität, denn es gibt Halbgruppen, die nicht kommutativ sind.

Satz 1.6.12 (Hauptsatz der Codierungstheorie)
In der freien Halbgruppe $[W\{a, b\}, ^\frown, e, \{a, b\}]$ mit genau zwei Erzeugenden existiert zu jedem $k \geq 1$ eine freie Unterhalbgruppe mit genau k Erzeugenden.

Beweis: Sei k gegeben. $E_k =_{\text{Def}} \{a \underbrace{b}_{1} a, \ldots, a \underbrace{b \ldots b}_{k} a\}$ Sei $E_k^\star$ die Menge aller Wörter, die durch endlich oftmaliges Verketten von Elementen aus E_k entstehen. $H_k = [E_k^\star, ^\frown, e, E_k]$ ist frei.

1.6.1 Induktive Beweise in $[W(X), ^\frown, e, X]$

Beispiel $[\mathbb{N}, +, 0, \{1\}]$. Um zu zeigen, daß eine Aussage $H(n)$ für alle n aus $\mathbb{N}$ gilt, genügt es zu zeigen:

A) $H(0)$

I) Wenn $H(n)$, so $H(n+1)$.

Wir verallgemeinern diese Aussage für Halbgruppen mit beliebigem Erzeugendensystem:

Induktionstheorem: Um zu zeigen, daß eine Aussage H auf alle Elemente p einer Halbgruppe $[M, \circ, 1, E]$ mit dem Erzeugendensysthem E zutrifft, genügt es zu zeigen

A) $H(1)$

I) Für alle Erzeugenden x gilt: Wenn $H(r)$ und $x \in E$, so $H(r \circ x)$
(bzw: Wenn $H(r)$ und $x \in E$, so $H(x \circ r)$)

Beweis des Induktionstheorems erfolgt indirekt.

Nehmen wir an, daß es Elemente $q \in M$ gibt, auf die H nicht zutrifft. Unter diesen Elementen kommt das Einselement nicht vor, weil $H(1)$ gilt (Anfangsschritt). Jedes dieser Elemente besitzt also eine Darstellung

$$q = q_1 \circ q_2 \circ \cdots \circ q_k$$

aus Erzeugenden $q_i \in E$. Es sei $q^\star$ ein Element mit einer kürzesten Darstellung

$$q^\star = q_1^\star \circ \cdots \circ q_{k^\star}^\star \quad (k^\star \text{ minimal}).$$

Wir setzen $q^{\star\star} = q_1^\star \circ \cdots \circ q_{k^\star-1}^\star$ falls $k^\star \geq 2$ und $q^{\star\star} = 1$ falls $k^\star = 1$. Wegen der Minimalität von $k^\star$ gilt $H(q^{\star\star})$ und es ist

$$q^\star = q^{\star\star} \circ q_k^\star, \quad q_{k^\star}^\star \in E$$

Aus I) erhalten wir damit $H(q^\star)$; Widerspruch.

Auch das Prinzip der Ordnungstheoretischen Induktion kann auf (freie) Halbgruppen übertragen werden:

Ordnungstheoretische Induktion in $[\mathbb{N}, \leq]$: Um zu zeigen, daß eine Aussage H für alle $n \in \mathbb{N}$ gilt g. z. z.: Wenn H auf alle $k < n$ zutrifft, so trifft H auf n zu.

Definition 1.6.13 (Halbordnung in $W(X)$)

1. $p \underline{\text{in}}\, q \leftrightarrow_{\text{Def}}$ es gibt Wörter r, s mit $q = rps$
2. $p \sqsubseteq q$ (p ist Anfangsstück von q) $\leftrightarrow_{\text{Def}}$ Es gibt s mit $q = ps$
3. $p \sqsupseteq q$ (p ist Endstück von q) $\leftrightarrow_{\text{Def}}$ Es gibt r mit $q = rp$

Satz 1.6.14
$[W(X), \underline{\text{in}}]$, $[W(X), \sqsubseteq]$, $[W(X), \sqsupseteq]$ sind reflexive Halbordnungen.

Beweis

- reflexiv: $p\, \underline{\text{in}}\, p$ $(r, s = e)$
- transitiv: $p\, \underline{\text{in}}\, q$ und $q\, \underline{\text{in}}\, r$, so $p \in q$
- antisymetrisch: $p\, \underline{\text{in}}\, q$ und $q\, \underline{\text{in}}\, p$ so $p = q$

Folgerung 1.6.15
Wenn $p\, \underline{\text{in}}\, q$ so $l(p) \leq l(q)$.
Wenn $p \sqsubseteq q$ so $l(p) \leq l(q)$.
Wenn $p \sqsupseteq q$ so $l(p) \leq l(q)$.

Satz 1.6.16 (Ordnungstheoretische Induktion in $W(X)$)
Um zu zeigen, daß eine Aussage H auf alle $p \in W(X)$ zutrifft, genügt es zu zeigen, daß für alle p gilt:

> Wenn für alle r mit $r \;\underline{\text{in}}\; p$ (bzw. $r \sqsubseteq p$ bzw. $r \sqsupseteq p$) und $r \neq p$ stets $H(r)$ gilt, so gilt $H(p)$.

Nehmen wir an, daß H nicht für alle $p \in W(X)$ gilt, dann existiert ein kürzestes Wort p so, daß H nicht auf p zutrifft. Alle r mit $r \;\underline{\text{in}}\; p$ (bzw. $r \sqsubseteq p$ bzw. $r \sqsupseteq p$) und $r \neq p$ sind aber echt kürzer als p, d. h. H trifft auf alle Wörter r zu; folglich trifft H auf p zu. Widerspruch.

1.6.2 Induktionsbeweise in Algebren $[M, \Phi, E]$

Wir betrachten eine beliebige Algebra $[M, \Phi, E]$ mit Erzeugendensystem E. Hierbei ist M eine Menge, Φ ist eine Menge von Abbildungen $\phi : M \times \cdots \times M \to M$ und E ist eine Teilmenge von M derart, daß jedes Element von M aus Elementen von E durch Anwendung von Funktionen aus Φ erzeugt werden kann.

Beispiel: $\left[\mathfrak{M}_{\text{fin}}, \{+a | a \in E\}, \{\emptyset\}\right]$, dabei ist die Funktion $+a$ für $a \in E$ (die Allmenge erster Stufe); $N \in \mathfrak{M}_{\text{fin}}$ definiert als $+a(N) =_{\text{Def}} N \cup \{a\}$. Es ist also zum Beispiel

$$\{a, b, c\} = +c\,(+b\,(+a\,(\emptyset)))\,.$$

Um zu zeigen, daß $H(m)$ für alle $m \in M$ gilt, genügt es zu zeigen, daß

1. $H(x)$ für alle Erzeugenden $x \in E$ gilt (Anfangsschritt)
2. Für alle $\phi^n \in \Phi$, $a_1 \ldots, a_n \in M$ mit $H(a_1), \ldots, H(a_n)$ gilt $H\underbrace{\left(\phi^n(a_1, \ldots a_n)\right)}_{\in M}$

1.6.3 Induktive Definitionen

Eine induktive Definition einer $(k+1)$-stelligen Funktion f im Bereich der natürlichen Zahlen folgt dem Schema

$$\begin{aligned} f(x_1, \cdots, x_k, 0) &= f(x_1, \cdots, x_k, 0) \\ f(x_1, \cdots, x_k, n+1) &= h(x_1, \ldots, x_k, n, f(x_1, \ldots, x_k, n)) \end{aligned} \qquad (1.6.2)$$

Die Definition ist implizit, da f auf der rechten und auf der linken Seite vorkommt. Eine implizite Definition muß gerechtfertigt werden.

Satz 1.6.17 (Dedekindscher Rechtfertigungssatz)
Sind g, h Funktionen, so gibt es genau eine Funktion f, die 1.6.2 erfüllt.

Wir zeigen

1. es existiert eine Funktion f
2. es existiert genau eine Funktion f.

Beweis:

Einzigkeit: Es seien f_1, f_2 Funktionen, die das Gleichungssystem 1.6.2 erfüllen. Wir zeigen durch Induktion über i, daß für alle $x_1, \ldots, x_k, i$

$$f_1(x_1, \ldots, x_k, i) = f_2(x_1, \ldots, x_k, i)$$

ist.

Im Anfangsschritt ist $i = 0$, also

$$\begin{aligned} f_1(x_1, \ldots, x_k, i) &= f_1(x_1, \ldots, x_k, 0) \\ &= g(x_1, \ldots, x_k) \\ &= f_2(x_1, \ldots, x_k, 0) \\ &= f_2(x_1, \ldots, x_k, i) \end{aligned}$$

Im Induktionschritt schließen wir von i auf $i + 1$:

$$\begin{aligned} f_1(x_1, \ldots, x_k, i+1) &= h(x_1, \ldots, x_k, i, f_1(x_1, \ldots x_k, i)) \\ &= h(x_1, \ldots, x_k, i, f_2(x_1, \ldots x_k, i)) \quad \text{(Induktionsvoraussetzung)} \\ &= f_2(x_1, \ldots, x_k, i+1) \end{aligned}$$

Existenz: Zum Beweis der Lösbarkeit des Gleichungssystems lösen wir die induktive Definition in eine unendliche Folge von expliziten Definitionen auf:

$$\begin{aligned} f_0(x_1, \ldots, x_k, j) &:= \begin{cases} g(x_1, \ldots, x_k), & \text{falls } j = 0 \\ \text{nicht definiert}, & \text{sonst} \end{cases} \\ f_1(x_1, \ldots, x_k, j) &:= \begin{cases} f_0(x_1, \ldots, x_k, j), & \text{falls } j < 1 \\ h(x_1, \ldots, x_k, 0, f_0(x_1, \ldots x_k, 0)), & \text{falls } j = 1 \\ \text{nicht definiert}, & \text{sonst} \end{cases} \\ &\;\;\vdots \\ f_{i+1}(x_1, \ldots, x_k, j) &:= \begin{cases} f_i(x_1, \ldots, x_k, j), & \text{falls } j < i+1 \\ h(x_1, \ldots, x_k, i, f_i(x_1, \ldots x_k, i)), & \text{falls } j = i+1 \\ \text{nicht definiert}, & \text{sonst} \end{cases} \\ &\;\;\vdots \end{aligned}$$

Diese sind alles explizite Definitionen, die Funktionen f_i existieren also gemäß Mengenbildungsaxiomen. Folglich existiert auch f mit

$$f(x_1, \ldots, x_k, i) =_{\text{Def}} f_i(x_1, \ldots, x_k, i)$$

und es gilt

$$f(x_1, \ldots, x_k, 0) = f_0(x_1, \ldots, x_k, 0) = g(x_1, \ldots, x_k)$$

sowie

$$\begin{aligned} f(x_1, \ldots, x_k, i+1) &= f_{i+1}(x_1, \ldots, x_k, i+1) \\ &= h(x_1, \ldots x_k, i, f_i(x_1, \ldots, x_k, i)) \\ &= h(x_1, \ldots x_k, i, f(x_1, \ldots, x_k, i)) \end{aligned}$$

d. h. f erfüllt das Gleichungssystem 1.6.2.

Dieses Definitionsprinzip kann auf Worthalbgruppen verallgemeinert werden (also auf beliebige *freie* Halbgruppen), aber *nicht* auf beliebige Halbgruppen oder gar auf beliebig erzeugte Algebren.

Es seien $\mathfrak{X}, \mathfrak{Y}$ beliebige Mengen und X ein Alphabet. Um eine Abbildung $f : \mathfrak{X} \times W(X) \to \mathfrak{Y}$ zu definieren genügt es anzugeben

- eine Abbildung $g : \mathfrak{X} \rightarrow \mathfrak{Y}$
- zu jedem $x \in X$ eine Abbildung $h_x : \mathfrak{X} \times W(X) \times \mathfrak{Y} \rightarrow \mathfrak{Y}$

Die Definition von f sieht dann so aus:

$$\left.\begin{array}{lcl} f(\mathfrak{x}, e) & = & g(\mathfrak{x}) \\ f(\mathfrak{x}, px) & = & h_x(\mathfrak{x}, p, f(\mathfrak{x}, p)) \end{array}\right\} \begin{array}{c} \mathfrak{x} \in \mathfrak{X} \\ p \in W(X) \\ x \in X \end{array}$$

Dieses Gleichungssystem (bestehend aus $\operatorname{card}(X) + 1$ Gleichungen) wird von genau einer Funktion $f : \mathfrak{X} \times W(X) \rightarrow \mathfrak{Y}$ erfüllt.

Kapitel 2

Aussagenlogik

In diesem Kapitel beschäftigen wir uns mit der Formalisierung eines Teilbereichs des menschlichen Denkens, dem logischen Schließen. Wir wollen ein mathematisches Modell dieses Teilbereiches angeben, das uns gestattet, logisches Schließen durch Rechnen zu ersetzen; dadurch können logische Schlüsse überprüft werden.

Logisches Schließen ist eine Operation mit Aussagen, die auf der Basis von sogenannten Schlußregeln arbeitet. Von einer richtigen Schlußregel erwartet man, daß sie von gültigen Aussagen zu gültigen Aussagen führt.

Es sind also zunächst folgende Fragen zu klären:

- Was ist eine Aussage?
- Wann ist eine Aussage wahr?
- Was ist eine gültige Schlußregel?

2.1 Grundbegriffe

Unter einer Aussage verstehen wir die sprachliche Widerspiegelung eines Sachverhalts (in Form eines Aussagensatzes). (z. B. es regnet; wenn es regnet, dann ist die Straße naß.)

Eine Aussage wird wahr genannt, wenn der ausgedrückte Sachverhalt vorliegt. Die Aussage „es regnet“ ist also genau dann wahr, wenn es regnet.

In der Realität ist häufig unklar, ob eine Aussage wahr ist oder nicht, weil Maßstäbe unscharf sind, z. B. „Gestern war schlechtes Wetter“. Wir gehen hier von einer Idealisierung der wirklichen Verhältnisse aus und verlangen als Axiom:

Satz 2.1.1 (Satz der Zweiwertigkeit)
Jede Aussage ist entweder wahr oder falsch.

Diese Idealisierung hat sich insbesondere in der Mathematik und Informatik bewährt. Die sogenannte Fuzzy–Logik bietet Ansätze, ohne dieses Axiom auszukommen.

Nach dem Satz der Zweiwertigkeit zerfällt die Menge aller Aussagen erschöpfend und disjunkt in zwei Klassen, die Menge W aller wahren Aussagen und die Menge F aller falschen Aussagen. Wir nennen W und F die Wahrheitswerte; wir haben also genau zwei Wahrheitswerte.

Neben den Sachverhalten selbst beobachten wir in der Realität Beziehungen zwischen Sachverhalten, die sich in Beziehungen und Operationen mit Aussagen widerspiegeln.

Eine n-stellige Aussagenfunktion α ist also eine Abbildung, die jedem n-Tupel von Aussagen eine Aussage zuordnet. Einige wichtige Aussagenfunktionen spiegeln sich sprachlich sehr einfach in Bindewörtern wider, z. B.

- Konjunktion „und“ $\quad \mathrm{und}(A, B) = A \,\mathrm{und}\, B$
- Alternative „oder“ $\quad \mathrm{oder}(A, B) = A \,\mathrm{oder}\, B$
- Negation „nicht“ $\quad \mathrm{nicht}(A) = \mathrm{nicht}\, A$
- Implikation „wenn…, so…“
- Äquivalenz „genau dann, wenn“

Aussagen, wahre wie falsche, können nach verschiedenen Gesichtspunkten geordnet werden, z. B. nach Wissensgebieten (etwa Physik, Mathematik, …). Wir streben hier eine Formalisierung der Logik an, die in allen Gebieten anwendbar ist, in denen logisch gedacht wird. Damit stellt sich die Frage, welche Eigenschaften von Aussagen in unserem Formalismus (dem Aussagenkalkül) widergespiegelt werden sollen. Wir beantworten diese Frage einschränkend: die einzige Eigenschaft ist Wahrheit bzw. Falschheit. Wir berücksichtigen hier beispielsweise nicht, daß Aussagen etwas über einzelne Gegenstände aussagen („3 ist eine Primzahl“) oder die Struktur einer Allaussage haben („jede Äquivalenzrelation ist transitiv“); das wird erst in der Prädikatenlogik geschehen.

Was geschieht bei dieser Abstraktion Aussage $\to$ Wahrheitswert mit den Aussagenverbindungen (Aussagenfunktionen)? Mit anderen Worten, kann zu jeder Aussagenfunktion

$$\alpha : \bigtimes_n \mathfrak{A} \to \mathfrak{A},$$

wobei $\mathfrak{A}$ die Menge aller Aussagen ist, eine Wahrheitsfunktion

$$\phi : \bigtimes_n \{W, F\} \to \{W, F\},$$

d. h. eine Abbildung, die jedem n-Tupel von Wahrheitswerten einen Wahrheitswert zuordnet, gefunden werden, so daß für $A_1, \ldots, A_n$ gilt:

$$WW(\alpha(A_1, \ldots, A_n)) = \phi(WW(A_1), \ldots, WW(A_n))$$

wobei WW die Funktion ist, die jeder Aussage A ihren Wahrheitswert $WW(A)$ zuordnet, also W wenn A wahr ist und F sonst.

Für die Aussagenfunktion „und“ funktioniert das offensichtlich; die Wahrheitsfunktion et mit der Tabelle

w_1	w_2	$\mathrm{et}(w_1, w_2)$
W	W	W
W	F	F
F	W	F
F	F	F

leistet das Verlangte, denn die Aussage „A und B“ ist genau dann wahr, wenn die Aussage A wahr ist und die Aussage B wahr ist.

Definition 2.1.2
Eine Aussagenfunktion $\alpha : \bigtimes_n \mathfrak{A} \to \mathfrak{A}$ heißt extensional, wenn es eine Wahrheitsfunktion (BOOLEsche Funktion) $\phi : \bigtimes_n \{W, F\} \to \{W, F\}$ so gibt, daß für alle $A_1, \ldots, A_n \in \mathfrak{A}$ gilt

$$WW(\alpha(A_1, \ldots, A_n)) = \phi(WW(A_1), \ldots, WW(A_n))$$

Die Aussagenfunktion „und" ist also extensional, man stellt leicht fest, daß dasselbe für „oder", „nicht", „wenn..., so..." und „genau dann, wenn" gilt; die zugehörigen (sogenannten klassischen) Wahrheitsfunktionen werden als vel, non, seq (von sequitur) und aeq bezeichnet:

w_1	w_2	$\text{vel}(w_1, w_2)$	$\text{seq}(w_1, w_2)$	$\text{aeq}(w_1, w_2)$	$\text{non}(w_1)$
W	W	W	W	W	F
W	F	W	F	F	F
F	W	W	W	F	W
F	F	F	W	W	W

Gibt es überhaupt Aussagenfunktionen, die nicht extensional sind, die wir also *nicht* durch Wahrheitsfunktionen widerspiegeln können? Das ist der Fall, als Beispiel betrachte man die Aussagenfunktionen „weil" bzw. „damit":

$$\begin{aligned} \text{weil}(A, B) &= A, \text{weil}\, B \\ \text{damit}(A, B) &= A, \text{damit}\, B \end{aligned}$$

die eine kausale bzw. pragmatische Beziehung beschreiben. Diese Aussagenfunktionen können also nicht durch Wahrheitsfunktionen repräsentiert werden.

2.1.1 Aufbau des Kalküls

In unserem Kalkül brauchen wir Variable für Wahrheitswerte, die wir Aussagenvariable nennen werden, und Zeichen (Funktoren) für Wahrheitsfunktionen. Aus den Zeichen p und $\star$ bilden wir Wörter, unter denen die Aussagenvariablen ausgezeichnet werden, ferner verwenden wir

$\neg$ als Zeichen für die Wahrheitsfunktion non
$\wedge$ als Zeichen für die Wahrheitsfunktion et
$\vee$ als Zeichen für die Wahrheitsfunktion vel
$\rightarrow$ als Zeichen für die Wahrheitsfunktion seq
$\leftrightarrow$ als Zeichen für die Wahrheitsfunktion aeq

sowie die technischen Zeichen (und). Das Alphabet des Aussagenkalküls ist also

$$X = \{p, \star, \neg, \wedge, \vee, \rightarrow, \leftrightarrow,), (\}$$

Definition 2.1.3 (Aussagenvariable)

A) p ist eine Aussagenvariable

I) Ist p eine Aussagenvariable, so auch $p^\frown\star$

Die Menge AV der Aussagenvariablen ist die kleinste Menge von Wörtern über X, die das Wort p enthält, und abgeschlossen ist in bezug auf das Anhängen des Zeichens $\star$.

$$\text{AV} = \{p\underbrace{\star\cdots\star}_{i} | i \geq 0\}$$

Schreibweise: $p\star$ wird abgekürzt als q, $p\star\star$ als r, allgemein $p\underbrace{\star\cdots\star}_{i}$ als p_i.

Definition 2.1.4 (Ausdruck)

A) Jede Aussagenvariable ist ein Ausdruck

I) Sind H_1, H_2 Ausdrücke, so auch die folgenden Zeichenreihen: $\neg H_1$, $(H_1 \wedge H_2)$, $(H_1 \vee H_2)$, $(H_1 \to H_2)$, $(H_1 \leftrightarrow H_2)$.

Die Menge ausd der Ausdrücke ist die kleinste Menge von Wörtern, die alle Aussagenvariablen enthält und abgeschlossen ist bezüglich der unter I) angegebenen Konstruktionen.

Beispiel: Es sind $\neg p$, $(\neg p \vee p)$, $((\neg p_7 \wedge p_5) \to p_1)$ Ausdrücke; kein Ausdrücke: e, 11, (p).

Durch die Klammerung ist für jeden Ausdruck kenntlich, auf welche Weise er aus Aussagenvariablen oder einfacheren Ausdrücken aufgebaut ist, genauer: jeder Ausdruck kann auf genau eine Weise aus Aussagenvariablen aufgebaut werden. Die Menge ausd bildet daher mit dem Erzeugendensystem AV und den angegebenen Konstruktionsoperationen eine freie Struktur, so daß wir im folgenden Funktionen induktiv auf ausd definieren können.

Bei der Schreibweise von Ausdrücken können folgende Klammersparregeln verwendet werden

1. Außenklammern weglassen.
2. Klammern in mehrfachen Alternativen oder Konjunktionen
3. Vorrangregeln
   - $\wedge$ bindet stärker als $\vee$
   - $\vee$ bindet stärker als $\to$
   - $\to$ bindet stärker als $\leftrightarrow$

- $p \wedge q \vee r \mathrel{\hat{=}} (p \wedge q) \vee r$
- $p \leftrightarrow r \to q \mathrel{\hat{=}} p \leftrightarrow (r \to q)$

Satz 2.1.5
Es gibt einen Algorithmus, der für jedes Wort $w \in W(X)$ entscheidet, ob $w \in$ ausd ist.

2.2 Semantik

Ein Kalkül κ ist gegeben durch sein Alphabet (hier X), die Menge (Sprache) der in diesem Kalkül sinnvollen Wörter über diesem Alphabet (hier ausd) und seine Semantik, d. h. eine Zuordnung von Bedeutungen zu den Wörtern seiner Sprache. Bei Logikkalkülen besteht die Angabe der Semantik aus der Menge S der (gültigen) Sätze und einem Deduktionsoperator.

Um über Gültigkeit eines Ausdruckes reden zu können, definieren wir zunächst den Wahrheitswert, den ein Ausdruck bei einer Belegung der Aussagenvariablen annimmt.

Definition 2.2.1 (Belegung)
$\beta : \text{AV} \to \{W, F\}$.

Definition 2.2.2 (wert (H, β))

A) wert $(p_i, \beta) = \beta\,(p_i)$

I)
- wert $(\neg H, \beta) =$ non (wert (H, β))
- wert $((H_1 \wedge H_2), \beta) =$ et (wert (H_1, β), wert (H_2, β))
- wert $((H_1 \vee H_2), \beta) =$ vel (wert (H_1, β), wert (H_2, β))
- wert $((H_1 \rightarrow H_2), \beta) =$ seq (wert (H_1, β), wert (H_2, β))
- wert $((H_1 \leftrightarrow H_2), \beta) =$ aeq (wert (H_1, β), wert (H_2, β))

Lemma 2.2.3
Es sei H ein Ausdruck, in dem genau die Variablen $p_{j_1}, \ldots, p_{j_k}$ vorkommen. β, β' seien Belegungen, die auf $p_{j_1}, \ldots, p_{j_k}$ übereinstimmen. Dann ist wert $(H, \beta) =$ wert (H, β').

Definition 2.2.4
Es sei $H \in$ ausd, $p_{j_1}, \ldots, p_{j_n}$ alle in H vorkommenden Aussagenvariablen mit $j_1 < \cdots j_n$.

$$\Phi_H\,(w_1, \ldots, w_n) := \text{wert}\,(H, \beta^\star)\,,\ \text{wobei}\ \beta^\star\,(p_{j_i}) = w_i\ 1 \leq i \leq n$$

ist die von H repräsentierte Wahrheitsfunktion.

($\Phi_H\,(\beta^\star\,(p_{i_1})\,, \ldots, \beta^\star\,(p_{j_n})) =$ wert $(H, \beta^\star)$ für alle Belegungen $\beta^\star$.)

Damit haben wir jedem Ausdruck eine Wahrheitsfunktion zugeordnet, die seine Bedeutung ist, denn er repräsentiert diese Wahrheitsfunktion im Kalkül. Es entsteht die Frage, ob alle Wahrheitsfunktionen durch Ausdrücke dargestellt werden können, oder ob wir beim Übergang von Wahrheitsfunktionen zu Ausdrücken wieder etwas verlieren wie beim Übergang von Aussagenfunktionen zu Wahrheitsfunktionen.

Satz 2.2.5 (Repräsentantentheorem)
Zu jeder Wahrheitsfunktion Φ existiert ein Ausdruck H mit $\Phi_H = \Phi$.

Beweis: Sei Φ gegeben durch die Tabelle:

w_1	$\ldots$	w_n	$\Phi(w_1, \ldots, w_n)$
W	$\ldots$	W	$\Phi(W, \ldots, W)$
	$\vdots$		$\vdots$

Eine Elementarkonjunktion in $p_1, \ldots, p_n$ ist ein Ausdruck H der Form:

$$H : [\neg]\,p_1 \wedge [\neg]\,p_2 \cdots \wedge [\neg]\,p_n$$

Sei H eine Elementarkonjunktion. Dann ist wert $(H, \beta) = W$ genau dann, wenn für $i = 1, \ldots, n$ gilt:

$$\beta\,(p_i) = \begin{cases} W, & \text{falls vor } p_i \text{ kein } \neg \text{ steht} \\ F, & \text{falls vor } p_i \text{ ein } \neg \text{ steht} \end{cases}$$

Beispiel: $p_1 \wedge \neg p_2 \wedge p_3 : \beta\,(p_1) = W,\ \beta\,(p_2) = F,\ \beta\,(p_3) = W.$

1.Fall: $\Phi =$ falsum, d. h. $\Phi(w_1, \ldots, w_n) \equiv F$, dann gilt für

$$H := (p_1 \wedge \neg p_1) \vee (p_2 \wedge \neg p_2) \vee \ldots \vee (p_n \wedge \neg p_n)$$

$\Phi_H = \Phi$

2.Fall: $\Phi \neq$ falsum, d. h. es gibt n-Tupel $[w_1, \ldots, w_n]$ mit $\Phi(w_1, \ldots, w_n) = W$. Es seien $\beta_1, \ldots, \beta_{i_k}$ alle Belegungen β von $p_1, \ldots, p_n$ so, daß $\Phi(\beta(p_1), \ldots, \beta(p_n)) = W$ ist. Zu β_i sei K_i die Elementarkonjunktion mit wert $(K_i, \beta_i) = W$. Dann gilt:

$H \equiv K_{i_1} \vee K_{i_2} \vee \cdots \vee K_{i_k}$ leistet das Verlangte, d. h. $\Phi_H = \Phi$.

2.3 Weitere semantische Begriffe

Definition 2.3.1
Eine logische Matrix ist ein Tupel $\mu = [M, M^\star, \phi_1, \phi_2, \phi_3, \phi_4, \phi_5]$ mit: $M^\star \subseteq M \neq \emptyset$, $\phi_1 : M \to M, \quad \phi_2, \ldots, \phi_5 : M \times M \to M$.

Die klassische logische Matrix:

$$[\{W, F\}, \{W\}, \text{non}, \text{et}, \text{vel}, \text{seq}, \text{aeq}]$$

Belegung: $\mathfrak{B}_\mu = \{\beta | \text{AV} \to M\}$; $\mathfrak{B} = \{\beta | \beta : \text{AV} \to \{W, F\}\}$

$\text{wert}_\mu(H, \beta)$ wird analog zu wert (H, β) definiert.

Beispiel: $\text{wert}_\mu((H_1 \wedge H_2), \beta) = \phi_2(\text{wert}_\mu(H_1, \beta), \text{wert}_\mu(H_2, \beta))$

Wir führen die semantischen Begriffe für die klassische logische Matrix ein:

Definition 2.3.2 (Erfüllbarkeit, Gültigkeit)
$\beta \in \mathfrak{B}, H \in \text{ausd}$

1. β erfüllt H $(\beta \text{erf} H) :\leftrightarrow \text{wert}(H, \beta) = W$

   in beliebiger logischer Matrix:

   $$\beta \text{erf}_\mu H :\leftrightarrow \text{wert}_\mu(H, \beta) \in M^\star$$

2. H ist erfüllbar ($H \in$ ef, ef$H$), wenn eine Belegung $\beta \in \mathfrak{B}$ existiert so, daß $\beta \text{erf} H$.
3. H wird (allgemein) gültig ($H \in$ ag, ag$H$) genannt, wenn jede Belegung $\beta \in \mathfrak{B}$ den Ausdruck H erfüllt. (H ist eine Identität, bzw. Tautologie.)
4. H ist Kontradiktion ($H \in$ kt, kt$H$), wenn es keine Belegung β gibt, die H erfüllt.

Folgerung 2.3.3

1. ag $\subset$ ef
2. ag$H$ gdw. nicht ef$\neg H$; ef$H$ gdw. nicht ag$\neg H$
3. Wenn $\beta \text{erf} H$, so nicht $\beta \text{erf} \neg H$
4. **Satz 2.3.4 (Satz vom Ausgeschlossenen Widerspruch für die Gültigkeit)**

   Es gibt keinen Ausdruck H mit ag$H$ und ag$\neg H$.

5. **Satz 2.3.5 (Satz vom ausgeschlossenen Dritten für die Erfüllbarkeit)**

   Für jedes $H \in$ ausd gilt: ef$H$ oder ef$\neg H$.

2.4 Modell, Folgern und Endlichkeitssatz

Definition 2.4.1
Es sei $X \subseteq$ ausd

- Eine Belegung β heißt Modell von X ($\beta \mathrm{Mod} X$), wenn für alle $H \in X$ gilt $\beta \mathrm{erf}\, H$
- Aus X folgt H ($X \mathrm{fol} H$), wenn jedes Modell β von X den Ausdruck H erfüllt.
- Der Folgerungsoperator fl ist wie folgt definiert: $\mathrm{fl}\,(X) := \{H | X \mathrm{fol} H\}$

Satz 2.4.2
Eigenschaften von fl:

1. $\mathrm{fl}\,(\emptyset) = \mathrm{ag}$.
2. Hülleneigenschaften von fl:
   (a) $X \subseteq \mathrm{fl}\,(X)$
   (b) Wenn $X \subseteq Y$, so $\mathrm{fl}\,(X) \subseteq \mathrm{fl}\,(Y)$.
   (c) $\mathrm{fl}\,(\mathrm{fl}\,(X)) = \mathrm{fl}\,(X)$.
3. Wenn $H \in \mathrm{fl}\,(X)$, so gibt es eine endliche Teilmenge $X^\star \subseteq X$ mit $H \in \mathrm{fl}\,(X^\star)$

Beweis (des Endlichkeitssatzes für das Folgern)
Wir überlegen uns zuerst, daß es genügt zu beweisen:

Endlichkeitsatz für Modelle: Besitzt jede endliche Teilmenge $Y^\star$ von Y ein Modell, so besitzt Y ein Modell.

Zu zeigen ist: Wenn jedes Modell β von X den Ausdruck H erfüllt, dann gibt es eine endliche Teilmenge $X^\star$ von X, so daß jedes Modell $\beta^\star$ von $X^\star$ H erfüllt.

Diese Aussage hat die Form: Wenn A, so B. Damit gleichwertig ist die

Kontraposition: Wenn nicht B, so nicht A.

Wenn: Für jede endliche Teilmenge $X^\star$ von X gibt es ein Modell $\beta^\star$ von $X^\star$ mit $\beta^\star$ erfüllt H nicht, (d. h. $\beta^\star \mathrm{erf} \neg H$).

so: es gibt ein Modell β von X, das H nicht erfüllt, d. h. $\neg H$ erfüllt.

Lemma 2.4.3
$\beta \mathrm{Mod} X$ und $\beta \mathrm{erf}\, H$ gdw. $\beta \mathrm{Mod}\,(X \cup \{H\})$.

Also ist der Endlichkeitssatz für fl gleichwertig mit:

Wenn: Für jedes endliche $X^\star \subseteq X$ gibt es ein $\beta^\star$ mit $\beta^\star \mathrm{Mod}\,(X^\star \cup \{\neg H\})$,

so: Es gibt ein Modell β mit

$$\beta \mathrm{Mod}\,(X \cup \{\neg H\})\,.$$

Diese Aussage ergibt sich aus dem Endlichkeitssatz für Modelle für $Y = X \cup \{\neg H\}$.

Wir zeigen: Wenn für jedes endliche $X^\star \subseteq X$ ein $\beta^\star$ mit $\beta^\star \mathrm{Mod}(X^\star \cup \{\neg H\})$ existiert,
dann besitzt jede endliche Teilmenge $Y^\star \subseteq X \cup \{\neg H\} = Y$ ein Modell.

Sei $Y^\star$ endliche Teilmenge von $Y = X \cup \{\neg H\}$.

Fall 1: $\neg H \in Y^\star$.

Sei $X^\star = Y^\star \setminus \{\neg H\} \subseteq X$. $X^\star$ besitzt ein Modell $\beta^\star$, das H nicht erfüllt:

$$\beta^\star \mathrm{Mod}\underbrace{\left(X^\star \cup \{\neg H\}\right)}_{Y^\star}$$

Fall 2: $\neg H \notin Y^\star$

Dann ist $Y^\star \subseteq X$, also es existiert $\beta^\star \mathrm{Mod}\,(Y^\star \cup \{\neg H\})$, also $\beta^\star \mathrm{Mod} Y^\star$.

Ad 2. (Beweis des Endlichkeitssatzes für Modelle)

Lemma 2.4.4

Vor.: Jede endliche Teilmenge $X^\star \subseteq X$ besitzt ein Modell.

Beh.: Zu jeder Aussagenvariable p_i gibt es einen Wahrheitswert w_i derart, daß jede endliche Teilmenge $X^\star$ von X ein Modell $\beta_i^\star$ mit $\beta_i^\star\,(p_i) = w_i$ hat.

Beweis: Es sei p_i fixiert. Für jede endliche Teilmenge $X^\star$ von X kann einer von vier Fällen eintreten:

Fall 1: Es gibt ein Modell $\beta^\star$ von $X^\star$ mit $\beta^\star\,(p_i) = W$ und es gibt ein Modell $\beta^{\star\star}$ von $X^\star$ mit $\beta^{\star\star}\,(p_i) = F$.

Fall 2: Es gibt ein Modell $\beta^\star$ von $X^\star$ mit $\beta^\star\,(p_i) = W$ und es gibt kein Modell $\beta^{\star\star}$ von $X^\star$ mit $\beta^{\star\star}\,(p_i) = F$

Fall 3: Kein $\beta^\star$ ...und ein $\beta^{\star\star}$ ...

Fall 4: kein $\beta^\star$ ...und kein $\beta^{\star\star}$...

Der Fall 4 kann nicht eintreten, da $X^\star$ ein Modell hat

Ann. Für $X_1^\star \subseteq X$ tritt der 2. Fall und für $X_2^\star \subseteq X$ tritt der 3. Fall ein. Dann $X_1^\star \cup X_2^\star \subseteq X$ besitzt Modell β, und weil $\beta \mathrm{Mod} X_1^{\star\star}$ gilt $\beta\,(p_i) \neq F$, und aus $\beta \mathrm{Mod} X_2^\star$ folgt $\beta\,(p_i) \neq W$ Widerspruch.

Fall 1 Für alle endlichen Teilmengen $X^\star$ mit X tritt 1) oder 2) ein. Dann setzen wir $w_i := W$.

Fall 2 Für alle endlichen Teilmengen $X^\star$ mit X tritt 1) oder 3) ein. Dann setzen wir $w_i := F$.

Damit ist das Lemma 2.4.4 bewiesen.

Wir wollen jetzt ein Modell für X konstruieren. Dabei gehen wir induktiv vor. Sei $X_0 := X$

$$X_{n+1} = \begin{cases} X_n \cup \{p_n\}\,, & \text{falls jede endliche Teilmenge } X^\star \subseteq X \\ & \text{ein Modell } \beta^\star \text{ mit } \beta^\star\,(p_i) = W \text{ hat} \\ X_n \cup \{\neg p_n\}\,, & \text{sonst} \end{cases}$$

Behauptung 1: Für alle $n \geq 0$ gilt: Jede endliche Teilmenge von X_n hat ein Modell.

Beweis Induktion über n.

A) $n = 0$ — trivial

I) $n \to n+1$
Nach Lemma: Zu p_n existiert w_n so, daß jede endliche Teilmenge $X^\star \subseteq X_n$ ein Modell $\beta^\star$ mit $\beta^\star(p_n) = w_n$ hat.

Fall 1: $w_n = W$:
Jede endliche Teilmenge $X^\star \subseteq X$ hat Modell $\beta^\star$ mit $\beta^\star(p_n) = W$

$$X_{n+1} = X_n \cup \{p_n\}$$

Sei $X^\star$ endliche Teilmenge von X_{n+1}, dann hat $X^\star$ ein Modell.

Fall 2: $w_n = F$:
$X_{n+1} := X_n \cup \{\neg p_n\}$ usw. analog Fall 1.

Setzen $Y = \bigcup_{n \geq 0} X_n$

Behauptung 2: Jede endliche Teilmenge $Y^\star$ von Y besitzt ein Modell.
Weil $Y^\star$ endlich ist, existiert ein m mit $Y^\star \subseteq X_m$

$$m = \max\{i | p_i \in X^\star \text{oder} \neg p_i \in X^\star\},$$

also hat $Y^\star$ ein Modell nach Behauptung 1.

Wir betrachten die Belegung $\bar{\beta} : \mathrm{AV} \to \{W, F\}$ mit

$$\bar{\beta}(p_i) = \begin{cases} W, & p_i \in Y \\ F, & \neg p_i \in Y \end{cases}$$

Behauptung: $\bar{\beta} \mathrm{Mod} X$, d. h. wenn $H \in X$, so $\bar{\beta} \mathrm{erf} H$

Es sei $H \in X, p_{j_1}, \ldots, p_{j_n}$ alle Aussagenvariablen von H.

$$Y^\star = \{H\} \cup \begin{cases} \{p_{j_v}\}, & p_{j_v} \in Y \\ \{\neg p_{j_v}\}, & \neg p_{j_v} \in Y \end{cases} \quad v = 1, \ldots, n$$

$\mathrm{card}(Y^\star) \leq n+1$, d. h. endlich, also $Y^\star$ besitzt ein Modell $\beta^\star$ (nach Behauptung 2) Dabei gilt: für $v = 1, \ldots, n$

$$\beta^\star(p_{j_v}) = \left\{ \begin{array}{ll} W, \text{falls} & p_{j_v} \in Y \\ F, \text{falls} & \neg p_{j_v} \in Y \end{array} \right\} = \bar{\beta}(p_{j_n})$$

Lemma 2.4.5

$$W = \mathrm{wert}(H, \beta^\star) = \mathrm{wert}\left(H, \bar{\beta}\right)$$

also $\bar{\beta} \mathrm{erf} H$.

2.4.1 Ableitbarkeitstheorem und Deduktionstheorem

$$(H^\star \to H) \in \mathrm{fl}(X) \text{ gdw. } H \in \mathrm{fl}(X \cup \{H^\star\}).$$

Beweis: $(\rightarrow)$
Vor: Jedes Modell von X erfüllt $(H^\star \rightarrow H)$

Beh: Jedes Modell von $X \cup \{H^\star\}$ erfüllt H.

Sei βMod $(X \cup \{H^\star\})$. βMod$X$, also βerf $(H^\star \rightarrow H)$ nach Voraussetzung. Es gilt

$$W = \text{wert}\,(H^\star \rightarrow H, \beta) = \text{seq}\big(\underbrace{\text{wert}\,(H^\star, \beta)}_{W}, \text{wert}\,(H, \beta)\big)$$

also wert $(H, \beta) = W$, d. h. βerf$H$.

$(\leftarrow)$
Vor: Jedes Modell von $X \cup \{H^\star\}$ erfüllt H.

Beh: Jedes Modell von X erfüllt $(H^\star \rightarrow H)$.

Sei βMod$X$.

Fall 1: βerf$\neg H^\star$, d. h. wert $(H^\star, \beta) = F$.
Dann ist wert $((H^\star \rightarrow H), \beta) = W$, d. h. βerf $(H^\star \rightarrow H)$

Fall 2: βerf$H^\star$
Dann ist βMod $(X \cup \{H^\star\})$. Folglich βerf$H$, also βerf $(H^\star \rightarrow H)$.

Ferner gilt: fl (ag) $\subseteq$ ag.
Nämlich fl (ag) = fl (fl $(\emptyset)$) = fl $(\emptyset)$ = ag

Definition 2.4.6 (Kalkül)
$\mathfrak{K} = [X, A, S, F]$ heißt Kalkül, wenn

1. X ist ein endliches Alphabet.
2. $A \subseteq W(X)$ ist eine Sprache über X.
3. $S \subseteq A$ ist eine Satzmenge (Menge der Theoreme)
4. $F : \mathfrak{P}(A) \rightarrow \mathfrak{P}(A)$ (Deduktionsoperator des Kalküls) mit
   - Hülleneigenschaften
   - Endlichkeitssatz (für Folgerungsoperator)
   - $F(S) \subseteq S$

Beispiel: $AK = [X, \text{ausd}, \text{ag}, \text{fl}]$ ist ein Kalkül (Aussagenkalkül).

Man unterscheidet:

- Kalkül mit semantisch definierter Satzmenge.

  ag = Menge der in der klassischen logischen Matrix gültigen Ausdrücke (fl $(\emptyset)$)

- Kalkül mit syntaktisch definierter Satzmegne.

  S = Menge aller mittels rein syntaktischer Unformungsoperationen aus einer endlichen Menge von Ausdrücken zu gewinnender Ausdrücke.

Abtrennungsregel: $\dfrac{H, (H \rightarrow H^\star)}{H^\star}$

Einsetzungsregel: $\dfrac{H\,(p_i)\,,H^\star}{H\,(p_i/_{H^\star})}$

Definition 2.4.7
Ein Kalkül heißt entscheidbar, wenn es einen Algorithmus gibt, der für jedes $H \in A$ entscheidet, ob $H \in S$ ist.

Satz 2.4.8
Der Aussagenkalkül ist entscheidbar.

Beweis: $H \in$ ag gdw. für alle $\beta \in \mathfrak{B}$ wert $(H, \beta) = W$.

H hängt nur von $p_1, \ldots p_n$ ab.

gdw. für jede Belegung β von $\{p_1, \ldots p_n\}$ gilt

$$\text{wert}\,(H, \beta) = W$$

Es sind also „nur“ 2^n Belegungen zu prüfen.

2.5 Aussagenlogisches Schließen

1. Wozu ist ag gut?
   Es sei $H \in$ ag; $p_1, \ldots, p_n$ alle Aussagenvariablen in H, dann ist $\Phi_H\,(w_1, \ldots, w_n) = W =$ wert (H, β) mit $\beta\,(p_i) = w_i$. $H \in$ ag *spiegelt* eine verum-funktion, d. h. *spiegelt* eine extensionale Aussagenfunktion, die stets eine wahre Aussage als Funktionswert hat, eine sogenannte Tautologie.

2. Was ist eine Schlußregel?
   „Wenn $A_1, \ldots, A_n$ gilt, so gilt auch $B_1, \ldots, B_m$“. Oder „Wenn $A_1, \ldots, A_n$, so $\alpha\,(A_1, \ldots, A_n)$“. Eine Schlußregel ist eine Tautologie, wobei die Implikation Hauptverknüpfung ist.

3. Wie kann man feststellen, ob eine Schlußregel gültig ist?
   Wenn die Schlußregel die allgemeine Form

   $$\text{wenn } A_1, \ldots, A_n, \text{ so } \alpha(A_1, \ldots, A_n) \tag{2.5.1}$$

   hat und α eine extensionale Aussagenfunktion ist, dann können wir zu der zu α gehörigen Wahrheitsfunktion Φ einen repräsentierenden Ausdruck H des Aussagenkalküls finden. Wir nehmen an, daß dieser Ausdruck genau die Variablen $p_1, \ldots, p_n$ enthält und betrachten den Ausdruck

   $$H^\star = p_1 \wedge p_2 \wedge \cdots \wedge p_n \to H.$$

   Wenn $H^\star \in$ ag ist, dann ist die Schlußregel (2.5.1) gültig, und umgekehrt. Wir können sagen, daß die Allgemeingültigkeit von $H^\star$ die Schlußregel (2.5.1) rechtfertigt.

Im folgenden geben wir einige aussagenlogische Schlußregeln an. Ist dabei der „Schluß“–Strich fett gedruckt, dann gilt die Regel auch in die umgekehrte Richtung.

1. **Konjunktionsregel**

$$\begin{array}{c} \text{Wenn } A, \text{ so } B \\ \text{Wenn } A, \text{ so } C \\ \hline \text{Wenn } A, \text{ so } (B \text{ und } C) \end{array}$$

Rechtfertigung: $(p \to q) \wedge (p \to r) \leftrightarrow (p \to q \wedge r) \in$ ag

2. **Alternative**

   (a) **Schluß auf eine Alternative**

$$\frac{\text{Wenn } A\text{, so } B}{\text{Wenn } A\text{, so } (B \text{ oder } C)}$$

   Rechtfertigung: $(p \to q) \to (p \to q \vee r) \in$ ag

   (b) **Schluß aus einer Alternative**

$$\frac{\begin{array}{c}\text{Wenn } A\text{, so } B \text{ oder } C\\ \text{Wenn } A \text{ und } B\text{, so } D\\ \text{Wenn } A \text{ und } C\text{, so } D\end{array}}{\text{Wenn } A\text{, so } D}$$

   $((p \to q \vee r) \wedge (p \wedge q \to s) \wedge (p \wedge r \to s) \to (p \to s)) \in$ ag

3. **Implikation**

$$\text{(a)}\ \frac{\text{Wenn } A \text{ und } B\text{, so } C}{\text{Wenn } A\text{, so (wenn } B\text{, so } C)}$$

   $(p \wedge q \to r) \to (p \to (q \to r)) \in$ ag

   (b) FREGEscher **Kettenschluß**

$$\frac{\begin{array}{c}\text{Wenn } A\text{, so (wenn } B\text{, so } C)\\ \text{Wenn } A\text{, so } B\end{array}}{\text{Wenn } A\text{, so } C}$$

   $(p \to (q \to r)) \wedge (p \to q) \to (p \to r) \in$ ag

   (c) **Kettenschluß**

$$\frac{\begin{array}{c}\text{Wenn } A\text{, so } B\\ \text{Wenn } B\text{, so } C\end{array}}{\text{Wenn } A\text{, so } C}$$

   $(p \to q) \wedge (q \to r) \to (p \to r) \in$ ag

4. **Äquivalenz**

$$\frac{\begin{array}{c}\text{Wenn } A\text{, so (wenn } B\text{, so } C)\\ \text{Wenn } A\text{, so (wenn } C\text{, so } B)\end{array}}{\text{Wenn } A\text{, so } (B \text{ gdw. } C)}$$

$(p \to (q \to r)) \wedge (p \to (r \to q)) \to (p \to (q \leftrightarrow r)) \in$ ag

5. **Negation**

   (a) **Kontraposition**

   $$\frac{\text{Wenn } A\text{, so } B}{\text{Wenn nicht } B\text{, so nicht } A.}$$

   $(p \to q) \to (\neg q \to \neg p) \in \text{ag}$

   (b) **Doppelte Negation**

   $$\frac{A}{\text{nicht nicht } A}$$

   $p \to \neg\neg p \in \text{ag}$

   (c) $$\frac{\begin{array}{c}\text{Wenn } A \text{ und } B\text{, so } C\\ \text{Wenn } A \text{ und } B\text{, so nicht } C\end{array}}{\text{Wenn } A\text{, so nicht } B}$$

   $(((p \wedge q) \to r) \wedge ((p \wedge q) \to \neg r)) \to (p \to \neg q) \in \text{ag}$

Das Haubersche Theorem

$n \geq 2$

$$\begin{array}{l}\text{Wenn } A_1\text{, so } B_1\\ \vdots\\ \text{Wenn } A_n\text{, so } B_n\end{array}$$

A_1 oder A_2 oder …oder A_n (Die Voraussetzungen A_i erschöpfen alle Fälle).

$$\frac{\begin{array}{l}\text{nicht } (B_1 \text{ und } B_2)\text{, nicht } (B_2 \text{ und } B_3)\text{, } \ldots\\ \text{nicht } (B_1 \text{ und } B_3)\text{, } \ldots\\ \vdots\\ \text{nicht } (B_1 \text{ und } B_n)\text{. (Die Behauptungen } B_i \text{ schließen sich paarweise aus)}\end{array}}{\begin{array}{l}A_1 \text{ gdw. } B_1\\ \vdots\\ A_n \text{ gdw. } B_n\end{array}}$$

Beweis: Annahme: Es gibt j so, daß A_j gdw. B_j falsch. Wenn A_j, so B_j ist wahr nach Voraussetzung, d. h. wenn B_j, so A_j ist falsch, d. h. B_j ist wahr und A_j falsch. Es gibt ein $i \neq j$ so, daß A_i wahr ist.

Wenn A_i, so B_i ist wahr, also B_i ist wahr und $i \neq j$ $\lightning$ nicht $(B_i$ und $B_j)$

2.6 Ableitbarkeit

Ziel: Syntaktische Charakterisierung des Folgerns.

Gesucht ist eine „syntaktische“ Operation $\vdash$ so, daß $X \mathrm{fol} H$ gdw. $X \vdash H$.

1. abl

   Definition 2.6.1 (mit Abtrennungsregel und Einsetzungsregel)

   A) Wenn $H \in X$, so $X \mathrm{abl} H$

   I) (a) Wenn $X \mathrm{abl}(H \to H')$ und $X \mathrm{abl} H$, so $X \mathrm{abl} H'$ (syntaktische Abtrennungsregel)

   (b) Wenn $X \mathrm{abl} H$ und $H' = H\left(p_i/_{H^\star}\right)$, so $X \mathrm{abl} H'$. (syntaktische Einsetzungsregel)

$$\mathrm{ab}(X) = \{H | X \mathrm{abl} H\}$$

2. abla: nur mit Abtrennungsregel

$$\mathrm{aba}(X) := \{H | X \mathrm{abla} H\}.$$

3. able: nur mit Einsetzungsregel

$$\mathrm{abe}(X) := \{H | X \mathrm{able} H\}.$$

Satz 2.6.2 (von der Rückverlegbarkeit der Einsetzung)

$$\mathrm{ab}(X) = \mathrm{aba}(\mathrm{abe}(X))$$

Beweis:
zu zeigen: Wenn $X \mathrm{abl} H$, so $\mathrm{abe}(X) \mathrm{abla} H$.

Beweis durch Induktion über H.

A) $H \in X$, dann ist $H \in \mathrm{abe}(X)$, also $\mathrm{abe}(X) \mathrm{abla} H$.

I) (a) Wir haben $X \mathrm{abl}(H' \to H)$ und $X \mathrm{abla} H$, nach Induktionsvoraussetzung ist also $\mathrm{abe}(X) \mathrm{abla}(H' \to H)$, $\mathrm{abe}(X) \mathrm{abla} H'$, also $\mathrm{abe}(X) \mathrm{abla} H$.

(b) Wir haben $X \mathrm{abl} H'$, $H = H'\left(p_i/_{H^\star}\right)$. Also gilt nach Induktionsvoraussetzung $\mathrm{abe}(X) \mathrm{abla} H'$.

Wenn hier $H' \in \mathrm{abe}(X)$ ist, dann ist $H = H'\left(p_i/_{H^\star}\right) \in \mathrm{abe}(X)$ also $\mathrm{abe}(X) \mathrm{abla} H$. Wenn $H' \notin \mathrm{abe}(X)$, so ist wegen $\mathrm{abe}(X) \mathrm{abla} H'$ auch $\mathrm{abe}(X) \mathrm{abla} H'\left(p_i/_{H^\star}\right)$, d. h. $\mathrm{abe}(X) \mathrm{abla} H$.

Satz 2.6.3 (Widerspruchsfreiheit von ab**)**
Wenn $X \subseteq \mathrm{ag}$, so $\mathrm{ab}(X) \subseteq \mathrm{ag}$.

Beweis: Induktion.

Satz 2.6.4 (Eigenschaften von $\mathrm{ab} : \mathfrak{P}(\mathrm{ausd}) \to \mathfrak{P}(\mathrm{ausd})$**)**

1. $\mathrm{ab}(\emptyset) = \emptyset$
2. ab hat die Hülleneigenschaften
3. Endlichkeitssatz: Wenn $H \in \mathrm{ab}(X)$, so gibt es eine endliche Teilmenge $X^\star \subseteq X$ mit $H \in \mathrm{ab}(X^\star)$
4. Ableitbarkeitstheorem: Wenn $(H^\star \to H) \in \mathrm{ab}(X)$, dann ist $H \in \mathrm{ab}(X \cup \{H^\star\})$.

   Das Deduktionstheorem $\ldots \leftarrow \ldots$ gilt nicht, denn
   $H^\star \in \mathrm{ab}(\{H^\star\}) = \mathrm{ab}(\emptyset \cup \{H^\star\})$, aber $(H^\star \to H^\star) \notin \mathrm{ab}(\emptyset)$
5. $\mathrm{ab}(\mathrm{ag}) \subseteq \mathrm{ag}$ (sogar gleich)

Folgerung: $[X, \mathrm{ausd}, \mathrm{ag}, \mathrm{ab}]$ ist ein Kalkül.

$\mathrm{ab}(\emptyset) = \emptyset \neq \mathrm{fl}(\emptyset) = \mathrm{ag}$
$\mathrm{fl}(X) \stackrel{?}{=} \mathrm{ab}(\mathrm{ag} \cup X)$ gilt ebenfalls nicht.

Satz 2.6.5
Ist $H \notin \mathrm{ag}$, so $\mathrm{ab}(\mathrm{ag} \cup \{H\}) = \mathrm{ausd}$. (ag ist syntaktisch vollständig bezüglich ab)

Beweis: Sei H fest, $p_1, \ldots, p_n$ alle Aussagenvariablen in H.

$H \notin \mathrm{ag} \to \mathrm{erf} \neg H$, d. h. es existiert $\beta^\star \in \mathfrak{B}$ mit $\mathrm{wert}(H, \beta^\star) = F$.

Für $i = 1, \ldots, n$ sei $H_i := \begin{cases} p_i, & \text{falls } \beta^\star(p_i) = F \\ \neg p_i, & \text{sonst.} \end{cases}$

Behauptung: $\mathrm{wert}(H_1 \vee \cdots \vee H_n, \beta^\star) = F$ gdw. $\beta^\star$ stimmt auf $p_1, \ldots, p_n$ mit $\beta^\star$ überein.

Beweis der Behauptung: $\mathrm{wert}(H_1 \vee \cdots \vee H_n, \beta) = F$ genau dann, wenn für alle $i = 1, \ldots, n$ $\mathrm{wert}(H_i, \beta) = F$, d. h.

$$\beta(p_i) = \left\{ \begin{array}{ll} F, & \text{falls } H_i = p_i \\ W, & \text{sonst} \end{array} \right\} = \beta^\star(p_i)$$

Behauptung: $(H \to H_1 \vee \cdots \vee H_n) \in \mathrm{ag}$

Annahme nicht, dann existiert $\beta \in \mathfrak{B}$: $\mathrm{wert}(H \to H_1 \vee \cdots \vee H_n, \beta) = F$

$\mathrm{wert}(H, \beta) = W$, $\underbrace{\mathrm{wert}(H_1 \vee \cdots H_n, \beta) = F}_{\beta = \beta^\star \text{ auf } p_1, \ldots p_n}$

$W = \mathrm{wert}(H, \beta) = \mathrm{wert}(H, \beta^\star) = F$ Widerspruch.

$$\frac{\begin{array}{c} H \in \mathrm{ab}(\mathrm{ag} \cup \{H\}) \\ (H \to H_1 \vee \cdots \vee H_n) \in \mathrm{ab}(\mathrm{ag} \cup \{H\}). \end{array}}{H_1 \vee \cdots \vee H_n \in \mathrm{ab}(\mathrm{ag} \cup \{H\}).}$$

Wir setzen ein für $p_i \begin{cases} p\ , \text{falls } H_i = p_i \\ \neg p, \text{falls } H_i = \neg p_i \end{cases}$ in $H_1 \vee \cdots \vee H_n$ und erhalten

$$H^\star = [\neg\neg]\, p \vee [\neg\neg]\, p \vee \cdots \vee [\neg\neg]\, p$$

$\rightarrow$

$$\frac{\begin{array}{c} H^\star \in \mathrm{ab}\,(\mathrm{ag} \cup \{H\}) \\ (H^\star \rightarrow p) \in \mathrm{ab}\,(\mathrm{ag} \cup \{H\}) \end{array}}{p \in \mathrm{ab}\,(\mathrm{ag} \cup \{H\})\,.} \qquad (\text{weil } H^\star \rightarrow p \in \mathrm{ag})$$

$H^{\star\star} \in$ ausd. $H^{\star\star} = p\left[p/_{H^{\star\star}}\right] \in \mathrm{ab}\,(\mathrm{ag} \cup \{H\})$.

Bemerkung: ag ist nicht syntaktisch vollständig bezüglich fl.

z. B. $p \notin$ ag; $H \in \mathrm{fl}\,(\mathrm{ag} \cup \{p\})$ gdw. $(p \rightarrow H) \in \mathrm{fl}\,(\mathrm{ag}) = \mathrm{ag}$ gdw. $(p \rightarrow H) \in \mathrm{ag}$
z. B. $(p \rightarrow q) \notin$ ag, so $q \notin \mathrm{fl}\,(\mathrm{ag} \cup \{p\})$.

Das Deduktionstheorem gilt für abla, wenn X hinreichend groß ist:

Satz 2.6.6

Voraussetzung:

1. Wenn der Ausdruck H eine der Formen

$$H_1 \rightarrow (H_2 \rightarrow H_1) \qquad (2.6.6.2)$$

$$H_1 \rightarrow H_1 \qquad (2.6.6.3)$$

$$(H_1 \rightarrow (H_2 \rightarrow H_3)) \rightarrow ((H_1 \rightarrow H_2) \rightarrow (H_1 \rightarrow H_3)) \qquad (2.6.6.4)$$

   hat, so ist $X \mathrm{abla} H$.
2. $(X \cup \{H^{\star\star}\})\,\mathrm{abla} H^\star$

Behauptung: $X \mathrm{abla}\,(H^{\star\star} \rightarrow H^\star)$

Beweis: Induktion über $H^\star$.

A) $H^\star \in X \cup \{H^{\star\star}\}$.

Fall 1 $H^\star = H^{\star\star}$ Nach Voraussetzung $X \mathrm{abla}\,(H^\star \rightarrow H^\star)$, also $X \mathrm{abla}\,(H^{\star\star} \rightarrow H^\star)$

Fall 2 $H^\star \neq H^{\star\star}$
Dann ist $H^\star \in X$. Nach Voraussetzung

$$\frac{\begin{array}{c} X \mathrm{abla} H^\star \rightarrow (H^{\star\star} \rightarrow H^\star) \\ X \mathrm{abla} H^\star \end{array}}{X \mathrm{abla}\,(H^{\star\star} \rightarrow H^\star)}$$

I)

$$\left.\begin{array}{c} X \cup \{H^{\star\star}\}\,\mathrm{abla} H_1 \rightarrow H^\star \\ X \cup \{H^{\star\star}\}\,\mathrm{abla} H_1 \end{array}\right\} \rightarrow X \cup \{H^{\star\star}\}\,\mathrm{abl} H^\star$$

Nach Induktionsvoraussetzung $X \mathrm{abla} H^{\star\star} \rightarrow (H_1 \rightarrow H^\star)$, $X \mathrm{abla} H^{\star\star} \rightarrow H_1$.

Nach Voraussetzung 2.6.6.4
$X \mathrm{abla}\,(H^\star \rightarrow (H_1 \rightarrow H^\star)) \rightarrow ((H^{\star\star} \rightarrow H_1) \rightarrow (H^{\star\star} \rightarrow H^\star))$ wegen Abtrennungsregel
folgt: $X \mathrm{abla}\,(H^{\star\star} \rightarrow H_1) \rightarrow (H^{\star\star} \rightarrow H^\star)$, also $X \mathrm{abla} H^{\star\star} \rightarrow H^\star$.

Die Ausdrücke (2.6.6.2), (2.6.6.3), (2.6.6.4) sind aus ag, also gültig!

$\mathrm{fl}\,(X) \stackrel{?}{=} \mathrm{aba}\,(\mathrm{ag} \cup X)$

Lemma 2.6.7
Es seien $F_1, F_2 : \mathfrak{P}\,(\mathrm{ausd}) \rightarrow \mathfrak{P}\,(\mathrm{ausd})$ mit

1. $F_1(\emptyset) \subseteq F_2(\emptyset)$
2. F_1 erfüllt den Endlichkeitssatz
3. Wenn $X^\star$ endlich, so gilt Deduktionstheorem für F_1: Wenn $H_2 \in F_1(X^\star \cup \{H_1\})$, so $(H_1 \rightarrow H_2) \in F_1(X^\star)$.
4. Wenn $X^\star$ endlich, X beliebig, $X^\star \subseteq X$, so $F_2(X^\star) \subseteq F_2(X)$.
5. Wenn $X^\star$ endlich, so gilt Ableitbarkeitstheorem für F_2:

$$\text{Wenn } (H_1 \rightarrow H_2) \in F_2(X^\star)\text{, so } H_2 \in F_2(X \cup \{H_1\})$$

Dann ist für alle $X \in$ ausd:

$$F_1(X) \subseteq F_2(X)$$

Beweis: Es sei $H \in F_1(X)$ Wegen (2.6.7.2) existiert endliches $X^\star = \{H_1, \ldots, H_k\}$ mit $H \in F_1(X^\star)$.
Falls $X^\star = \emptyset$, d. h. $H \in F_1(\emptyset) \subseteq F_2(\emptyset) \subseteq F_2(X)$, sonst $H \in F_1\big(\underbrace{\{H_1, \ldots, H_{n-1}\}}_{X^\star} \cup \{H_n\}\big)$.
Mit (2.6.7.3) ergibt sich $(H_n \rightarrow H) \in F_1(\{H_1, \ldots, H_{n-2}\} \cup \{H_{n-1}\})$, usw.
$(H_1 \rightarrow (H_2 \rightarrow \cdots (H_n \rightarrow H)\cdots) \in F_1(\emptyset) \subseteq F_2(\emptyset)$.
Mit Ableitbarkeitstheorem für F_2: $\rightarrow H \in F_2(\{H_1, \ldots, H_n\}) \subseteq F_2(X)$

Anwendung:

$$\left.\begin{array}{l} \bullet\ F_1(X) = \mathrm{fl}(X) \\ \bullet\ F_2(X) = \mathrm{aba}(\mathrm{ag} \cup X). \end{array}\right\} \mathrm{fl}(X) \subseteq \mathrm{aba}(\mathrm{ag} \cup X)$$

$$\left.\begin{array}{l} \bullet\ F_1(X) = \mathrm{aba}(\mathrm{ag} \cup X) \\ \bullet\ F_2(X) = \mathrm{fl}(X) \end{array}\right\} \mathrm{aba}(\mathrm{ag} \cup X) \subseteq \mathrm{fl}(X)$$

Satz 2.6.8 (Vollständigkeitstheorem für den Aussagenkalkül)
$\mathrm{fl}(X) = \mathrm{aba}(\mathrm{ag} \cup X)$.

Die damit gegebene Charakterisierung des Folgerns durch das Ableiten mit der Abtrennungsregel allein ist noch keine rein syntaktische Charakterisierung des Folgerns, weil auf der rechten Seite der Gleichung noch die Menge ag vorkommt, die unter Bezug auf die Semantik definiert ist. Es bleibt also übrig, diese Menge syntaktisch zu charakterisieren.

2.6.1 Das Axiomensystem axa

Das Axiomensystem axa besteht aus den folgenden 15 Ausdrücken:

1. $p \rightarrow (q \rightarrow p)$ (Prämissenbelastung)
2. $((p \rightarrow q) \rightarrow p) \rightarrow p$ (Satz von Peirce)
3. $(p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow (p \rightarrow r))$ (Kettenschluß)
4. $p \wedge q \rightarrow p$

5. $p \wedge q \rightarrow q$
6. $(p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow (q \wedge r)))$
7. $p \rightarrow p \vee q$
8. $q \rightarrow p \vee q$
9. $(p \rightarrow r) \rightarrow ((q \rightarrow r) \rightarrow ((p \vee q) \rightarrow r))$
10. $(p \leftrightarrow q) \rightarrow (p \rightarrow q)$
11. $(p \leftrightarrow q) \rightarrow (q \rightarrow p)$
12. $(p \rightarrow q) \rightarrow (q \rightarrow p) \rightarrow (p \leftrightarrow q)$
13. $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$
14. $p \rightarrow \neg\neg p$
15. $\neg\neg p \rightarrow p$

Satz 2.6.9
$\mathrm{axa} \subseteq \mathrm{ag}$

Satz 2.6.10 (Widerspruchsfreiheit von axa **bezüglich** ab**)**

$$\mathrm{ab}\,(\mathrm{axa}) \subseteq \mathrm{ag}$$

Satz 2.6.11 (Vollständigkeit von axa **bezüglich** ab**)**

$$\mathrm{ab}\,(\mathrm{axa}) \supseteq \mathrm{ag}$$

Zeigen für $H^\star \in \mathrm{ausd}$:

$$\text{Wenn } H^\star \notin \mathrm{ab}\,(\mathrm{axa})\,,\ \text{so } H^\star \notin \mathrm{ag}$$

Satz 2.6.12 (Lindenbaumscher Ergänzungssatz)
$M \subseteq \mathrm{ausd}$, $H^\star \notin F\,(M)$. Es sei F ein Deduktionsoperator, dann gibt es eine Menge $M^\star$ mit

1. $M^\star \supseteq M$
2. $H^\star \notin F\,(M^\star)$
3. Für alle $H \in \mathrm{ausd}$ gilt: Wenn $H \notin F\,(M^\star)$, so $H^\star \in F\,(M^\star \cup \{H\})$.
4. $F\,(M^\star) = M^\star$.

Beweis: $\mathrm{ausd} = \{H_0, H_1, \ldots\}$.

$N_0 := M$.
$$N_{i+1} := \begin{cases} N_i \cup \{H_i\}\,, & H^\star \notin F\,(N_i \cup \{H_i\}) \\ N_i, & \text{sonst} \end{cases}$$
$M^\star = \bigcup_{i\geq 0} N_i$.

Zu 1: $M \subseteq M^\star$ ist klar.

Zu 2: $H^\star \notin F(M^\star)$

Wäre $H^\star \in F(M^\star)$, so würde es $X^\star \subseteq M^\star$ $X^\star$ – endlich geben, mit $H^\star \in F(X^\star)$. Weil $X^\star$ endlich, existiert ein k mit $X^\star \subseteq N_k$, also mit $H^\star \in F(N_k)$ $\lightning$ zur Konstruktion.

Zu 3: Sei $H = H_k \in$ ausd; $H \notin F(M^\star)$. Nach Konstruktion ist $H^\star \in F(N_k \cup \{H\})$, sonst wäre $H = H_k \in N_k \subseteq M^\star \subseteq F(M^\star)$. Also $H^\star \in F(M^\star \cup \{H\})$.

Zu 4: Es sei $H \in F(M^\star)$.

Behauptung: $H \in M^\star$
Es sei $H = H_k$.

zu zeigen: $H^\star \notin F(N_k \cup \{H_k\})$. Nun ist $H^\star \notin F(M^\star)$, also $H^\star \notin F(M^\star \cup \{H\})$, weil $H \in F(M^\star)$. $H^\star \notin F(N_k \cup \{H\})$, weil $N_k \subseteq M^\star$.

Anwendung mit $M = \text{ab}(\text{axa})$; $F = \text{aba}$

$H^\star \notin \text{aba}(\text{ab}(\text{axa}))$. (sonst $H^\star \in \text{ab}(\text{axa})$)

Es gibt $M^\star \subseteq$ ausd mit

1. $\text{ab}(\text{axa}) \subseteq M^\star$
2. $H^\star \notin \text{aba}(M^\star)$
3. Für alle H: Wenn $H \notin \text{aba}(M^\star)$, so $H^\star \in \text{aba}(M^\star \cup \{H\})$.
4. $\text{aba}(M^\star) = M^\star$.

Folgerung: Wenn $(M^\star \cup \{H_1\})\,\text{abla}H_2$, so $M^\star \text{abla}(H_1 \to H_2)$.

zu zeigen: $p \to p, (p \to (q \to r)) \to ((p \to q) \to (p \to r)) \in \text{ab}(\text{axa})$

Lemma 1:

$$\begin{aligned}
(H_1 \to H_2) \in M^\star &\text{ gdw. Wenn } H_1 \in M^\star, \text{ so } H_2 \in M^\star \\
H_1 \wedge H_2 \in M^\star &\text{ gdw. } H_1 \in M^\star \text{ und } H_2 \in M^\star \\
H_1 \vee H_2 \in M^\star &\text{ gdw. } H_1 \in M^\star \text{ oder } H_2 \in M^\star \\
H_1 \leftrightarrow H_2 \in M^\star &\text{ gdw. } H_1 \in M^\star \text{ gdw. } H_2 \in M^\star \\
\neg H_2 \in M^\star &\text{ gdw. } H_1 \notin M^\star
\end{aligned}$$

Beweis: $(\to)$

$$\left.\begin{array}{l}(H_1 \to H_2) \in M^\star \\ H_1 \in M^\star\end{array}\right\} \Rightarrow H_2 \in M^\star \text{ wegen Abtrennungsregel.}$$

$(\leftarrow)$
Wenn $H_1 \in M^\star$, so $H_2 \in M^\star$, d. h. $H_1 \notin M^\star$ oder $H_2 \in M^\star$. Sei zunächst $H_1 \notin M^\star$, dann ist $H^\star \in \text{aba}(M^\star \cup \{H\})$, also

$(H_1 \to H^\star) \in \text{abla}(M^\star)$
Ann.: $(H_1 \to H_2) \notin M^\star$
Dann: $(H_1 \to H_2) \to H^\star \in \text{aba}(M^\star)$ und $(H_1 \to H^\star) \to ((H_1 \to H_2) \to H^\star) \to H^\star) \in \text{ab}(\text{axa}) \subseteq M^\star$, d. h. weil $M^\star$ abgeschlossen gegen Abtrennung: $H^\star \in M^\star$
$\lightning$.

Bleibt: $H_2 \in M^\star$ Es ist $H_2 \to (H_1 \to H_2) \in \text{ab}(\text{axa}) \subseteq M^\star$ (Prämissenbelastung) $\to H_1 \to H_2 \in M^\star$.

(Rest ohne Beweis)

Jetzt geben wir eine Belegung $\beta^\star$ an, die H falsch macht:

$$\beta^\star(p_i) = \begin{cases} W, & p_i \in M^\star \\ F, & \text{sonst} \end{cases}$$

Lemma 2: wert $(H, \beta^\star) = W$ gdw. $H \in M^\star$,
($\rightarrow$wert $(H^\star, \beta^\star) = F$, d. h. $H^\star \notin$ ag

Beweis: Induktion über H

A) H ist AV p_i
wert $(H, \beta^\star) = \beta^\star(p_i) = W$ gdw. $p_i \in M^\star$

I) $H \rightarrow \neg H$
wert $(\neg H, \beta^\star) = W$ gdw. wert $(H, \beta^\star) = F$ gdw. $H \notin M^\star$ gdw. $\neg H \in M^\star$

analog weiter.

$\boxed{\text{Ist } H \in \text{ag?}}$ Wie sieht ein syntaktisches Verfahren zur Entscheidung dieser Frage aus?

1. Maschine, die alle Ausdrücke aus AXA = ab (axa) aufzählt: $H_1, H_2, H_3, \ldots$
2. Maschine (Abtrennungs-): $\{H_1\}$ abla$H$
   $\{H_1, H_2\}$ abla$H$
   $\{H_1, \ldots H_n\}$ abla$H$
3. Nachsehen, ob H erzeugt wurde
   - falls ja: stop
   - nein: weiter

Wenn $H \in$ ag, so erhalten wir einen Ruhezustand: „ja“. Wenn $H \notin$ ag, so hält das Verfahren nicht an.

Wir wissen: Wenn $H \notin$ ag, so ab (ag $\cup \{H\}$) = ausd, d. h. (ag $\cup \{H\}$) abl $(p \wedge \neg p)$, d. h. ein Widerspruch ist ableitbar.

Programm

1. Zeichen für Widerspruch $\perp$

2. Ausdrücke normalisieren

3. Abtrennungsregel anpassen

1. Das Zeichen $\perp$ wird in das Alphabet des AK aufgenommen. Die Ausdrucksdefinition wird im Anfangsschritt ergänzt:

   „$\perp$“ ist ein Ausdruck Setzen fest: wert $(\perp, \beta) = F$, für alle $\beta \in \mathfrak{B}$.

   Die Menge $\{\perp\}$ hat kein Modell. $\perp \in$ fl (X) gdw. X kein Modell besitzt (X widersprüchlich ist).

2. Einschränkung der Ausdrucksmenge:

Definition 2.6.13 (GENTZEN-**Ausdruck (Klausel)**)
Ein Ausdruck $H \in$ ausd heißt Klausel, wenn H eine der Formen hat:

- $p_1 \wedge p_2 \wedge \cdots \wedge p_m \rightarrow q_1 \vee q_2 \vee \cdots \vee q_n \quad (m, n \geq 1)$
- $q_1 \vee q_2 \vee \cdots \vee q_n \; (n \geq 1)$
- $p_1 \wedge \cdots \wedge p_m \rightarrow \perp \; (m \geq 1)$
- $\perp$

Wobei $p_1, \ldots, p_m, q_1, \ldots, q_n$ paarweise verschiedene AV sind.

Ausdrucksfähigkeit?

Definition 2.6.14
Ausdrücke H_1, H_2 heißen semantisch äquivalent $H_1 \sim_{\text{sem}} H_2$ gdw. $(H_1 \leftrightarrow H_2) \in$ ag

Satz 2.6.15
Jeder Ausdruck H ist semantisch äquivalent zu einer Konjunktion von Klauseln.

$$H \sim_{\text{sem}} K_1 \wedge K_2 \wedge \cdots \wedge K_m$$

$\neg\perp \sim_{\text{sem}} (p \rightarrow p)$.

o. B. d. A. seien $p_1, \ldots, p_n$ die AV in H.

Fall 1: $H \in$ ag.
$$H \sim_{\text{sem}} \underbrace{(p_1 \rightarrow p_1)}_{\text{Klausel}} \wedge (p_2 \rightarrow p_2) \wedge \cdots \wedge (p_n \rightarrow p_n)$$
Fall 2: $H \notin$ ag
es gibt Belegung β mit $\text{wert}(H, \beta) = F$. Zu jeder Belegung β betrachten wir $A_\beta := [\neg]^{\beta(p_1)} p_1 \vee \cdots \vee [\neg]^{\beta(p_n)} p_n$.
Wobei: $[\neg]^F := e \quad [\neg]^W := \neg$.

Beispiel: $\begin{matrix} p_1 & p_2 & p_3 \\ F & W & F \end{matrix} \rightarrow A_\beta = p_1 \vee \neg p_2 \vee p_3$.

Lemma: $\text{wert}(A_\beta, \beta^\star) = F$ gdw. $\beta(p_i) = \beta^\star(p_i), i = 1, \ldots, n$

Behauptung

$$H \sim_{\text{sem}} \bigwedge_{\text{wert}(H,\beta)=F} A_\beta$$

Beweis: **z. z.:** $(H \leftrightarrow A_1 \wedge \cdots \wedge A_k) \in$ ag

$\text{wert}(H, \beta) = F$ gdw. $\text{wert}(A_1 \wedge \cdots \wedge A_k, \beta) = F$ gdw. es gibt ein i mit $\text{wert}(A_i, \beta) = F$.

Kanonische Konjunktive NF

n. z. z.: Jedes A_β ist semantisch äquivalent zu einer Klausel

Fälle

(a) A_β hat kein $\neg$: $p_1 \vee p_2 \vee \cdots \vee p_n$. (Das ist eine Klausel)

(b) alle AV mit $\neg$: $\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n \sim_{\text{sem}} p_1 \wedge p_2 \wedge \cdots \wedge p_n \to \bot$. (Klausel)

(c) sonst: A_β ist semantisch äquivalent zu $r_1 \wedge \cdots \wedge r_i \to r_{i+1} \vee \cdots \vee r_n$. (Klausel)

3. Die Schnittregel
Cut (H_1, H_2, H) („durch Anwendung der Schnittregel auf Klauseln H_1, H_2 entsteht eine Klausel H")

$$\frac{\left.\begin{array}{c} H_1 : [L \to]\, q_1 \vee \cdots \vee q_n \\ H_2 : p_1 \wedge \cdots \wedge p_m \to R \end{array}\right\}\text{Klauseln} \qquad \text{es gibt } i, k \text{ mit } 1 \leq i \leq n, 1 \leq k \leq m \text{ und } q_i = p_k.}{H : [L]\, p_1 \wedge \cdots \wedge p_{k-1} \wedge p_{k+1} \wedge \cdots \wedge p_m \to R \vee q_1 \vee \cdots \vee q_{i-1} \vee q_{i+1} \cdots \vee q_n}$$

„semantisch äquivalent vereinfacht"

Satz 2.6.16 (Rechtfertigung der Schnittregel)
Wenn Cut (H_1, H_2, H), so $H \in \text{fl}\,(\{H_1, H_2\})$.

Wenn β Modell von $\{H_1, H_2\}$, so $\beta \text{erf}\, H$.

Annahme: wert $(H, \beta) = F$

$\to$ wert $(L, \beta) = W$, für $j = 1, \ldots, n$ mit $j \neq k$ $\beta\,(p_j) = W$
wert $(R, \beta) = F$, für $j = 1, \ldots, m$ mit $j \neq k$ $\beta\,(p_j) = W$

Betrachten H_2.
Nach Voraussetzung wert $(H_2, \beta) = W$ wegen wert $(R, \beta) = F_i$
wert $(p_0 \wedge \cdots \wedge p_n, \beta) = F$

$$\beta\,(p_k) = F = \beta\,(q_i)$$

$\to$wert $(H_1, \beta) = F$ $\lightning$

Cut-Ableitbarkeit $Y \vdash H$

Y sei Menge von Klauseln, H eine Klausel.

A) Wenn $H \in Y$, so $Y \vdash H$

I) Wenn $H_1, H_2 \in Y$ mit Cut (H_1, H_2, H), so $Y \vdash H$

sonst nichts.

wissen: Wenn $Y \vdash H$, so $H \in \text{fl}\,(Y)$

Satz 2.6.17
Wenn $\bot \in \text{fl}\,(Y)$ (d. h. Y hat kein Modell) und $(Y \cup \{p_i \to \bot\}) \vdash \bot$, so $Y \vdash \bot$

Lemma: Wenn $(Y \cup \{p_i\}) \vdash \bot$, so $(Y \vdash \bot)$.

Hilfssatz: Wenn $(Y \cup \{p_i\}) \vdash \bot$, so $Y \vdash \bot$ oder $Y \vdash (p_i \to \bot)$.

Betrachten eine Ableitung von $\bot$ aus $Y \cup \{p_i\}$.

Fall 1: p_i wird nicht benutzt, dann $Y \vdash \bot$.

Fall 2: p_i benutzt
lasse diese Cut-Schritte heraus.
$\to$ Fall A: $Y \vdash \bot$.
Fall B: $Y \vdash (p_i \to \bot)$.

qed. HS

Zurück zum Lemma

aus $Y \cup \{p_i\} \vdash \bot$. Nach HS haben wir

entweder: $Y \vdash \bot \to$ fertig.

oder: $Y \vdash (p_i \to \bot)$ wegen $Y \cup \{p_i\} \vdash p_i$ und Schnittregel ergibt sich $Y \vdash \bot$.

qed. Lemma

Zurück zum Satz

Indirekt:

zeigen: Wenn $Y \nvdash \bot$, so hat Y ein Modell.
Lindenbaumsche Konstruktion:

$$\begin{array}{lcl} Y_0 & := & Y \\ Y_{n+1} & := & \begin{cases} Y_n \cup \{p_n\}\,, & \text{falls } (Y_n \cup \{p_n\} \nvdash \bot) \\ Y_n \cup \{p_n \to \bot\}\,, & \text{sonst.} \end{cases} \\ Y^\star & := & \text{kleinste Menge von Klauseln, die alle } Y_i \text{ enthält und} \\ & & \text{abgeschlossen ist in Bezug auf die Schnittregel.} \end{array}$$

Dann:

1. $Y \subseteq Y^\star$
2. Für jede AV p_i ist $p_i \in Y^\star$ oder $(p_i \rightarrow \bot) \in Y^\star$
3. $Y^\star \nvdash \bot$ (wegen Endlichkeitssatz)

betrachten β mit

$$\beta(p_i) := \begin{cases} W, & \text{falls } p_i \in Y^\star \\ F, & \text{falls } (p_i \rightarrow \bot) \in Y^\star \end{cases}$$

Behauptung β ist Modell von Y.

Zu zeigen: Wenn $\mathrm{wert}(H, \beta) = F$, so $H \notin Y$. $H : p_1 \wedge \cdots \wedge p_m \rightarrow q_1 \vee \cdots \vee q_n$ $\mathrm{wert}(H, \beta) = F$

Für $i = 1, \ldots, m$ ist $\beta(p_i) = W$, d. h. $p_i \in Y^\star$
$j = 1, \ldots, n$ ist $\beta(p_i) = F$, d. h. $(q_j \rightarrow \bot) \in Y^\star$

Es gilt:
$\mathrm{Cut}(p_1 \wedge \cdots \wedge p_m \rightarrow q_1 \vee \cdots \vee q_n, p_1, p_2 \wedge \cdots \wedge p_m \rightarrow q_1 \vee \cdots \vee q_n)$
$\mathrm{Cut}(p_2 \wedge \cdots \wedge p_m \rightarrow q_1 \vee \cdots \vee q_n, p_2, p_3 \wedge \cdots \wedge p_m \rightarrow q_1 \vee \cdots \vee q_n)$
$\vdots$
$\mathrm{Cut}(p_m \rightarrow q_1 \vee \cdots \vee q_n, p_m, q_1 \vee \cdots \vee q_n)$
$\mathrm{Cut}(q_1 \vee \cdots \vee q_n, q_1 \rightarrow \bot, q_2 \vee \cdots \vee q_n)$
$\vdots$
$\mathrm{Cut}(q_n, q_n \rightarrow \bot, \bot)$

Wäre $H \in Y$, so hätten wir $H \in Y^\star$ und folglich $Y^\star \vdash \bot$ in Widerspruch zu 3. Also ist $H \notin Y$, was zu zeigen war.

Satz 2.6.18
Es sei Y eine Menge von Klauseln, die ein Modell hat; $\bot \notin \mathrm{fl}(Y)$.

Dann gilt für alle Aussagenvariablen p_i

1. Wenn $p_i \in \mathrm{fl}(Y)$, so $Y \vdash p_i$
2. Wenn $(p_i \vdash \bot) \in \mathrm{fl}(Y)$, so $Y \vdash (p_i \rightarrow \bot)$.

(Die Schnittregel ist vollständig für das Folgern von Formeln der Form p_i bzw. $(p_i \rightarrow \bot)$).

Beweis. Sei $p_i \in \mathrm{fl}(Y)$, d. h. jedes Modell von Y erfüllt p_i, folglich

$$\bot \in \mathrm{fl}(fl(Y \cup \{p_i \rightarrow \bot\})),$$

d. h. kein Modell von Y erfüllt $(p_i \rightarrow \bot)$. Nach Satz 2.6.17 folgt: $(Y \cup \{p_i \rightarrow \bot\}) \vdash \bot$. Eine entsprechende Ableitung nehmen wir her und lassen die Schritte heraus, wo $p_i \rightarrow \bot$ benutzt wird. Es entsteht ein Beweis für $Y \vdash \bot$ oder für $Y \vdash p_i$. $Y \vdash \bot$ kann nicht sein, weil Y ein Modell hat, also $Y \vdash p_i$.

Damit ist 1. bewiesen, 2. zeigt man analog.

Satz 2.6.19
Wenn Y endliche Menge von Klauseln ist, so ist der Schnittregelabschluß von Y endlich.

Beweis Die Menge der AV, die in Klauseln in Y vorkommen ist endlich. Die Menge der AV, die in Schnittregelabschluß von Y vorkommen ist endlich.

Damit erhalten wir ein Entscheidungsverfahren für $H \in \mathrm{ag}$?

$H \in \mathrm{ag}$ gdw. $\{\neg H\}$ hat kein Modell.

Es sei Y eine Menge von Klauseln mit

$$K_j(Y) \sim_{\mathrm{sem}} \neg H$$

$H \in \mathrm{ag}$ gdw. Y hat kein Modell gdw. $\perp \in \mathrm{fl}(Y)$ gdw. $Y \vdash \perp$.

H gegeben:

1. Berechne Y. (endliche Menge von Klauseln mit $K_j(Y) \sim_{\mathrm{sem}} \neg H$)
2. Berechne $Y^\star :=$ Schnittregelabschluß(Y).
3. $\perp \in Y^\star$, gdw. ag$H$

Beispiel:

$$\begin{array}{rcl} H & = & p \to (q \to p) \\ \neg H & = & \neg(p \to (q \to p)) \end{array}$$

Berechnung von Y:

1. Elimination von $\to$:
$$\neg(p \to (\neg q \vee p))$$
$$\neg(\neg p \vee (\neg q \vee p))$$
2. $\neg$ vor die Variablen treiben, $\neg\neg$ weglassen
$$p \wedge \neg(\neg q \vee p)$$
$$p \wedge q \wedge \neg p$$

$Y = \{p, q, p \to \perp\}$

Offenbar Cut$(p, p \to \perp, \perp)$, also $\perp \in Y^\star$, d. h. $H \in \mathrm{ag}$.

2.7 Widerspruchsfreiheit, Vollständigkeit, Nichtableitbarkeit in AK $[X, \mathrm{ausd}, \mathrm{ag}, \mathrm{ab}]$

Definition 2.7.1 (Widerspruchsfreiheit)

1. (Gödel)
   $X \subseteq \mathrm{ausd}$ heißt semantisch widerspruchsfrei genau dann, wenn $\mathrm{ab}(X) \subseteq \mathrm{ag}$
2. (Hilbert)
   X heißt klassisch widerspruchsfrei genau dann, wenn es keinen Ausdruck $H \in \mathrm{ausd}$ mit $H \in \mathrm{ab}(X)$ und $\neg H \in \mathrm{ab}(X)$ gibt.
3. (Post)
   X heißt syntaktisch widerspruchsfrei genau dann, wenn $\mathrm{ab}(X) \neq \mathrm{ausd}$.

Satz 2.7.2

1. Wenn X semantisch widerpruchsfrei, so ist X klassisch widerpruchsfrei.
2. Wenn X klassisch widerspruchsfrei, so X syntaktisch widerspruchsfrei.
3. Die Umkehrungen gelten nicht.

Beweis:
zu 1: weil niemals H und $\neg H$ zugleich allgemeingültig
zu 2: p, $\neg p$ sind nicht beide ableitbar, also $\mathrm{ab}\,(X) \neq \mathrm{ausd}$.
zu 3: $X_1 = \{\neg\,(p \to p)\} \not\subseteq \mathrm{ag}$. X_1 nicht semantisch widerspruchsfrei.

$\mathrm{ab}\,(X_1) = \{\neg\,(H \to H)\,|H \in \mathrm{ausd}\}$ klassisch widerspruchsfrei.
$X_2 = \{p \to p, \neg\,(p \to p)\}$ nicht klassisch widerspruchsfrei

Behauptung: $p \notin \mathrm{ab}\,(X_2)$. d. h. X_2 syntaktisch widerspruchsfrei.

Beweis: später (siehe unten), nicht ableitbar.

Satz 2.7.3

	semantisch		jede endlich Teilmenge
X ist	klassisch	widerspruchsfrei gdw.	$X^\star$ von X diese
	syntaktisch		Eigenschaft hat.

Beweis: $(\to)$
semantisch

$$\mathrm{ab}\,(X^\star) \subseteq \mathrm{ab}\,(X) \subseteq \mathrm{ag}$$

klassisch

$$\mathrm{ab}\,(X^\star) \subseteq \mathrm{ab}\,(X) \subseteq \mathrm{ag}$$

und es gibt kein $H \in \mathrm{ab}\,(X)$ mit $\neg H \in \mathrm{ab}\,(X)$

syntaktisch

$$\mathrm{ab}\,(X^\star) \subseteq \mathrm{ab}\,(X) \neq \mathrm{ausd}$$

$(\leftarrow)$
semantisch
Für $H \in X$ gilt:

$$\mathrm{ab}\,(\{H\}) \subseteq \mathrm{ag} \to H \in \mathrm{ag}$$

folglich $X \subseteq \mathrm{ag}$
und $\mathrm{ab}\,(X) \subseteq \mathrm{ag}$.
klassisch indirekt:

$$H^\star \in \mathrm{ab}\,(H)\,, \neg H^\star \in \mathrm{ab}\,(X)$$

Nach Endlichkeitssatz: Es gibt endliche $X^\star \subseteq X$ mit $H^\star \in \mathrm{ab}\,(H^\star)$ und es gibt $X^{\star\star}$ mit $\neg H^\star \in \mathrm{ab}\,(X^{\star\star})$

Folglich $H, \neg H \in \mathrm{ab}\,(X^\star \cup X^{\star\star})$. Das ist eine endlich Teilmenge von X, die klassisch nicht widerpruchsfrei ist. ↯

syntaktisch: $\mathrm{ab}\,(X) \subset \mathrm{ausd}$
indirekt: $\mathrm{ab}\,(X) = \mathrm{ausd}$.

$p \in \mathrm{abl}\,(X)$ endliche $X^\star$ mit $p \in \mathrm{ab}\,(X^\star) = \mathrm{ausd}$.

$\to X^\star$ nicht syntaktisch widerspruchsfrei. ↯

Definition 2.7.4 (Vollständigkeit)

1. $X \subseteq$ ausd heißt semantisch vollständig genau dann, wenn $\mathrm{ab}\,(X) \supseteq$ ag
2. $X \subseteq$ ausd heißt klassisch vollständig genau dann, wenn für jedes $H \in$ ausd gilt $H \in \mathrm{ab}\,(X)$ oder $\neg H \in \mathrm{ab}\,(X)$.
3. $X \subseteq$ ausd heißt syntaktisch vollständig genau dann, wenn für jedes $H \in$ ausd gilt: Wenn $H \notin \mathrm{ab}\,(X)$, so $\mathrm{ab}\,(X \cup \{H\}) =$ ausd

Bemerkung:

1. axa ist semantisch widerspruchsfrei und semantisch vollständig.
2. Es gibt im AK keine klassisch vollständige und klassisch widerspruchsfreie Menge X.

Beweis: X – klassisch vollständig
Betrachtet p.

$$\underbrace{\underbrace{p \in \mathrm{ab}\,(X)}_{\mathrm{ab}\,(X) = \mathrm{ausd}.}}_{\substack{\text{nicht syntaktisch}\\ \text{widerpruchsfrei}}} \qquad \text{oder} \qquad \underbrace{\neg p \in \mathrm{ab}\,(X)}_{\text{in } \neg p \; p \text{ ersetzen durch } \neg p}$$

$$\downarrow \qquad\qquad\qquad\qquad \to \neg\neg p \in \mathrm{ab}\,(X)$$

nicht klassisch widerpruchsfrei $\qquad\qquad$ $\to X$ nicht klassisch widerspruchsfrei

Satz 2.7.5

1. Wenn X semantisch vollständig, so ist X syntaktisch vollständig.
2. Umkehrung gilt nicht

Behauptung: Es sei $H \notin \mathrm{ab}\,(X)$, und ag $\subseteq \mathrm{ab}\,(X)$.

Dann ist $H \notin$ ag also $\mathrm{ab}\,(\mathrm{ag} \cup \{H\}) =$ ausd.

Folglich $\mathrm{ab}\,(\mathrm{ab}\,(X) \cup \{H\}) = \mathrm{ab}\,(X \cup \{H\}) =$ ausd

Beweis von (2.7.5.2)

$$X = \{\neg p\}\,.$$

$\mathrm{ab}\,(X) = \{\neg H | H \in \mathrm{ausd}\} \subset \mathrm{ausd}, X$ syntaktisch widerspruchsfrei.

Nach Lindenbaum existiert eine Menge Y mit

1. $Y \supseteq X = \{\neg p\}$
2. Y ist syntaktisch widerspruchsfrei und syntaktisch vollständig
3. $\mathrm{ab}\,(Y) = Y$

Y ist nicht semantisch vollständig, d. h. ag $\not\subseteq \mathrm{ab}\,(Y)$

sonst wäre axa $\subseteq \mathrm{ab}\,(Y)$ und $\neg p \in Y \setminus \mathrm{axa} \subseteq Y$ d. h. $\mathrm{ab}\,(\mathrm{axa} \cup \{\neg p\}) = \mathrm{ausd} \subseteq Y$

d. h. Y – nicht syntaktisch widerspruchsfrei $\lightning$.

Problem:
$p \notin \mathrm{ab}\,(\{p \to p, \neg\,(p \to p)\})$. Wie beweist man das?

Leicht: $H \notin \underbrace{\mathrm{ab}\,(\mathrm{axa})}_{\mathrm{ag}}$ (zeigen $H \notin \mathrm{ag}$) entscheidbar

Vermutung: Ableitbarkeit semantisch charakterisieren. Die klassische logische Matrix $[\{W, F\}, \{W\}, \mathrm{non}, \mathrm{et}, \mathrm{vel}, \mathrm{seq}, \mathrm{aeq}]$ ersetzen durch eine Matrix $\mu = [M, M^\star, \Phi_1, \Phi_2, \ldots, \Phi_5]$

$\beta \mathrm{erf}_\mu H$ (über μ) genau dann, wenn $\mathrm{wert}_\mu\,(H, \beta) \in M^\star$.

$\mathrm{ag}_\mu =$ Menge der $H \in$ ausd mit Für alle $\beta \in \mathfrak{B}_\mu \rightarrow \mathrm{wert}_\mu\,(H.\beta) \in M^\star$.

Satz 2.7.6
$\mathrm{abe}\left(\mathrm{ag}_\mu\right) = \mathrm{ag}_\mu$ für jede logische Matrix μ

Beweis: Man zeigt durch Induktion über H:
Wenn $H = H_1\left(p/_{H^\star}\right)$ und $H_1 \in \mathrm{ag}_\mu$, so $H \in \mathrm{ag}_\mu$.

Für aba gilt das nicht, betrachten wir als Beispiel die Matrix $\mu_0 = [\{W, F\}, \{W\}, \mathrm{non}, \mathrm{et}, \mathrm{vel}, \Phi_4, \mathrm{aeq}]$ mit $\Phi_4\,(w, w') \equiv W$. Hierbei ist $(p \rightarrow p) \in \mathrm{ag}_{\mu_0}$ und $((p \rightarrow p) \rightarrow p) \in \mathrm{ag}_{\mu_0}$, d. h. $p \in \mathrm{aba}\left(\mathrm{ag}_{\mu_0}\right)$, aber $p \notin \mathrm{ag}_{\mu_0}$.

Hinreichend für die Widerspruchsfreiheit der Abtrennungsregel:

$$\text{Wenn } w \in M^\star \text{ und } \Phi_4\,(w, w') \in M^\star, \text{ so } w' \in M^\star.$$

$$\text{d. h. Wenn } w \in M^\star \text{ und } w' \in M \setminus M^\star, \text{ so } \Phi_4\,(w, w') \in M \setminus M^\star. \tag{2.7.5}$$

Definition 2.7.7
Eine logische Matrix μ heißt normal, wenn Φ_4 die Bedingung 2.7.5 erfüllt.

Folgerung: μ–normal, so ist $\mathrm{ab}\left(\mathrm{ag}_\mu\right) = \mathrm{ag}_\mu$.

Satz 2.7.8 (Satz von Lindenbaum**)**
Zu jeder Menge $X \subseteq$ ausd gibt es eine höchstens abzählbare normale logische Matrix μ mit $\mathrm{ab}\,(X) \subseteq \mathrm{ag}_\mu$.

Beweis: $\mu = [\mathrm{ausd}, \mathrm{ab}\,(X)\,; \Phi_1, \ldots, \Phi_5]$ mit $\Phi_1\,(H) = \neg H$, $\Phi_2\,(H_1, H_2) = (H_1 \wedge H_2)$, $\Phi_3(H_1, H_2) = (H_1 \vee H_2)$, $\Phi_4\,(H_1, H_2) = (H_1 \rightarrow H_2)$, $\Phi_5\,(H_1, H_2) = (H_1, \leftrightarrow H_2)$.

normal: Sei $H \in \mathrm{ab}\,(X)$ und $(H \rightarrow H') \in \mathrm{ab}\,(X)$, so $H' \in \mathrm{ab}\,(X)$. (Abtrennungsregel)

1. Sei $H \in \mathrm{ag}_\mu$, d. h. $\mathrm{wert}_\mu\,(H, \beta) \in \mathrm{ab}\,(X)$ für alle $\beta \in \mathfrak{B}_\mu$.

$$\beta : \mathrm{AV} \rightarrow \mathrm{ausd}.$$

also speziell für $\beta^\star$ mit

$$\beta^\star\,(p_i) = p_i\colon \underbrace{\mathrm{wert}_\mu\,(H, \beta^\star)}_{H} \in \mathrm{ab}\,(X)$$

$(\leftarrow)$ Sei $H \in \mathrm{ab}\,(X)$ z. z. $H \in \mathrm{ag}_\mu$.

$$\begin{gathered} \mathrm{abe}\,(\{H\}) \subseteq \mathrm{ab}\,(X)\,. \\ \{\mathrm{wert}_\mu\,(H, \beta)\,|\beta\text{–Belegung}\} \subseteq \mathrm{ab}\,(X) \\ \rightarrow H \in \mathrm{ag}_\mu \end{gathered}$$

Bemerkung: Es geht im allgemeinen nicht mit einer endlichen Matrix.

Satz 2.7.9 (Semantische Charakterisierung von ab**)**
Es ist $H \in \mathrm{ab}\,(X)$ genau dann, wenn für jede normale höchstens abzählbare logische Matrix μ mit $X \subseteq \mathrm{ag}_\mu$ stets $H \in \mathrm{ag}_\mu$.

Beweis: $(\rightarrow)$
Es sei $X \mathrm{abl} H$ $(H \in \mathrm{ab}\,(X))$ μ–normal $X \subseteq \mathrm{ag}_\mu$

Dann ist $H \in \mathrm{ab}\,(X) \subseteq \mathrm{ag}_\mu$ (weil μ–normal) also $H \in \mathrm{ag}_\mu$

$(\leftarrow)$

$$H \in \bigcap_{\substack{\mu\text{–normal} \\ X \subseteq \mathrm{ag}_\mu}} \mathrm{ag}_\mu$$

Nach Satz von Lindenbaum gibt es $\mu^\star$ mit $\mathrm{ab}\,(X) = \mathrm{ag}_{\mu^\star}$. Dabei $X \subseteq \mathrm{ag}_{\mu^\star}$. Folglich $H \in \mathrm{ag}_{\mu^\star} = \mathrm{ab}\,(X)$. d. h. $H \in \mathrm{ab}\,(X)$.

Folgerung 2.7.10 (Satz über Nichtableitbarkeit)
$H \notin \mathrm{ab}\,(X)$ genau dann, wenn es eine höchstens abzählbare logische Matrix μ mit $X \subseteq \mathrm{ag}_\mu$ und $H \notin \mathrm{ag}_\mu$ gibt.

Beispiel:

$$\begin{gathered} p \notin \mathrm{ab}\,(\{p \rightarrow p, \neg\,(p \rightarrow p)\}) \\ \mu = [\{W, F\}, \{W\}, \Phi_1, \mathrm{et}, \mathrm{vel}, \mathrm{seq}, \mathrm{aeq}] \\ \Phi_1 : \Phi_1\,(W) = W, \Phi_1\,(F) = F. \end{gathered}$$

μ normal, da $\Phi_4 = \mathrm{seq}$.

$$\begin{aligned} \mathrm{wert}_\mu\,(p \rightarrow p, \beta) &= \mathrm{seq}\,(\beta\,(p)\,, \beta\,(p)) = W \in \{W\} \\ &\hphantom{=} \qquad\qquad\qquad\qquad\quad p \rightarrow p \in \mathrm{ag}_\mu \\ \mathrm{wert}_\mu\,(\neg\,(p \rightarrow p)\,, \beta) = \Phi_1\,(\mathrm{wert}\,(p \rightarrow p, \beta)) &= \mathrm{wert}_\mu\,(p \rightarrow p, \beta) \in \{W\} \end{aligned}$$

aber $\beta^\star\,(p) = F \rightarrow \mathrm{wert}_\mu\,(p, \beta^\star) = F$ d. h. $p \notin \mathrm{ag}_\mu$.

Satz 2.7.11
axa ist unabhängig, d. h. wenn $H \in \mathrm{axa}$, so $\mathrm{ab}\,(\mathrm{axa} \setminus \{H\}) \neq \mathrm{ag}$. $(H \notin \mathrm{ab}\,(\mathrm{axa} \setminus \{H\}).)$

Dualitätstheorem

Alphabet $A = \{M, \star, \cup, \cap, \bar{}, =, (,)\}$

Syntax: Induktive Definition von Mengenvariablen:

A) M ist eine Mengenvariable.

I) Wenn das Wort $\mathcal{Z}$ eine Mengenvariable ist, so auch $\mathcal{Z}\star$.

E) sonst nichts.

$$\begin{array}{ccccccc} MV & := & \{ & M, & M\star, & M\star\star, & \ldots & \} \\ & & & = & = & = & \text{usw.} \\ & & & M_1 & M_2 & M_3 & \end{array}$$

Mengenterme:

A) Jede Mengenvariable ist ein Mengenterm

I) 1. Ist T_1 ein Mengenterm, so ist $\overline{T_1}$ ein Mengenterm

2. Sind T_1, T_2 Mengenterme, so sind $(T_1 \cup T_2)$, $(T_1 \cap T_2)$ Mengenterme.

E) Sonst nichts.

Gleichungen: Sind T_1, T_2 Mengenterme, so heißt

$$T_1 = T_2$$

Gleichung.

Eine Abbildung $f : \{M_0, \ldots\} \to \mathfrak{P}(E)$ heißt Belegung.

Die von einem Term T bei einer Belegung f beschriebene Menge Set (T, f)

A) $\operatorname{Set}(M_i, f) := f(M_i)$

I) $\operatorname{Set}(\overline{T}, f) := \overline{\operatorname{Set}(T, f)} = E \setminus \operatorname{Set}(T, f)$
$\operatorname{Set}(T_1 \overset{\cup}{\cap} T_2, f) = \operatorname{Set}(T_1, f) \overset{\cup}{\cap} \operatorname{Set}(T_2, f)$

Eine Gleichung $G = T_1 = T_2$ heißt gültig $:\leftrightarrow$ Für alle Belegungen f ist $\operatorname{Set}(T_1, f) = \operatorname{Set}(T_2, f)$.

Satz 2.7.12 (Dualitätstheorem)
Ist G eine gültige Gleichung und entsteht G' aus G indem gleichzeitig an allen Stellen „$\cap$" durch „$\cup$" und „$\cup$" durch „$\cap$" ersetzt wird, dann ist G' gültig.

Beispiel:

$$\begin{array}{ccc} (M_0 \cup M_1) & = & \overline{(\overline{M_0} \cap \overline{M_1})} \\ & \downarrow & \\ (M_0 \cap M_1) & = & \overline{(\overline{M_0} \cup \overline{M_1})} \end{array}$$

Beweis durch Reduktion auf das Dualitätstheorem der Aussagenlogik. Zu jedem Term T konstruieren wir einen Ausdruck H_T:

A) $T \equiv M_i \quad H_T \equiv p_i$

I) $$\begin{array}{ll} T \equiv \overline{T'} & H_T \equiv \neg H_{T'} \\ T \equiv (T_1 \cup T_2) & H_T \equiv (H_{T_1} \vee H_{T_2}) \\ T \equiv (T_1 \cap T_2) & H_T \equiv (H_{T_1} \wedge H_{T_2}) \end{array}$$

Hilfssatz Sei T Mengenterm, $a \in E$ und f Belegung, ferner

$$\beta_{a,f}(p_i) := \begin{cases} W, & \text{falls } a \in f(M_i) \\ F, & \text{sonst} \end{cases}$$

Dann gilt:

$$a \in \operatorname{Set}(T, f) \text{ gdw. } \operatorname{wert}(H_T, \beta_{a,f}) = W$$

Beweis durch Induktion über T

A) $T = M_i$
$a \in \mathrm{Set}(M_i, f) = f(M_i)$ gdw. wert $(p_i, \beta_{a,f}) = W$ gilt.

$$
\begin{array}{rll}
\text{I)} \quad a \in \mathrm{Set}\left(\overline{T}, f\right) & \text{gdw.} & a \in \overline{\mathrm{Set}\,(T, f)} \\
& \text{gdw.} & \text{nicht } a \in \mathrm{Set}\,(T, f) \\
& \text{gdw.} & \text{nicht wert}\,(H_T, \beta_{a,f}) = W \\
& \text{gdw.} & \text{wert}\,(H_T, \beta_{a,f}) = F \\
& \text{gdw.} & \text{wert}\,(\neg H_T, \beta_{a,f}) = W \\
& \text{gdw.} & \text{wert}\left(H_{\overline{T}}, \beta_{a,f}\right) = W \\
a \in \mathrm{Set}\,(T_1 \cap T_2, f) & \text{gdw.} & a \in \mathrm{Set}\,(T_1, f) \text{ und } a \in \mathrm{Set}\,(T_2, f) \\
& \text{gdw.} & \text{wert}\,(H_{T_1}, \beta_{a,f}) = W \text{ und wert}\,(H_{T_2}, \beta_{a,f}) = W \\
& \text{gdw.} & \text{wert}\,(H_{T_1} \wedge H_{T_2}, \beta_{a,f}) = W \\
& \text{gdw.} & \text{wert}\,(H_{T_1 \cap T_2}, \beta_{a,f}) = W
\end{array}
$$

analog für $T = T_1 \cup T_2$.

Satz 2.7.13
$T_1 = T_2$ gültig gdw. H_{T_1}, H_{T_2} semantisch äquivalent
$\updownarrow$
für alle f : Set $(T_1, f) =$ Set (T_2)
$\updownarrow$
für alle f, alle $a \in E$: $a \in$ Set (T_1, f) gdw. $a \in$ Set (T_2, f)
$\updownarrow$
für alle β : wert $(H_{T_1}, \beta) = W$ gdw. wert $(H_{T_2}, \beta) = W$

Satz 2.7.14 (Dualitätstheorem der Aussagenlogik)
Es seien H_1, H_2 Ausdrücke, in denen die Zeichen $\rightarrow, \leftrightarrow$ nicht vorkommen, ferner sei H_i' der aus H_i durch simultanes Ersetzen von $\wedge$ durch $\vee$ und von $\vee$ durch $\wedge$ entstehende Ausdruck. Dann gilt:

$$\text{Wenn ag}\,(H_1 \leftrightarrow H_2)\,,\text{ so ag}\,(H_1' \leftrightarrow H_2')\,.$$

Offenbar gilt dann:

$$
\begin{array}{rll}
G \equiv T_1 = T_2 \text{ gültig} & \rightarrow \text{ag}\,(H_{T_1} \leftrightarrow H_{T_2}) & \\
& & \leftarrow \text{Dualität} \\
& \rightarrow \text{ag}\left(H'_{T_1} \leftrightarrow H'_{T_2}\right) & \\
& \rightarrow T_1' = T_2' \text{gültig.} &
\end{array}
$$

Beweis: Wir zeigen: Wenn $H_1 \rightarrow H_2 \in$ ag, so $H_2' \rightarrow H_1' \in$ ag. Es seien o. B. d. A. $p_1, \ldots, p_n$ alle AV in $H_1 \rightarrow H_2$. Dann ist

$$(H_1 \rightarrow H_2)\left[p_1/\neg p_1, \ldots, p_n/\neg p_n\right] = (H_1^\star \rightarrow H_2^\star) \in \text{ag}$$

wobei $H_i^\star = H_i\left[p_1/\neg p_1, \ldots, p_n/\neg p_n\right]$.

Nun ist $\neg(H_0 \wedge H_{00}) \sim_{\text{sem}} \neg H_0 \vee \neg H_{00}$ und $\neg(H_0 \vee H_{00}) \sim_{\text{sem}} \neg H_0 \wedge \neg H_{00}$.

Mittels dieser Äquivalenz treiben wir die Negationszeichen nach außen. ($\leftarrow$ anwenden von rechts nach links) Dabei geht $H_1^\star$ in $\neg H_1'$, $H_2^\star$ in $\neg H_2'$ über, wir erhalten also

$$(H_1' \rightarrow \neg H_2') \in \text{ag}$$

also $(H_2' \rightarrow H_1') \in$ ag (Kontraposition).

Beispiel:

$$
\begin{array}{cl}
M = M \cup (M \cap N) & \text{Absorptionsgesetz} \\
\text{übersetzen} \rightarrow & \\
p \leftrightarrow p \wedge (p \vee q) & \\
p \leftrightarrow p \vee (p \wedge q) & \\
\rightarrow & \\
M = M \cap (M \cup N). &
\end{array}
$$

Kapitel 3

Prädikatenlogik

3.1 Einleitung

Unzulänglichkeiten des Aussagenkalküls:

Was wird im Aussagenkalkül widergespiegelt

Aussagen	$\rightarrow$	Wahrheitwerte	$\rightarrow$	Aussagenvariable
extens. Aussagenfunktionen	$\rightarrow$	Wahrheitsfunktionen	$\rightarrow$	Ausdrücke

Nur die aussagenlogische Struktur von Aussagen wird widergespiegelt; nicht aber:

1. Aussagen betreffen Gegenstände, sie entstehen aus „Aussageformen"
   - „x ist gerade"
   - „k ist Primzahl" (Aussageformen)
   - „x ist größer als z"
2. Aussagen betreffen Eigenschaften von und Beziehungen zwischen Gegenständen
   - „Die Menge $\mathbb{N}$ ist unendlich"
   - „Die Relation $<$ ist transitiv"
3. Aussagen können die Form von All- oder Existenzaussagen haben
   - „Jede natürliche Zahl ist Summe von vier Quadraten"
   - „Es gibt eine gerade Primzahl"

Logische Schlüsse, bei denen solche Strukturen eine Rolle spielen, können nicht im Aussagenkalkül überprüft werden, weil sie nicht widergespiegelt werden.

z. B.: (modus barbara, klassischer Syllogismus)

Alle Studenten sind	Menschen	$\forall x\,(Sx \rightarrow Mx)$
Alle Menschen sind	fleißig	$\forall x\,(Mx \rightarrow Fx)$
Alle Studenten sind	fleißig	$\forall x\,(Sx \rightarrow Fx)$

- Was brauchen wir für unser Modell?
- Wie weit soll es gehen?
- Wollen wir auch z. B. Existenz- oder Allaussagen für Eigenschaften, Relationen usw. formulieren?

Stufen: Prädikatenkalkül der

- *1. Stufe* (elementar) Nur Variablen für Gegenstände werden quantifiziert.
  - „Es gibt einen Gegenstand x mit ...“
  - „Für alle Individuen x gilt ...“
- *2. Stufe* Eigenschaften von Gegenständen (d. h. Mengen, bzw. 1-stellige Attribute) und Beziehungen zwischen Gegenständen (d. h. Relationen, bzw. n-stellige Attribute werden zusätzlich quantifiziert.
  - „Für jede Menge M gilt: Wenn jede symmetrische und über M reflexive Relation Äquivalenzrelation ist, so hat M höchstens zwei Elemente.“

$\vdots$

- volle Stufigkeit: alles erlaubt

weitere Unterteilung der höheren Stufen:

1. „schwache“ Logik: Nur endliche Mengen werden quantifiziert.
2. nach Stellenzahl der Attributvariablen: z. B. 1-stellige (nur Variablen für Mengen)

also was wollen wir in unserem Modell widerspiegeln?

a)	Gegenstände	$\rightarrow$	Individuenzeichen
b)	Beziehungen, Eigenschaften von Individuen (Attribute)		Attributenzeichen
c)	funktionale Abhängigkeiten zwischen Gegenständen (Funktionen)		Funktionszeichen
Was soll quantifiziert werden?			
d)	Individuen		Individuenvariable

sonst nichts $\rightarrow$ elementare Sprache (Sprache 1. Stufe)

was soll an Struktur widergespiegelt werden:

aussagenlogische Struktur	aussagenlogische Verknüpfungen $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
Quantifikationen	prädikatenlogische Verknüpfungen
Gleichheit, Identität	Gleichheitsattribut

Definition 3.1.1

1. I heißt Individuenbereich := I ist *nichtleere* Menge (Menge von Gegenständen, über die wir Aussagen machen wollen) ($\neq \emptyset$ weil sonst viele Schlüsse nicht funktionieren z. B. $\dfrac{\text{für alle } x \text{ gilt } H(x)}{\text{es gibt ein } x \text{ mit } H(x)}$)
2. $i \geq 1$
   α^i ist ein i-stelliges Attribut über I:

$$\alpha^i : \bigtimes_i I \rightarrow \{W, F\}$$

Die Menge $R_{\alpha^i} = \left\{[x_1, x_2, \ldots, x_i] \,|\, \alpha^i (x_1, \ldots, x_i) = W\right\}$ heißt die Relation von α^i ($i = 1$: Menge von α^i)

Das Gleichheitsattribut Id_I über I ist definiert durch

$$\mathrm{Id}_I (x, y) = \begin{cases} W, & \text{falls } x \text{ gleich } y \text{ ist} \\ F, & \text{sonst} \end{cases}$$

3. ϕ^i ist eine i-stellige Funktion über I:

$$\phi^i : \bigtimes_i I \to I$$

Definition 3.1.2

$$\begin{aligned}
\mathrm{Om}\left(\alpha^1\right) &= \begin{cases} W, & \text{falls für alle } x \in I \text{ gilt: } \alpha^1(x) = W \\ F, & \text{sonst} \end{cases} \\
\mathrm{Ex}\left(\alpha^1\right) &= \begin{cases} W, & \text{falls für wenigstens ein } x \in I \text{ gilt: } \alpha^1(x) = W \\ F, & \text{sonst} \end{cases} \\
\mathrm{gl}\left(\alpha^1, \beta^1\right) &= \begin{cases} W, & \text{falls card}\left(\left\{x|x \in I \wedge \alpha^1(x) = W\right\}\right) = \\ & \qquad \text{card}\left(\left\{x|x \in I \wedge \beta^1(x) = W\right\}\right) \\ F, & \text{sonst} \end{cases} \\
\mathrm{gl}^n!!\left(\alpha^1\right) &= \begin{cases} W, & \text{falls es genau } n \text{ Elemente } x \text{ aus } I \text{ mit} \\ & \quad \alpha^1(x) = W \text{ gibt} \\ F, & \text{sonst} \end{cases}
\end{aligned}$$

In unserem Kalkül werden nur $\mathrm{Om}\left(\alpha^1\right)$ und $\mathrm{Ex}\left(\alpha^1\right)$ verwendet. gl läßt sich nicht durch Om und Ex ausdrücken.

3.1.1 Syntax der elementaren Sprache mit Signatur $[X, P, F, K]$

Basis:

$$\begin{array}{rcll}
X & = & \{x_i | i \in \mathbb{N}\} & \text{– Individuenvariablen} \\
 & & \{x, x\star, x\star\star, \ldots\} & \\
P & = & \left\{A_i^{(j)} | 0 \neq i, j \in \mathbb{N}\right\} & \text{– Attributenzeichen} \\
 & & A\underbrace{\star\star\cdots}_{i}\underbrace{|\cdots|}_{j} & \\
F & = & \left\{F_i^{(j)} | 0 \neq i, j \in \mathbb{N}\right\} & \text{– Funktionszeichen} \\
K & = & \{a_i | i \in \mathbb{N}\} & \text{– Konstanten, Individuenzeichen}
\end{array}$$

$[X, P, F, K]$ – Signatur der Sprache des Prädikatenkalkül 1. Ordnung

Definition 3.1.3 (Term)

A) Jede Individuenkonstante und jede Individuenvariable ist ein Term.

I) Ist F_i^j ein j-stelliges Funktionszeichen und sind $T_1, \ldots, T_j$ Terme, so ist $F_i^j (T_1, \ldots, T_j)$ ein Term

Beispiel: $F_1^2 \left(F_5^1 (x_j), a_3\right)$.

Definition 3.1.4 (Ausdruck)

A) (Prädikative Ausdrücke)

1. Sind T_1, T_2 Terme, so ist $T_1 = T_2$ ein Ausdruck (Gleichung)
2. Ist A_i^j ein j-stelliges Attributenzeichen und sind $T_1, \ldots, T_j$ Terme, so ist $A_i^j T_1 \cdots T_j$ ein Ausdruck.

I) 1. (Aussagenlogische Zusammensetzung)
Sind H_1, H_2 Ausdrücke, so auch $\neg H_1$, $(H_1 \wedge H_2)$, $(H_1 \vee H_2)$, $(H_1 \rightarrow H_2)$, $(H_1 \leftrightarrow H_2)$.

2. (prädikatenlogische Zusammensetzung)
Ist H ein Ausdruck, x_j eine Variable und in H kommt x_j vor, aber keines der Wörter $\forall x_j, \exists x_j$, so sind $\forall x_j H, \exists x_j H$ Ausdrücke.

E) Sonst nichts

$$\begin{aligned} \text{ausd} &= \text{Menge aller Ausdrücke} \\ &= \text{elementare Sprache der gegebenen Signatur} \\ &= \text{Sprache des PK 1. Stufe mit Identität (Gleichheitszeichen)} \end{aligned}$$

3.1.2 Einige syntaktische Eigenschaften

Definition 3.1.5
Es sei H ein Ausdruck, x_j eine Variable.

1. x_j kommt in H vollfrei vor
   (a) x_j kommt in H vor.
   (b) Die Zeichenreihen $\forall x_j, \exists x_j$ kommen nicht vor.
2. x_j kommt in H an der n-ten Stelle quantifiziert vor, wenn
   (a) x_j steht in H an der n-ten Stelle, und $n \geq 2$.
   (b) An der $(n-1)$-ten Stelle in H kommt $\exists$ oder $\forall$ vor.

Satz 3.1.6
H ist ein Ausdruck, in dem x_j an der n-ten Stelle quantifiziert vorkommt. Dann gibt es einen Ausdruck H_1 mit

1. in H_1 kommt x_j vollfrei vor.
2. Wörtern Z_1, Z_2 mit $H = Z_1 Q x_j H_1 Z_2$, wobei $Q \in \{\forall, \exists\}$.

Beweis: Induktion über H.

A) Wenn H prädikativ, d. h. $T_1 = T_2$ oder $A_j T_1 \ldots T_j$, so klar (hier kommt x_j nicht quantifiziert vor).

Im Induktionsschritt betrachten wir zuerst den Fall, daß H durch aussagenlogische Zusammensetzung entsteht. Wenn $H \equiv \neg H_0$, so ist x_j in H_0 an der $(n-1)$-ten Stelle quantifiziert; nach Induktionsvoraussetzung hat H_0 die Form

$$H_0 \equiv Z_1 Q x_j H_1 Z_2$$

also

$$H \equiv \neg Z_1 Q x_j H_1 Z_2.$$

Wenn $H \equiv (H_0 \otimes H_{00})$ ist, wobei $\otimes$ eines der Zeichen $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ ist, so befindet sich die n-te Stelle (an der x_j quantifiziert steht) entweder im Ausdruck H_0 oder in H_{00}, dieser kann nach Induktionsvoraussetzung als $Z_1 Q x_j H_1 Z_2$ geschrieben werden, womit sich eine entsprechende Zerlegung für H ergibt, etwa bei $H_0 \equiv Z_1 Q x_j H_1 Z_2$

$$H = \underbrace{(Z_1}_{Z'_1} Q x_j H_1 \underbrace{Z_2 \otimes H_2)}_{Z'_2}$$

Bleibt der Fall $H \equiv Q' x_i H_{00}$ (prädikatenlogische Zusammensetzung)

Fall 1) $x_i = x_j$, $H \equiv Q x_j H_{00}$
Dann ist $n = 2$ und $Q' = Q$, $H_1 = H_{00}$, $Z_1 = Z_2 =$ leeres Wort.

Fall 2) $\alpha_i \neq x_j$
Dann kommt x_j in H_{00} an der $(n-2)$-ten Stelle quantifiziert vor. Nach Induktionsvoraussetzung ist $H_{00} \equiv Z_1 Q x_j H_1 Z_2$, also $H \equiv Q' x_i Z_1 Q x_j H_1 Z_2$.

□

Definition 3.1.7

1. Der im Satz 3.1.6 mit H_1 bezeichnete Ausdruck heißt Wirkungsbereich des Quantors, der in H an der $(n-1)$-ten Stelle steht.
2. x_j kommt in H an der n-ten Stelle gebunden vor, wenn
   (a) $l(H) \geq n \geq 2$
   (b) x_j steht in H an der n-ten Stelle.
   (c) x_j kommt an der n-ten Stelle quantifiziert vor oder steht im Wirkungsbereich eines mit x_j versehenen Quantors.
3. x_j kommt in H an der n-ten Stelle frei vor, wenn
   (a) x_j steht in H an der n-ten Stelle,
   (b) x_j ist an der n-ten Stelle nicht gebunden.
4. H heißt Aussage (abgeschlossen), wenn H keine freien Variablen enthält.

3.2 Semantik elementarer Sprachen

3.2.1 Interpretation, Belegung, Wert

Es sei I ein Individuenbereich.

g ist eine Interpretation von AUSD über I, wenn g eine Abbildung ist, die

1. jedem Individuenzeichen a_i ein Element $g(a_i) \in I$
2. jedem Funktionszeichen F_i^k eine k-stellige Funktion $g\left(F_i^k\right) : \bigtimes_k I \rightarrow I$ und
3. jedem Attributzeichen A_i^k ein k-stelliges Attribut $g\left(A_i^k\right) : \bigtimes_i I \rightarrow \{W, F\}$

zuordnet.

Zu jedem I, g gehört die interpretierende Algebra $\left[I, \left\{g\left(F_i^k\right) | i \in \mathbb{N}\right\}, R_{g(A^k)}, \ldots\right]$

Definition 3.2.1

1. f heißt Belegung über I, wenn f jeder Inividuenvariablen x_i ein Individuum $f(x_i) \in I$ zuordnet.

2. $\text{element}_{I,g}(T, f)$ wird wie folgt induktiv definiert:

A) Für Variable x_i: $\quad \text{element}_{I,g}(x_i, f) = f(x_i)$
Für Konstanten a_i: $\quad \text{element}_{I,g}(a_i, f) = g(a_i)$

I) $\text{element}_{I,g}\left(F_i^j(T_1, \ldots, T_j), f\right) =$
$$g\left(F_i^j\right)(\text{element}_{I,g}(T_1, f), \ldots, \text{element}_{I,g}(T_f, f)).$$

3. $\text{wert}_{I,f}(H, f)$ wird induktiv wie folgt definiert:

A) $\text{wert}_{I,g}(T_1 = T_2, f) = \text{Id}_I(\text{element}_{I,g}(T_1, f), \text{element}_{I,g}(T_2, f))$
$\text{wert}_{I,g}(A_i^k T_1 \ldots T_k, f) = g(A_i^k)(\text{element}_{I,g}(T_1, f), \ldots, \text{element}_{I,g}(T_k, f))$

I) $\text{wert}_{I,g}(\neg H, f) = \text{non wert}_{I,g}(H, f)$
$\text{wert}_{I,g}((H_1 \wedge H_2), f) = \text{et}(\text{wert}_{I,g}(H_1, f), \text{wert}_{I,g}(H_2, f))$
$\text{wert}_{I,g}((H_1 \vee H_2), f) = \text{vel}(\text{wert}_{I,g}(H_1, f), \text{wert}_{I,g}(H_2, f))$
$\text{wert}_{I,g}((H_1 \rightarrow H_2), f) = \text{seq}(\text{wert}_{I,g}(H_1, f), \text{wert}_{I,g}(H_2, f))$
$\text{wert}_{I,g}((H_1 \leftrightarrow H_2), f) = \text{aeq}(\text{wert}_{I,g}(H_1, f), \text{wert}_{I,g}(H_2, f))$
$\text{wert}_{I,g}(\forall x_j H, f) = \text{Om}\left(\alpha^1_{H,I,g,f,x_j}\right)$
$\text{wert}_{I,g}(\exists x_j H, f) = \text{Ex}\left(\alpha^1_{H,I,g,f,x_j}\right)$
wobei: $\alpha^1_{H,I,g,f,x_j}(y) = \text{wert}_{I,g}\left(H, [f]_y^j\right) \quad [f]_y^j(x_i) = \begin{cases} y, & \text{falls } i = j \\ f(x_i), & \text{sonst} \end{cases}$

Beispiel $H \equiv \exists x_0 A_0^2 x_0 x_1$, $I = \mathbb{N}$, $g(A_0^2) =$ „ $<$ “, $f(x_1) = 5$.
Dann ist
$$\text{wert}_{I,g}\left(\exists x_0 A_0^2 x_0 x_1, f\right) = \text{Ex}\left(\alpha^1_{A_0^2 x_0 x_2, \mathbb{N}, g, f, x_0}\right)$$
wobei für $k \in \mathbb{N}$
$$\begin{aligned} \alpha^1_{A_0^2 x_0 x_1, \mathbb{N}, g, f, x_0}(k) &= \text{wert}\left(A_2^0 x_0 x_1, [f]_k^0\right) \\ &= g\left(A_2^0\right)\left([f]_k^0(x_0), [f]_k^0(x_1)\right) \\ &= \text{„} < \text{“}(k, 5) = \begin{cases} W, & \text{falls } k < 5 \\ F, & \text{sonst} \end{cases} \end{aligned}$$
Es gibt also ein $k \in I = \mathbb{N}$ mit
$$\alpha^1_{A_0^2 x_0 x_1, \mathbb{N}, g, f, x_0}(k) = W$$
d. h.
$$\text{wert}_{I,g}\left(\exists x_0 A_0^2 x_0 x_1, f\right) = \text{Ex}\left(\alpha^1_{A_0^2 x_0 x_1, \mathbb{N}, g, f, x_0}\right) = W.$$
Bei einer Belegung f mit $f(x_1) = 0$ ist jedoch
$$\text{wert}_{I,g}\left(\exists x_0 A_0^2 x_0 x_1, f\right) = F.$$

3.2.2 Erfüllbarkeit, Gültigkeit

Definition 3.2.2
Sei $H \in$ AUSD

1. f erfüllt H in der Interpretation g über I; $(f\mathrm{erf}_{I,g}H)$, wenn $\mathrm{wert}_{I,g}(H,f) = W$.
2. H ist erfüllbar in g über I, wenn es eine Belegung $f : X \to I$ gibt, mit $\mathrm{wert}_{I,g}(H,f) = W$.
3. H heißt erfüllbar über I ($H \in \mathrm{ef}_I$, $\mathrm{ef}_I H$), wenn es g, f gibt, mit: $\mathrm{wert}_{I,g}(H,f) = W$.
4. H heißt erfüllbar($H \in \mathrm{ef}$, $\mathrm{ef}H$), wenn es I, g, f gibt, mit $\mathrm{wert}_{I,g}(H,f) = W$.

Beipiel: $H = \exists x_0 \exists x_1 \neg x_0 = x_1$
Wenn I Einermenge, so ist H nicht erfüllbar über I.

$H = \forall x_0 \forall x_1\ x_0 = x_1$
H ist erfüllbar über I gdw. I Einermenge.

Definition 3.2.3
Sei $H \in$ AUSD

1. H ist allgemeingültig in der Interpretation g über I $\left(H \in \mathrm{ag}_{I,g}\right)$, wenn für alle Belegungen f : $\mathrm{wert}_{I,g}(H,f) = W$.
2. H ist allgemeingültig über I ($H \in \mathrm{ag}_I$, $\mathrm{ag}_I H$), wenn für alle g, f gilt: $\mathrm{wert}_{I,g}(H,f) = W$.
3. H ist allgemeingültig ($H \in \mathrm{ag}$, $\mathrm{ag}H$), wenn für alle I, f, g gilt: $\mathrm{wert}_{I,g}(H,f) = W$.

Definition 3.2.4
Sei H Aussage.

1. H heißt wahr in der Interpretation g über I, wenn H erfüllbar in g über I ist.
2. H heißt falsch in g über I, wenn $\neg H$ erfüllbar in g über I ist.

Zentrales Lemma:

Sei $H \in$ AUSD, f Belegung, g Interpretation, I Individuenbereich.

1. Der Wahrheitswert $\mathrm{wert}_{I,g}(H,f)$ hängt nur ab von der Belegung der Variablen und der Interpretation der Zeichen, die in H vorkommen.
2. Kommt die Variable x_j in H nicht frei vor (quantifiziert oder gebunden), so gilt für alle $a \in I : \mathrm{wert}_{I,g}(H,f) = \mathrm{wert}_{I,g}\left(H, [f]_a^j\right)$.
3. Ist H Aussage, so gilt: H erfüllbar in g über I gdw. H allgemeingültig in g über I.
4. Ist H Aussage und enthält keine Zeichen, so ist H allgemeingültig über I gdw. H erfüllbar über I.

Aus den Definitionen 3.2.2-3.2.4 folgt

Satz 3.2.5

1. $H \in \mathrm{ef}_I$ gdw. $\neg H \notin \mathrm{ag}_I$
2. $H \in \mathrm{ef}$ gdw. $\neg H \notin \mathrm{ag}$
3. $\mathrm{ag}_I \subset \mathrm{ef}_I$, $\mathrm{ag} \subset \mathrm{ef}$

Für (3.2.5.3) ist die Festsetzung wichtig, daß $I \neq \emptyset$ ist, denn $\neg x_j = x_j$ würde über $I = \emptyset$ gültig sein.

Die Frage nach der Gültigkeit eines Ausdrucks ist durch diesen Satz auf die Frage nach der Erfüllbarkeit seiner Negation reduziert. Um prädikatenlogische Schlußregeln zu verifizieren, brauchen wir also ein Verfahren, um die Erfüllbarkeit von Ausdrücken zu entscheiden.

Gibt es ein solches Verfahren?

Wir werden zeigen:

Wenn I unendliche Menge ist, so ist ef_I nicht entscheidbar.

Dazu unternehmen wir einen Ausflug in die Berechnungstheorie:

3.3 Berechenbarkeit, Entscheidbarkeit

Jeder kennt eine Vielzahl von Algorithmen (Rechenverfahren, Bedienungsanleitungen,
Kochrezepte, ...) und hat daraus einen intuitiven Begriff des Machbaren (mit endlichen Mitteln und in endlicher Zeit) abstrahiert. Dieser Begriff reicht aus, um zu verifizieren, daß ein angegebenes Verfahren ein bestimmtes Problem löst (z. B. das Entscheidungsproblem im Aussagenkalkül). Dieser Begriff bietet aber keinen Ansatzpunkt für einen Beweis dessen, daß ein Problem unlösbar ist. Dazu muß der Algorithmenbegriff präzisiert werden. Jede Präzisierung bringt aber unvermeidlich eine Einschränkung der zugelassenen Vorgehensweisen mit sich, so daß nach einem Unlösbarkeitsbeweis die Frage entsteht, ob es an der Präzisierung oder am Problem liegt, daß keine Lösung existiert.

Dieser Frage ist man dadurch entkommen, daß man den Algorithmenbegriff mehrfach in unterschiedlicher Weise präzisiert und die Gleichwertigkeit der verschiedenen Präzisierungen bewiesen hat. Diese Ansätze können wie folgt sortiert werden:

1. Axiomatischer Ansatz (Church, Kleene)
   Man erklärt gewisse Funktionen per Axiom für berechenbar und definiert Operationen mit Funktionen, die per definitionem die Berechenbarkeit erhalten.
2. Maschinen–Ansatz (Turing)
   Man definiert einen Typ von Rechenmaschinen und erklärt als berechenbar genau das, was diese Maschinen berechnen können.
3. Semiotischer Ansatz (Markow, Post)
   Rechnen bzw. algorithmisches Vorgehen wird als Manipulation von Zeichenreihen (Wörtern) nach gewissen Regeln verstanden.
4. Beweistheoretischer Ansatz (Gödel)
   Das Berechnen eines Funktionswertes $k = f(i)$ wird als Beweisen der Gleichung $f(i) = k$ verstanden.

Wir werden uns im folgenden nur mit dem axiomatischen und dem Maschinen–Ansatz befassen.

Was ist ein Problem?

Als Problem bezeichnen wir eine Familie von Aufgaben, die von einem oder mehreren Parametern abhängen. Dabei unterscheiden wir Berechnungsprobleme

$$\{f(x_1, \ldots, x_n) =? \mid x_1, \ldots, x_n \in \mathbb{N}\}$$

und Entscheidungsprobleme, wie z. B.

$$\{H \in \mathrm{ag} | H \in \mathrm{AUSD}\}$$

In dem einen Fall geht es um die Berechnung eines Wertes (z. B. einer natürlichen Zahl), im anderen um die Bestimmung eines Wahrheitswertes.

Das Berechnungsproblem $\{f(x_1, \ldots, x_n) =? \mid x_1, \ldots, x_n \in \mathbb{N}\}$ der Funktion f heißt *lösbar* bzw. die zahlentheoretische Funktion f heißt *berechenbar*, wenn es einen Algorithmus gibt, der für jedes $x_1, \ldots, x_n \in \mathbb{N}$ folgendes leistet:

Wenn f für $[x_1, \ldots, x_n]$ definiert ist, dann stoppt die Anwendung des Algorithmus auf $[x_1, \ldots, x_n]$ nach endlich vielen Schritten mit dem Wert $f(x_1, \ldots, x_n)$ als Resultat; wenn f für $[x_1, \ldots, x_n]$ nicht definiert ist, dann stoppt die Anwendung des Algorithmus niemals.

Wir verlangen also *nicht*, daß der Algorithmus erkennt. daß f für $[x_1, \ldots, x_n]$ nicht definiert ist und mit einer Fehlermeldung stoppt.

Jedes Entscheidungsproblem, also auch

$$\{H \in \mathrm{ag}? \mid H \in \mathrm{AUSD}\},$$

kann auf ein Berechnungsproblem zurückgeführt werden; dazu geht man zur charakteristischen Funktion der zu entscheidenden Menge über, hier:

$$\chi_{\mathrm{AG}}(H) = \begin{cases} 0, \text{falls } H \in \mathrm{ag} \\ 1, \text{sonst} \end{cases}$$

und hat das Problem

$$\{\chi_{\mathrm{AG}}(H) =? \mid H \in \mathrm{AUSD}\}$$

zu lösen. Durch eineindeutige Numerierung der Menge aller Ausdrücke kommt man dazu, daß man nur die Berechenbarkeit zahlentheoretischer Funktionen untersuchen muß

3.4 Axiomatische Charakterisierung der Berechenbarkeit

Definition 3.4.1
ANF = Menge der folgenden Funktionen

1. $N(x) = x + 1$ (Nachfolgerfunktion)
2. $C_i^n(x_1, \ldots, x_n) = i$ (n-stellige Konstanten)
3. $I_k^n(x_1, \ldots, x_n) = x_k$ (Argumentauswahl)

Satz 3.4.2
Alle Funktionen aus ANF sind intuitiv–anschaulich berechenbar (und total definiert).

Definition 3.4.3 (Substitution)
Die Funktion $\phi^{(n)}$ entsteht durch Substitution aus $\psi^{(m)}$ und $\chi_1^{(n)}, \ldots, \chi_m^{(n)}$ gdw. $\phi(x_1, \ldots, x_n) = \psi\left(\chi_1^{(n)}(x_1, \ldots, x_n), \ldots, \chi_m^{(n)}(x_1, \ldots, x_n)\right)$. ($\chi$ müssen nicht überall definiert sein.)

Satz 3.4.4
Sind ψ und $\chi_1, \ldots, \chi_m$ intuitiv–anschaulich berechenbare Funktionen und entsteht ϕ durch Substitution von ψ und $\chi_1, \ldots, \chi_m$, so ist ϕ intuitiv–anschaulich berechenbar.

$C_i^n(x_1, \ldots x_n) = N(C_0^n(x_1, \ldots, x_n))$

Definition 3.4.5 (Induktive Definition, die primitive Rekursion)
Die Funktion $\phi^{(n+1)}$ entsteht durch primitive Rekursion aus $\psi^{(n)}$ und $\chi^{(n+2)}$, wenn ϕ die Lösung des folgenden Gleichungssystems ist:

$$\begin{aligned} \phi(x_1, \ldots, x_n, 0) &= \psi(x_1, \ldots, x_n) \\ \phi(x_1, \ldots, x_n, i+1) &= \chi(x_1, \ldots, x_n, i, \phi(x_1, \ldots, x_n, i)). \end{aligned} \tag{3.4.1}$$

Satz 3.4.6
Sind ϕ und ψ gegebene Funktionen, so existiert genau ein ϕ mit (3.4.1) aus Definition 3.4.5.

Satz 3.4.7
Sind ψ, χ intuitiv–anschaulich berechenbar und ϕ entsteht durch primitive Rekursion aus ψ und χ, so ist ϕ intuitiv–anschaulich berechenbar.

Definition 3.4.8 (primitiv-rekursive Funktionen)
PRM = die kleinste Klasse von zahlentheoretischen Funktionen, die ANF enthält und abgeschlossen bezüglich Substitution und primitiver Rekursion ist.

Beispiel
Addition: $+(m, n)$
$+(m, 0) = I_1^1(m)$
$+(m, n+1) = N\left(I_3^3(m, n, +(m, n))\right)$

Satz 3.4.9
Die primitiv-rekursiven Funktionen sind total

Offensichtlich sind die primitiv-rekursiven Funktionen nicht alle berechenbaren, denn z. B. die partiellen Funktionen gehören nicht zu PRM

Peterfunktion:

$$\begin{aligned} &P : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ &P(0, n) = n+1 \\ &P(m+1, 0) = P(m, 1) \\ &P(m+1, n+1) = P(m, P(m+1, n))) \end{aligned}$$

z. z.: P berechenbar; betrachten:

```
PROCEDURE Peter(m,n : CARDINAL) : CARDINAL
BEGIN
  IF m = 0 THEN RETURN(n + 1); ELSE
    IF n = 0 THEN RETURN Peter(m − 1, 1);
    ELSE RETURN Peter(m − 1, Peter(m, n − 1));
    END;
  END;
END Peter;
```

Lemma 3.4.10
Zu jeder einstelligen primitiv-rekursiven Funktion ϕ gibt es eine Zahl m derart, daß für alle $n \in \mathbb{N}$ gilt $\phi(n) < P(m, n)$.

Beweis: siehe Peter: „Rekursive Funktionen“.

Konsequenz: P nicht primitiv-rekursiv, denn sonst definieren wir

$$Q(n) := P\left(I_1^1(n), I_1^1(n)\right) = P(n, n)$$

und Q ist primitiv-rekursiv.

Nach Lemma: $\exists m^\star$: $Q(n) < P(m^\star, n)$. Folglich $Q(m^\star) < P(m^\star, m^\star) = Q(m^\star)$.
↯

Folglich ist eine Erweiterung nötig, um alle berechenbaren Funktionen zu bekommen:

Wir erweitern um Suche nach Wert, definieren also Minimum-Operator.

Definition 3.4.11 (Minimum-Operator)
Es sei ψ eine $(n+1)$-stellige zahlentheoretische Funktion. Die (partielle) Funktion ϕ entsteht durch Anwenden des Minimum-Operators auf Ψ, wenn

$$\phi(x_1, \ldots, x_n) = \mu\left(\psi(x_1, \ldots, x_m, j) = 0\right) = \begin{cases} \text{das kleinste } j \in \mathbb{N}\text{, mit } \psi(x_1, \ldots, x_n, j) = \\ 0 \text{ und } \forall i < j \text{ ist } \psi(x_1, \ldots, x_m, i) \text{ definiert,} \\ \text{falls solches existiert.} \\ \text{n.d., sonst} \end{cases}$$

(Das ist Formalisierung des Systematischen Probierens.)

Satz 3.4.12
Ensteht ϕ durch Anwendung des Minimum-Operators auf ψ und ist ψ intuitiv–anschaulich berechenbar, so ist ϕ intuitiv–anschaulich berechenbar.

Beweis:

```
PROCEDURE PHI(x_1, ...x_n : CARDINAL) : CARDINAL;
VAR i, j:CARDINAL; BEGIN
  i := 0
  LOOP
    j := PSI(x_1, ...x_n, i);
    IF j = 0 THEN RETURN i_j;
    ELSE INC(i)
    END
  END
END PHI;
```

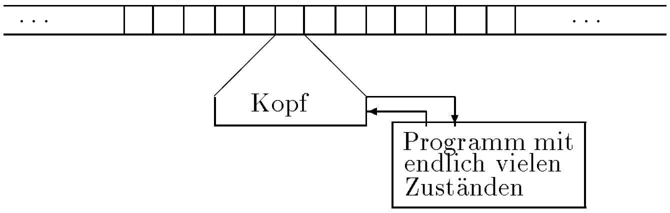


Abbildung 3.1: TURING–Maschine

Definition 3.4.13 (partiell-rekursive Funktionen)
PREK ist die kleinste Klasse von Funktionen, die ANF enthält und abgeschlossen ist bezüglich Substitution, primitiver Rekursion und Anwendung des Minimum-Operators.

Folgerung: PRM $\subseteq$ PREK.

Definition 3.4.14 (allgemein-rekursive (rekursive) Funktionen REK)

$$\mathrm{REK} = \mathrm{PREK} \cap \mathrm{TOTAL}.$$

$$\mathrm{PRM} \underset{\neq}{\subseteq} \mathrm{REK} \underset{\neq}{\subseteq} \mathrm{TOTAL}$$

CHURCHsche These:
Eine zahlentheoretische Funktion ist genau dann intuitiv–anschaulich berechenbar, wenn sie partiell-rekursiv ist.

3.5 Zum Maschinen–Ansatz

A.M Turing 1936

- Band, beidseitig unbegrenzt
- eingeteilt in Felder
- in jedem Feld ein Zeichen aus einem endlichen Alphabet oder Leerzeichen

Definition 3.5.1
$T = [X, Z, z_0, \delta]$ ist TURING–Maschine, wenn:

1. X endliches Alphabet, $\star \notin X$ (Leerzeichen)
2. Z endliche Menge von Zuständen
3. $\delta : Z \times (X \cup \{\star\}) \rightarrow (X \cup \{\star\}) \times B \times Z$, wobei $B = \{R, L, N, S\}$

Arbeitsweise:

1. T arbeitet taktweise, in Takt 1 ist T im Zustand z_0.

2. Ist z_{i-1} der Zustand von T im Takt i und x das Zeichen im betrachteten Feld und $\delta(z_{i-1}, x) = [y, b, z]$, so wird y in das betrachtete Feld geschrieben. Dann wird die Kopfbewegung b ausgeführt (bei $b = S$ wird gestoppt) und in den Zustand $z_i = z$ übergegangen.

Definition 3.5.2 (TURING–berechenbar)
Sei $\phi : \bigtimes_n \mathbb{N} \to \mathbb{N}$ eine zahlentheoretische Funktion.

ϕ heißt TURING–berechenbar, wenn es eine TM $T = [\{|\}, Z, z_0, \delta]$ so gibt, daß für alle $x_1, x_2, \ldots, x_n \in \mathbb{N}$ gilt:

Wenn $[x_1, \ldots, x_n] \in D_\phi$ und T wird in der Situation $\cdots\star\star\underbrace{|\cdots|}_{x_1+1}\star\underbrace{|\cdots|}_{x_2+1}\star\cdots\star\underbrace{|\cdots|}_{x_n+1}\star\underset{\substack{\triangle\\ z}}{\star}$ gestartet, so stoppt T nach endlich vielen Takten in der Situation

$$\cdots\star\star\underbrace{|\cdots|}_{x_1+1}\star\underbrace{|\cdots|}_{x_2+1}\star\cdots\star\underbrace{|\cdots|}_{x_n+1}\star\quad\underbrace{|\cdots|}_{\phi(x_1,\ldots,x_n)+1}\quad\underset{\substack{\triangle\\ z_0}}{\star}$$

Wenn $[x_1, \ldots, x_n] \notin D_\phi$, so kommt T nicht zum Stop.

Wir verlangen noch zusätzlich, daß der Kopf bei der Berechnung nicht über das zweite leere Feld links von den Argumenten hinausläuft.

Ziel: ϕ TURING–berechenbar gdw. ϕ partiell-rekursiv.

Dazu entwickeln wir einen Programm–Kalkül:

Bausteine (für TURING–Programme)

- $X = \{|\}$–fest.
- „Gehe ein Feld nach rechts“

r	$\star$	$\vert$
1	$\star$R2	$\vert$R2
2	$\star$S	$\vert$S

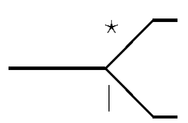
- „Gehe ein Feld nach links“

l	$\star$	$\vert$
1	$\star$L2	$\vert$L2
2	$\star$S	$\vert$S

- „Schreibe | auf das betrachtete Feld“

„|“	$\star$	$\vert$
1	$\vert$N2	$\vert$N2
2	S	$\vert$S

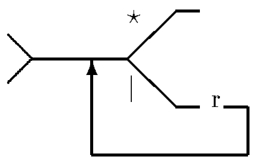
- „bedingter Sprung“



	$\star$	$\vert$
1	$\star$N2	$\vert$N3
2	$\star$S	–
3	–	$\vert$S

- Verkettung: $P_1; P_2$ bzw. $P_1 \rightarrow P_2$
  - P_1 habe Zustände $1, \ldots, l$
  - P_2 habe Zustände $1, \ldots, k$
  - In P_2 alle Adressen um l erhöhen: $l+1, \ldots, l+k$
  - In P_1 alle Stoppanweisungen ersetzen durch $\star$N$(l+1)$ bzw. $|$N$(l+1)$ (Übergang in den Anfangszustand von P_2)

- „Nach rechts auf den ersten $\star$ gehen“: R



„R“	$\star$	$\vert$
1	$\star$N2	$\vert$N3
2	$\star$S	–
3	–	$\vert$S$\leftrightarrow$N4
4	$\star$R5	$\vert$R5
5	$\star$S$\leftrightarrow$N1	$\vert$S$\leftrightarrow$N1

wobei $\leftrightarrow$ für „ersetzen“ steht und „–“ für beliebig.

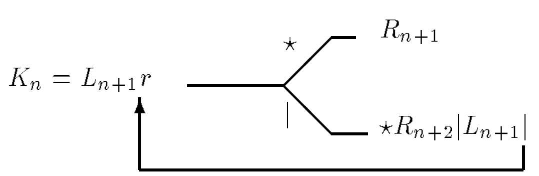
- $n \geq 1$ R_n: „Gehe nach rechts auf den n-ten $\star$, der $\star$ unter dem Kopf mitgezählt.“
  - $R_1 := R$
  - $R_n := (Rr)^{n-1}$R

- L_n: „Gehe nach links ...“
  - $L_1 = L$
  - $L_n = (Ll)^{n-1}\, L.$

- K_n: „Kopiere die n-te Strichfolge links vom Kopf“
  d. h. $\star\underbrace{|\cdots|}_{k_n}\star\cdots\star\underbrace{|\cdots|}_{k_n}\star\cdots\star \rightarrow$

  $\star\underbrace{|\cdots|}_{k_n}\star\cdots\star\underbrace{|\cdots|}_{k_n}\star\underbrace{|\cdots|}_{k_1}\underset{\triangle}{\star}\ \star\cdots\star$

  $k_1 = 0$ erlaubt



Satz 3.5.3
Alle Anfangsfunktionen sind TURING–berechenbar

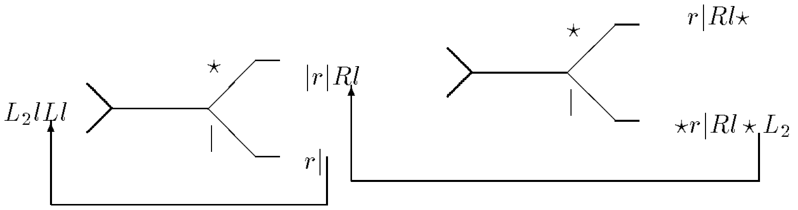
Beweis: ANF:

1. $N(x) = x + 1$:
   $\star\star\underbrace{|\cdots|}_{x+1}\star_{\triangle}\ \cdots\star\star\underbrace{|\cdots|}_{x+1}\star\star\underbrace{|\cdots|}_{x+2}\star_{\triangle}$ Das Programm $K_1 r$ berechnet n.

2. $C_i^n(x_1, \ldots, , x_n) = i$
   Das Programm $(r|)^{i+1}\, r$ berechnet C_i^n.

3. $I_k^n(x_1, \ldots, x_n) = x_k$.
   K_{n-k+1} leistet das Verlangte.

Löschprogramm Lö



Satz 3.5.4
Wenn ϕ durch Substitution aus ψ und $\chi_1, \ldots, \chi_m$ entsteht und $\psi, \chi_1, \ldots, \chi_m$ sind TURING–berechenbar, so ist ϕ TURING–berechenbar.

Beweis: $\phi(x_1, \ldots, x_n) = \psi(\chi_1(x_1, \ldots, x_n), \ldots, \chi_m(x_1, \ldots, x_n))$

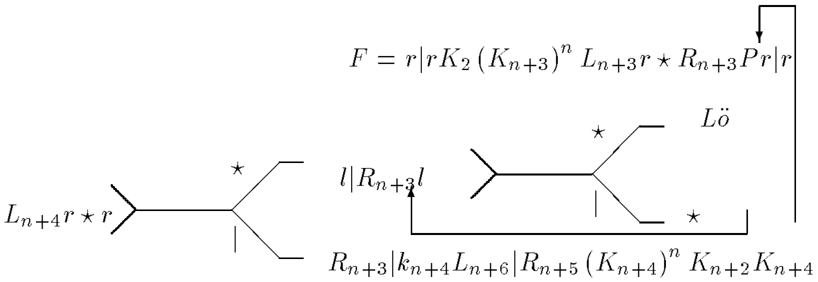
Sei H_i berechne χ_i; P berechne ψ. Dann wird ϕ berechnet durch

$$\begin{aligned} F \;=\; & r|r\,(K_{n+1})^n\, L_{n+1} l \star R_{n+2} H_1\,(K_{n+1})^n\, H_2 \cdots (K_{n+1})^n\, H_m \\ & K_{(m-1)n+m} K_{(m-2)n+m} \cdots K_m P\, Lö \end{aligned}$$

Satz 3.5.5
Entsteht ϕ durch primitive Rekursion aus ψ und χ und sind ψ, χ TURING–berechenbar, so ist ϕ TURING–berechenbar.

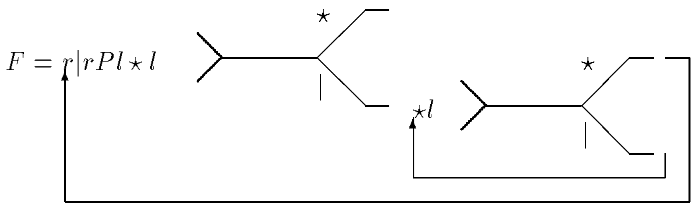
Beweis: Sei P berechne ψ, H berechne χ.

F berechnet ϕ



Satz 3.5.6
Entsteht ϕ durch Anwendung des ν-Operators auf ψ und ψ ist TURING–berechenbar, so ist ψ TURING–berechenbar.

Beweis: F berechne ϕ; P berechne ψ



Folgerung: Alle partiell–rekursiven Funktionen sind TURING–berechenbar.

Um die Umkehrung zu beweisen, verwenden wir ein Verfahren, das nach Kurt GÖDEL auch Gödelisierung genannt wird: Mit Hilfe eineindeutiger und intuitiv–anschaulich berechenbarer Abbildungen wird der Formalismus der TURING–Maschinen in die Arithmetik der natürlichen Zahlen abgebildet. Dadurch gehen Beziehungen zwischen TURING–Maschinen und ihren Konfigurationen in Beziehungen zwischen Zahlen über, die unter Umständen durch partiell–rekursive Funktionen beschrieben werden. Daß die von einer gegebenen TURING–Maschine berechnete zahlentheoretische Funktion partiell–rekursiv ist, bedeutet ja nichts anderes, als daß die Gödelzahl der Stopp–Konfiguration partiell–rekursiv von der Gödelzahl der Start–Konfiguration abhängt.

Zur Vorbereitung geben wir wichtige Beispiele für primitiv–rekursive Funktionen an.

Hilfssatz: Die folgenden zahlentheoretischen Funktionen sind primitiv–rekursiv.

1. Addition $m + n$
2. Multiplikation $m \cdot n$
3. Vorgänger $V(m) := \begin{cases} n-1, & n > 0 \\ 0, & \text{sonst} \end{cases}$
4. Arithmetische Differenz
$$m \mathbin{\dot{-}} n = \begin{cases} m-n, & m \geq n \\ 0, & \text{sonst} \end{cases} \left| \begin{array}{l} m \mathbin{\dot{-}} 0 := m \\ m \mathbin{\dot{-}} (n+1) = V\left(m \mathbin{\dot{-}} n\right) \end{array} \right.$$
5. Betrag einer Differenz
$$|m - n| = \left(m \mathbin{\dot{-}} n\right) + \left(n \mathbin{\dot{-}} m\right)$$
6. sg
$$\begin{aligned} \mathrm{sg}(0) &= 0 \\ \mathrm{sg}(m+1) &= 1 \end{aligned}$$
7. $\overline{\mathrm{sg}}$
$$\overline{\mathrm{sg}}(n) = 1 \mathbin{\dot{-}} \mathrm{sg}(n)$$
8. Allgemeine Summe: Sei g $(n+1)$-stellige primitiv–rekursive Funktion. Dann ist $f(m_1, \ldots, m_n, k) := \sum\limits_{i=0}^{k} g(m_1, \ldots, m_n, i)$ primitiv–rekursiv.

   Bemerkung:
$$\begin{aligned} f(m_1, \ldots, m_n, 0) &= g(m_1, \ldots, m_n) \\ f(m_1, \ldots, m_n, k+1) &= f(m_1, \ldots, k) + g(m_1, \ldots m_n, k+1) \end{aligned}$$

9. allgemeines Produkt g: wie oben

$$f(m_1,\ldots,m_n,k)=\prod_{i=0}^{k} g(m_1,\ldots,m_n,i)$$

ist primitiv-rekursiv.

10. Division mit Rest

$$\begin{aligned}\left[\frac{x}{y}\right] &:= \begin{cases}0, & g=0\\ x\mathrm{DIV}y, & \text{sonst}\end{cases}\\ \left[\frac{x}{y}\right] &= \sum_{j=0}^{x}\mathrm{sg}\left(\prod_{i=0}^{j}\left[(x+1)\dot{-}(i+1)\cdot y\right]\right)\\ \mathrm{rest}(x,y) &= x\dot{-}\left[\frac{x}{y}\right]\cdot y \text{ – primitiv–rekursiv}\end{aligned}$$

11. Beschränkter Minimum Operator g sei primitiv–rekursiv.

$$f(m_1,\ldots,m_n,k):=\mu\left(i\le k\wedge g(m_1,\ldots,m_n,i)=0\right)=\begin{cases}\text{kleinste } i, \text{ mit } i\le k \text{ und } g(m_1,\ldots,m_n,i)= \\ 0, \text{ falls es existiert}\\ 0, \text{ sonst}\end{cases}$$

Beh.: f ist primitiv-rekursiv

Bew.:

$$f(m_1,\ldots,m_n,k)=$$
$$\left[\sum_{i=0}^{k}\mathrm{sg}\left(\prod_{j=0}^{i}g(m_1,\ldots,m_n,j)\right)\right]\cdot\overline{\mathrm{sg}}\left(\left[\sum_{i=0}^{k}\mathrm{sg}\left(\prod_{j=0}^{i}g(m_1,\ldots,m_n,j)\right)\right]\dot{-}k\right).$$

12. $q(n)=q_n$ – die n-te Primzahl ist primitiv–rekursiv.

$$\begin{aligned}q(0) &= 2\\ q(n+1) &= \mu\left(j\le(g(n)!+1)\wedge\left(q(n)+1\dot{-}j\right)+\sum_{k=2}^{j-1}\overline{\mathrm{sg}}(\mathrm{rest}(j,k))=0\right).\end{aligned}$$

13. Der Exponent der n-ten Primzahl in der Primzahldarstellung von x.

$$\exp(x,n)=\sum_{j=1}^{x}\overline{\mathrm{sg}}\underbrace{\left(\mathrm{rest}\left(x,q_n^j\right)\right)}_{0\leftrightarrow q_n^i/x}.$$

Bevor wir den TURING–Maschinen $T=[X,Z,z_0,\delta]$ ihre Gödelzahl zuordnen, machen wir einige Einschränkungen, die ihre Berechnungsfähigkeit nicht beeinträchtigen. Wir setzen voraus, daß $X=\{|\}$ ist und setzen

$$x_0:=\star \quad , \quad x_1:=|.$$

Die Zustandsmenge sei numeriert als

$$Z=\{z_1,\ldots,z_m\}$$

wobei $z_0=z_1$ der Anfangszustand ist. Die Menge $B=\{N,R,L,S\}$ sei als

$$b_0=N \quad , \quad b_1=R \quad , \quad b_2=L \quad \text{und} \quad b_3=S$$

numeriert und wir setzen voraus, daß die Maschine beim Stopp nichts mehr ändert: Wenn $\delta(z,x)=[x',S,z']$, dann $z=z'$ und $x=x'$.

Die Gödelzahl $\text{gö}\,(T)$ der Turing–Maschine T

Die Turing–Maschine T ist durch die Tabelle der Funktion δ vollständig beschrieben.

1. Tabelleneintrag:
$$\text{gö}\,([x_i, b_j, z_k]) := 2^i 3^j 4^k.$$
2. Zeile in der Tabelle von δ: $\delta\,(z_\mu, \cdot)$
$$\text{gö}\,(\delta, z_\mu) = 2^{\text{gö}(\delta(z_\mu, x_0))} \cdot 3^{\text{gö}(\delta(z_\mu, x_1))}.$$
3. $\text{gö}\,(T) = \prod\limits_{\mu=1}^{m} q_{\mu-1}^{\text{gö}(\delta, z_\mu)}$.

Es sei TM die Menge aller TM der angegebenen Art.

Lemma 3.5.7
Die Abbildung $\text{gö} : \mathcal{TM} \to \mathbb{N}$ ist eineindeutig. Die charakteristische Funktion

$$\chi_{\mathcal{TM}}\,(i) = \left\{ \begin{array}{ll} 0, & \text{falls eine TM } T \in \mathcal{TM} \\ & \text{mit gö}\,(T) = i \text{ existiert} \\ 1, & \text{sonst} \end{array} \right\} \text{ist primitiv–rekursiv}$$

(d. h. die Menge der Gödelzahlen ist entscheidbar).

Die Gödelzahl $\text{gö}(\sigma)$ einer endlichen Bandbeschriftung σ

Wir numerieren die Felder unseres („halben") Bandes von links nach rechtes mit $0, 1, 2, \ldots$ Eine Bandbeschriftung σ ist dann eine Abbildung, die jeder Feldnummer die Nummer des in diesem Feld stehenden Buchstabens zuordnet, d. h.

$$\sigma : \mathbb{N} \to \{0, 1\}$$

σ ist endlich, wenn auf fast allen Feldern das Zeichen $\star$ steht, also wenn

$$j_\sigma := \text{SUP}\{i | \sigma(i) = 1\}$$

existiert (das Supremum der leeren Menge ist 0). Wir setzen

$$\text{gö}(\sigma) = \prod_{j=0}^{j_\sigma} q_j^{\sigma(j)}$$

Lemma 3.5.8
Σ sei die Menge aller endlichen Bandbeschriftungen

1. Die Abbildung $\text{gö} : \Sigma \to \mathbb{N}$ ist eineindeutig.
2. Die charakteristische Funktion χ_Σ mit $\chi_\Sigma\,(i) = \left\{ \begin{array}{ll} 0, & \text{falls ein } \sigma \in \Sigma \text{ mit gö}\,(\sigma) = i \\ & \text{existiert} \\ 1, & \text{sonst} \end{array} \right.$
   ist primitiv–rekursiv.
   $\chi_\Sigma\,(i) = 0$ gdw. $i > o$ und für alle $j\,(0 \leq j \leq i)$ gilt $\exp\,(i, j) \leq 1$.
   $\chi_B\,(i) = \text{sg}\left(\overline{\text{sg}}\,(i) + \sum_{j=0}^{i} \left(\exp\,(i, j) \dot{-} 1\right)\right)$.

Die Gödelzahl einer Konfiguration einer TM T

Eine Konfiguration k der TM T ist ein Tripel $[j, \sigma, z_i]$, wobei j die Nummer des Feldes, auf dem der Kopf steht, σ die Beschriftung des Bandes und z_i der aktuelle Zustand ist. $K = [j, \sigma, z_i]$,

$$\text{gö}\,(K) = 2^j \cdot 3^{\text{gö}(\sigma)} \cdot 5^i$$

Lemma 3.5.9

1. Die Abbildung $\text{gö} : \mathfrak{K} \to \mathbb{N}$ ist eineindeutig.
2. Die charakteristische Funktion $\chi_K\,(k) := \begin{cases} 0, & \text{falls es ein } K \in \mathfrak{K} \text{ gibt mit } k = \text{gö}\,(K) \\ 1, & \text{sonst} \end{cases}$
ist primitiv-rekursiv.

   $\chi_K\,(k) = 0$ gdw. $k > 0$ und $k = 2^{\exp(k,0)}.3^{\exp(k,1)}.5^{\exp(k,2)}$ und $\chi_\Sigma\,(\exp\,(k,1)) = 0$ und $1 \leq \exp\,(k,2)$.

   $$\chi_K\,(k) = \text{sg}\left(\overline{\text{sg}}\,(k) + |k - 2^{\exp(k,0)} \cdot 3^{\exp(k,1)} \cdot 5^{\exp(k,2)}| + \chi_B\,(\exp\,(k,1)) + \overline{\text{sg}}\,(\exp\,(k,2))\right).$$

Die Gödelzahl der Folgekonfiguration der Konfiguration mit der Gödelzahl N bei der TM mit der Gödelzahl t

$F\,(t, N) = 2^u \cdot 3^v \cdot 5^w$ mit:

- für $N = 2^j \cdot 3^s \cdot 5^i$ $(N = \text{gö}\,([j, \sigma, z_i]) \quad s = \text{gö}(\sigma))$
- und $\kappa = \exp\,(s, j)$ (Nummer des Zeichens im Feld j bei σ: $\sigma\,(j) = x_\kappa$)
- $\lambda = \exp\,(t, i-1)$ (Zeile des Zustands z_i in TM T).
- $\mu = \exp\,(\lambda, \kappa)$ $(\delta\,(z_i, x_\kappa))$

gilt:

$$\begin{aligned} u &= \left.\begin{cases} j, & \text{falls } \exp\,(\mu,1) = 0 \quad (\star N) \\ j+1, & \text{falls } \exp\,(\mu,1) = 1 \quad (\star R) \\ j-1, & \text{falls } \exp\,(\mu,1) = 2 \quad (\star L) \end{cases}\right\} = j + \exp\,(\mu,1) \dot{-} \left(\exp\,(\mu,1) \dot{-} 1\right) \cdot 3 \\ v &= \frac{s}{q_j^\kappa} \cdot q_j^{\exp(\mu,0)} \\ w &= \exp\,(\mu, 2) \end{aligned}$$

Stop: $\exp\,(\mu,1) = 3$ nicht berücksichtigt $\delta\,(z_i, x) = [x, \sigma, z_i]$

Lemma 3.5.10

$$\tilde{F}\,(t, N) := \begin{cases} F\,(t,N), & \text{falls } \chi_{\mathcal{TM}}\,(t) = \sigma \text{ und } \chi_K\,(N) = 0 \text{ und } \text{gö}^{-1}\,(N) \\ & \text{keine Stop–konfiguration von } \text{gö}^{-1}\,(t) \text{ ist} \\ 0, & \text{sonst} \end{cases}$$

ist primitiv-rekursiv.

Die Folge der Gödelzahlen der Konfigurationen, die von der TM T bei Start in einer Anfangs–Konfiguration durchlaufen werden

Bei Stop wird die letzte Konfiguration wiederholt. Eine Anfangs–Konfiguration (bei der Berechnung einer n-stelligen Funktion) sieht wie folgt aus:

$\star|^{a_1+1}\star\cdots\star\underset{\triangle}{|^{a_n+1}\star}\ \star\cdots$, d. h.

$$K_{a_1a_2\cdots a_n} := \left[n+\sum_{v=1}^{n}(a_v+1)\,, \sigma_{a_1,\dots a_n}\,, z_1\right]$$

$A_T\,(a_1,\dots,a_n,i)$ sei die Gödelzahl der i-ten Konfiguration in der Folge der Konfigurationen, die T bei Start in $K_{a_1,\dots,a_n}$ durchläuft

Dann ist $A_T\,(a_1,\dots,a_n,0) = \text{gö}\,(K_{a_1,\dots,a_n})$;

$$A_T\,(a_1,\dots,a_n,i+1) = \begin{cases} A_T\,(a_1,\dots,a_n,i)\,, \text{ falls dies Stop–Konfiguration ist} \\ F\,(\text{gö}\,(T)\,, A_T\,(a_1,\dots,a_n,i))\,, \text{ sonst} \end{cases}$$

Also: A_T ist primitiv-rekursiv.

Lemma 3.5.11
Die Funktion $A\,(t,a_1,\dots,a_n,j) = \begin{cases} A_T\,(a_1,\dots,a_n,j)\,, \text{ falls } \chi_{\mathcal{TM}}\,(t)=0, T=\text{gö}^{-1}\,(t) \\ 0, \text{ sonst} \end{cases}$
ist primitiv-rekursiv.

Die Funktion β

$$\beta\,(t,a_1,\dots,a_m,j) := \begin{cases} 0, & \text{falls } j = 2^{\exp(j,0)}\cdot 3^{\exp(j,0)} \text{ und} \\ & \exp\,(j,1) = A\,(t,a_1,\dots,a_n,\exp\,(j,0)) > 0 \text{ und} \\ & \quad \mu = \exp(\quad \exp[t,\exp(\underbrace{\exp\,(j,1)}_{\text{w. Kopf}},2) \dot{-} 1], \\ & \qquad\qquad \exp\,[\exp\,(\exp\,(j,1)\,,1)\,,\exp\,(\exp(j,1),0)]) = 3 \\ 1, & \text{sonst} \end{cases}$$

Lemma 3.5.12

1. $\beta\,(t,a_1,\dots,a_n) = 0$ gdw
   (a) t ist Gödelnummer einer TM T,
   (b) es gibt Zahlen k,l mit $j = 2^k\cdot 3^l$
      i. $k \geq 0$
      ii. l ist Gödelzahl der Konfiguration, die T nach k Takten erreicht hat, wenn T in $K_{a_1,\dots,a_n}$ gestartet wurde.
      iii. Im Takt k hat T schon gestoppt.
2. β ist primitiv-rekursiv.

Die Resultatfunktion α

$$\alpha(n) := \begin{cases} b, & \text{falls } n > 0 \text{ und für die Zahl } n^\star = \exp(n,1) \text{ gilt} \\ & \quad 1.\ \chi_K(n^\star) = 0 \ (\star n^\star = 2^{k\star} \cdot 3^{\text{gö}(\sigma)} \ldots 5^i \star) \\ & \quad 2.\ \text{Für } k^\star = \exp(n^\star, 0) \text{ mit } \sigma \text{ mit } \sigma(i) = \exp(\exp(n^\star,1),1) \text{ gilt} \\ & \qquad b = \left[\sum_{j=0}^{k^\star-2} \left(\prod_{i=j+1}^{k^\star-1} \sigma(i) \mathbin{\dot{-}} \prod_{i=j}^{k^\star-1} \sigma(i)\right)(k^\star - j - 1)\right] - 1 \\ 0, & \text{sonst} \end{cases}$$

Beispiel:

Lemma 3.5.13

1. Ist $n > 0, n^\star = \exp(n,1) = \text{gö}([k^\star, \sigma, z_l])$ mit $\sigma = \star W \star |^{b+1} \star \underset{\triangle}{\star} \cdots$, so ist

   $\alpha(n) = b$

2. α ist primitiv-rekursiv.

Satz 3.5.14
Jede Turing-berechenbare Funktion ist partiell-rekursiv.

Beweis: Es sei f n-stellig, berechnet von TM T, ferner sei

- $t = \text{gö}(T)$
- $a_1, \ldots, a_n \in \mathbb{N}$.
- $[a_1, \ldots, a_n] \in D_f$ gdw. T bei Start in $K_{a_1,\ldots,a_n}$ stoppt mit einer Konfiguration der Form von Lemma 3.5.13 gdw. es gibt ein j mit $\beta(t, a_1, \ldots, a_n, j) = 0$.

Wenn $[a_1, \ldots, a_n] \in D_f$ $f(a_1, \ldots, a_n) = \alpha(\mu(\beta(t, a_1, \ldots, a_n, j) = 0))$.
Wenn $[a_1, \ldots, a_n] \notin D_f$

$\rightarrow$ T stoppt nicht bei Start in $K_{a_1,\ldots,a_n}$

$\rightarrow$ es gibt kein j mit $\beta(\cdots, j) = 0$.

$\rightarrow$ $\alpha(\cdots)$ — nicht definiert.

$\rightarrow$ $f(a_1, \ldots, a_n) = \alpha(\mu(\beta(t, a_1, \ldots, a_n, j) = 0))$.

$\rightarrow$ F — partiell–rekursiv.

□

f — partiell–rekursiv $\rightarrow$ es gibt eine TM T, die f berechnet $\rightarrow$ $f = \alpha(\mu(\beta(\cdots)))$.

Folgerung 3.5.15 (Kleenescher Darstellungssatz)
Es gibt eine primitiv–rekursive Funktion α derart, daß für jede Stellenzahl n eine $(n+2)$-stellige primitiv–rekursive Funktion β so existiert, daß zu jeder partiell–rekursiven Funktion f eine Zahl t existiert so, daß für alle $[a_1, \ldots, a_n]$ gilt:

$$f(a_1, \ldots, a_n) = \alpha(\mu(\beta(t, a_1, \ldots, a_n, j) = 0)).$$

3.6 Die Unentscheidbarkeit des PK 1

1. Darstellung zahlentheoretischer Funktionen im PK

   $n \to A^1 \to$ (Interpretation) Prädikat, das auf genau n Elemente von I zutrifft.

   Zugehörige Anzahlaussage $\exists i!!xH(x)$ sei Abkürzung für:

$$\begin{array}{ll} \text{falls } i=0 & \neg\exists xH(x) \\ i=1 & \exists x_1 (H(x_1) \wedge \forall x_2 (H(x_2) \to x_2 = x_1)) \\ \vdots & \\ i & \exists x_1 \cdots \exists x_i \big(H(x_1) \wedge \cdots \wedge H(x_i) \wedge \neg x_1 = x_2 \wedge \cdots \neg x_1 = \\ & x_3 \wedge \cdots \wedge \neg x_{i-1} = x_i \wedge \forall x_{i+1} (H(x_{i+1}) \to x_{i+1} = \\ & x_1 \vee \cdots \vee x_{i+1} = x_i)\big) \end{array}$$

   $\phi : \mathbb{N}^m \to \mathbb{N}$ heißt durch $H \in$ AUSD bzgl. $\left\{A_1^1, \ldots, A_{m+1}^1\right\}$ in I dargestellt, wenn für alle $j_1, \ldots, j_m \in \mathbb{N}$ gilt: $\phi(j_1, \ldots, j_m) = j_{m+1}$ gdw. $(H \wedge \exists j_1!!xA_1x \wedge \cdots \wedge \exists j_n!!xA_mX \wedge \exists j_{m+1}!!xA_{m+1}x) \in \mathrm{ef}_I$

   Beispiel: $N(k) = k+1$ bzgl. A_1, A_2
   $H \equiv \exists x_1 (\neg A_1 x_1 \wedge \forall x_2 (A_2 x_2 \leftrightarrow A_1 x_2 \vee x_2 = x_1))$.
   $N(j) = k$ gdw. $(H \wedge \exists j!!xA_1 \wedge \exists k!!xA_2 x) \in \mathrm{ef}_I$

2. Konstanten $C_i^n(j_1, \ldots, j_m) = i$:
   $H \equiv \exists i!!xA_{n+1}x$

3. Argumentauswahlfunktionen $I_i^n(j_1, \ldots, j_n) = j_i$
   $H \equiv \forall x (A_i x \leftrightarrow A_{n+1} x)$

Folgerung 3.6.1
Die ANF–Funktionen sind im PK darstellbar.

Satz 3.6.2
Alle partiell–rekursiven Funktionen sind im PK darstellbar.

Beweis: *ohne*

3.6.1 Kodierung von Ausdrücken durch Zahlen–„Gödelisierung“

Alphabet Y	$\neg$	$\wedge$	$\vee$	$\leftarrow$	$\leftrightarrow$	(	)	,	=	$\forall$	$\exists$	a	x	A	F	$\star$	|
Numerieren:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Für $\xi_1\xi_2\cdots\xi_n \in W(Y)$ sei

$$\text{gö}(\xi_1 \ldots \xi_n) = \prod_{j=0}^{n-1} q_j^{N(\xi_i)}$$

z. B.: $\text{gö}(x = x\star) = 2^{13} \cdot 3^9 \cdot 5^{13} \cdot 7^{16}$

Satz 3.6.3

1. Die Funktion gö ist eineindeutig.

2. Die charakteristische Funktion χ_{AUSD} mit

$$\chi_{\text{AUSD}}(n) = \begin{cases} 0, & \text{falls es } H \in \text{AUSD gibt, mit } n = \text{gö}(H) \\ 1, & \text{sonst} \end{cases}$$

ist primitiv-rekursiv.

Annahme: I unendlich, ef_I–entscheidbar.

$$\rightarrow \chi_{\text{ef}_I}(H) = \begin{cases} 0, & H \in \text{ef}_I \\ 1, & \text{sonst} \end{cases}$$

ist berechenbar, d. h. die Funktion

$$\chi_{\text{gö}(\text{ef}_I)}(n) = \begin{cases} 0, & n = \text{gö}(H) \text{ für } H \in \text{ef}_I \\ 1, & \text{sonst} \end{cases}$$

ist berechenbar $\rightarrow$ partiell–rekursiv $\rightarrow$ (überall definiert) allgemein–rekursiv.
□

Sei $H \in \text{AUSD}$

1. $S(H) \equiv H \wedge \exists \text{gö}(H)!!x_1 A_1 x_1 \wedge \exists_0!!x_1 A_2 x_1$
2. $\sigma(n) := \begin{cases} \text{gö}(S(H)), & n = \text{gö}(H) \\ 0, & \text{sonst } (\chi_{\text{AUSD}}(n) = 1) \end{cases}$

Lemma 3.6.4
$\sigma(n)$ ist allgemein-rekursiv.

Für beliebiges $H \in \text{AUSD}$ gilt: $H \in \text{ef}_I$ gdw. $\chi_{\text{gö}(\text{ef}_I)}(\text{gö}(H)) = 0$.
also

$$\begin{aligned} S(H) \in \text{ef}_I \quad & \text{gdw.} \quad \chi_{\text{gö}(\text{ef}_I)}(\text{gö}(S(H))) = 0. \\ & \text{gdw.} \quad \chi_{\text{gö}(\text{ef}_I)}(\sigma(\text{gö}(H))) = 0. \end{aligned}$$

also $S(H) \notin \text{ef}_I$ gdw. $\overline{\text{sg}}\left(\chi_{\text{gö}(\text{ef}_I)}(\sigma(\text{gö}(H)))\right) = 0$.

Wir setzen $\psi(n) := \overline{\text{sg}}\left(\chi_{\text{gö}(\text{ef}_I)}(\sigma(n))\right)$ ist allgemein–rekursiv. Nach dem Darstellungssatz gilt:

Es gibt $H^\star \in \text{AUSD}$ mit $\psi(m) = n$ gdw. $(H^\star \wedge \exists m!!xA_1x_1 \exists n!!xA_2x) \in \text{ef}_I$

Also: $\psi(m) = 0$ gdw. $(H^\star \wedge \exists n!!xA_1x_1 \exists_0!!xA_2x) \in \text{ef}_I$,
d. h. für alle $H \in \text{AUSD}$ gilt:

$$\psi(\text{gö}(H)) = 0 \text{ gdw. } (H^\star \wedge \exists n!!xA_1x_1 \exists_0!!xA_2x) \in \text{ef}_I$$

haben:

$$(H \wedge \exists \text{gö}(H)!!xA_1x_1 \wedge \exists_0!!xA_2x) \notin \text{ef}_I \text{ gdw.} \tag{3.6.2}$$
$$S(H) \notin \text{ef}_I \text{ gdw.}$$
$$\psi(\text{gö}(H)) = 0 \text{ gdw.}$$
$$(H^\star \wedge \exists \text{gö}(H)!!xA_1x \wedge \exists_0!!xA_2x) \in \text{ef}_I\ . \tag{3.6.3}$$
$$\text{für } H = H^\star \text{ (3.6.2) in Widerspruch zu (3.6.3).} \tag{3.6.4}$$

$\rightarrow \text{ef}_I$ nicht entscheidbar.
□

Lösbare Fälle des Entscheidungsproblems:

1. endlicher Individuenbereich (hier kommt man mit Probieren durch)
2. „Klassenkalkül“ $\to$ PK1
   - ohne Funktionszeichen
   - ohne Konstanten
   - ohne Gleichheitszeichen
   - nur 1-stellige Attributenzeichen

Terme = Individuenvariable
prädikative Ausdrücke: $A_j x_i$

Satz 3.6.5
Es sei $H \in$ AUSD ohne Funktionszeichen, ohne Konstanten, ohne $=$ und mit k verschiedenen 1-stelligen Attributenzeichen, o. B. d. A. $A_1, \ldots, A_k$. Dann ist ef$H$ gdw. ein I mit $0 < \operatorname{card}(I) \leq 2^k$ existiert, mit $\text{ef}_I H$.

Beweis: Wenn $\text{ef}_I H$, so ef$H$
Haben $H \in \text{ef} \to$ es gibt Individuenbereich $I \neq \emptyset$ mit

$$\text{wert}_{I,g}(H, f) = W.$$

In H kommen $A_1, \ldots, A_k$ vor, sei $\alpha_i := g(A_i)$, $i = 1, \ldots, k$, d. h. $\alpha_I : I \to \{W, F\}$.

Wir definieren $a, b \in I$

$$a \sim b :\leftrightarrow \alpha_1(a) = \alpha(b) \wedge \alpha_2(b) = \alpha_2(b) \wedge \cdots \wedge \alpha_k(a) = \alpha_k(b)$$

Lemma 3.6.6
$\sim$ ist Äquivalenzrelation.

Betrachten $\overline{I} = {}^{I}\!/_{\sim}$, für $a \in I : [a]$ die Klasse nach $\sim$, in der a liegt.

Lemma 3.6.7
$1 \leq \operatorname{card}\left(\overline{I}\right) \leq 2^k$.

- Definieren $\overline{g}, \overline{f}$

$$\begin{aligned} \overline{g}(A_i)([a]) &:= g(A_i)(a) = \alpha_i(a) \,(\star \text{ o. k. nach def. von } \sim \star) \\ \overline{f}(x_i) &:= [f(x_i)] \end{aligned}$$

- z. z.: $\text{wert}_{I,g}(H, f) = \text{wert}_{\overline{I},\overline{g}}\left(H, \overline{f}\right)$

Beweis durch Induktion über H für alle Ausdrücke, die höchstens die Attributzeichen $A_1, \ldots, A_K$ enthalten.

A) $A_i x_j$

$$\begin{aligned} &\text{wert}_{\overline{I},\overline{g}}\left(A_i x_j, \overline{f}\right) = \\ &\quad \overline{g}(A_i)\left(\overline{f}(x_j)\right) = \overline{g}(A_i)([f(x_j)]) = g(A_i)(f(x_j)) = \text{wert}_{I,g}(A_i x_j, f). \end{aligned}$$

I) $-$

$$\begin{aligned} &\text{wert}_{\overline{I},\overline{g}}\left(\neg H, \overline{f}\right) = \\ &\quad \text{non}\left(\text{wert}_{\overline{I},\overline{g}}\left(H, \overline{f}\right)\right) = \text{non}\left(\text{wert}_{I,g}(H, f)\right) = \text{wert}_{I,g}(\neg H, f) \end{aligned}$$

–

$$\mathrm{wert}_{\overline{I},\overline{g}}\left(\left(H_1 \begin{matrix}\wedge\\ \vee\\ \rightarrow\\ \leftrightarrow\end{matrix} H_2\right), \overline{f}\right) =$$

$$\begin{matrix}\mathrm{et}\\ \vdots\end{matrix}\left(\mathrm{wert}_{\overline{I},\overline{g}}\left(H_1, \overline{f}\right), \mathrm{wert}_{\overline{I},\overline{g}}\left(H_1, \overline{f}\right)\right) = \mathrm{wert}_{I,g}\left(\left(H_1 \begin{matrix}\wedge\\ \vdots\end{matrix} H_2, f\right)\right)$$

– prädikatenlogische Zusammensetzung

$$\mathrm{wert}_{\overline{I},\overline{g}}\left(\forall x_j H, \overline{f}\right) = \mathrm{wert}_{I,g}\left(\forall x_j H, f\right) =$$

$$\mathrm{Om}\left(\alpha^1_{H,\overline{I},\overline{g},\overline{f},x_j}\right) = \begin{cases} W, & \text{falls für alle } \overline{\mathrm{i}} \in \overline{I} \alpha_{H,\overline{I},\overline{g},\overline{f},x_j}\left(\overline{i}\right) = W \\ F, & \text{sonst} \end{cases}$$

Es genügt zu zeigen:
(Für alle $\overline{i} \in \overline{I}$ ist $\alpha_{H,\overline{I},\overline{g},\overline{f},x_j i}\left(\overline{i}\right) = W$) gdw.
(für alle $i \in I$ gilt $\alpha_{H,I,g,f,x_j}(i) = W$)

$$\alpha_{H,\overline{I},\overline{g},\overline{f},x_j}([a]) = \mathrm{wert}_{\overline{I},\overline{g}}\left(H, \left[\overline{f}\right]^j_{[a]}\right) =$$

$$(\text{nach Ind.-Vor. und def. } f)\ \mathrm{wert}_{I,g}\left(H, [f]^j_a\right) = \alpha_{H,I,g,f,x_j}(a)$$

□

Analog für $\exists x_j H$.

Satz 3.6.8
Wenn H kein „=“ enthält, wenn $\mathrm{ef}_I H$ und $\mathrm{card}(I) \leq \mathrm{card}(J)$, so $\mathrm{ef}_J H$. ($\mathrm{ef}_I \subseteq \mathrm{ef}_J$).

Wir haben gesehen, daß die Menge ef_I genau dann entscheidbar ist, wenn I endlich ist.

Betrachten wir den folgenden Ausdruck H_0:

$$H_0 = \forall x\, \neg Axx \wedge \forall x \forall y \forall z (Axy \wedge Ayz \rightarrow Axz) \wedge \forall x \exists y\, Axy$$

Wenn H_0 in einem Individuenbereich I erfüllbar ist, dann existiert in I eine irreflexive und transitive zweistellige Relation, nennen wir sie „kleiner“, bei der zu jedem x ein y existiert mit x „kleiner“ y. Folglich ist I unendlich.

Damit gilt für jeden Ausdruck H, in dem das Attributzeichen A nicht vorkommt:

$(H \wedge H_0) \in \mathrm{ef}$ gdw. es einen unendlichen Individuenbereich I mit $H \in \mathrm{ef}_I$ gibt.

Man kann zeigen, daß H in einem unendlichen Individuenbereich I genau dann erfü llbar ist, wenn H im Individuenbereich $\mathbb{N}$ erfüllbar ist (Satz von Löwenheim–Skolem), d. h.

$$(H \wedge H_0) \in \mathrm{ef} \text{ gdw. } H \in \mathrm{ef}_{\mathbb{N}}.$$

Aus der Entscheidbarkeit von ef würde also die Entscheidbarkeit von $\mathrm{ef}_{\mathbb{N}}$ folgen, d. h.

ef ist nicht entscheidbar (also auch ag nicht).

3.7 Aussagenlogische Erfüllbarkeit und Gültigkeit

Die aussagenlogisch gültigen Ausdrücke des Prädikatenkalküls bilden eine wichtige Teilmenge von ag, die entscheidbar ist.

Definition 3.7.1

1. Ein Ausdruck $H \in$ AUSD heißt aussagenlogisch einfach, wenn er entweder prädikativer Ausdruck ist oder mit einem Quantor beginnt.

2. Es sei AE die Menge der aussagenlogisch einfachen Ausdrücke. Jede Abbildung $\beta : \mathrm{AE} \to \{W, F\}$ wird aussagenlogische Belegung genannt.

   Es ist klar, daß jeder Ausdruck $H \in$ AUSD des Prädikatenkalküls in eindeutiger Weise aus aussagenlogisch einfachen Ausdrücken mit Hilfe der aussagenlogischen Zusammensetzungen aufgebaut ist.

   Die Abbildung $\mathrm{werta}(H, \beta)$ wird für $H \in$ AUSD, $\beta : \mathrm{AE} \to \{W, F\}$ wie folgt induktiv definiert:

   Anfangsschritt:

   $$\text{Wenn } H \in \mathrm{AE}, \text{ so } \mathrm{werta}(H, \beta) = \beta(H)$$

   Induktionsschritte:

   $$\text{Wenn } H \equiv \neg H_1, \text{ so } \mathrm{werta}(H, \beta) = \mathrm{non}(\mathrm{wert}(H_1, \beta))$$
   $$\text{Wenn } H = (H_1 \wedge H_2)\,, \text{ so } \mathrm{werta}(H, \beta) = \mathrm{et}(\mathrm{werta}(H_1, \beta), \mathrm{werta}(H_2, \beta))$$

   und analog für $\vee$, $\to$, $\leftrightarrow$.

Ein Ausdruck $H \in$ AUSD heißt aussagenlogisch erfüllbar (bzw. gültig), wenn $\mathrm{werta}(H, \beta) = W$ für ein (bzw. alle) aussagenlogischen Belegungen β gilt. Es sei efa bzw. aga die Menge aller aussagenlogisch erfüllbaren bzw. gültigen Ausdrücke.

Satz 3.7.2
Es sei $I \neq \emptyset$, g Interpretation in I, f Belegung über I; und für $H \in$ AE sei $\beta(H) = \mathrm{wert}_{I,g}(H, f)$. Dann gilt für $H^\star \in$ AUSD

$$\mathrm{wert}_{I,g}(H^\star, f) = \mathrm{werta}(H^\star, \beta)$$

Diese Aussage beweist man leicht durch Induktion über den Aufbau von $H^\star$ aus aussagenlogisch einfachen Ausdrücken.

Folgerung 3.7.3

- ef $\subset$ efa
  $$\exists x(Ax \wedge \neg Ax) \in \mathrm{efa} \setminus \mathrm{ef}$$

- aga $\subset$ ag
  $$\forall x(Ax \vee \neg Ax) \in \mathrm{ag} \setminus \mathrm{aga}$$

- Die Mengen aga und efa sind entscheidbar.

3.8 Folgern, Ableiten, Widerlegen

3.8.1 Folgern

Sei $X \in$ AUSD $[g, f]$ ist ein Modell von X in I, wenn für alle $H \in X$ gilt: $\text{wert}_{I,g}(H, f) = W$.

Aus X folgt H (in I), $X \text{fol}_I H$, wenn jedes Modell von X in I den Ausdruck H erfüllt. Aus X folgt H: $X \text{fol} H$, wenn für jedes $I \neq \emptyset$ gilt: $X \text{fol}_I H$.

$\text{fl}_I(X) :=$ Menge aller H mit $X \text{fol} H$. $\text{fl}(X)$ analog

Satz 3.8.1 (Eigenschaften von fl_I, fl)

0. $H \in \text{fl}_I$ gdw. die Menge $X \cup \{\neg H\}$ kein Modell in I hat.
1. $\text{fl}_I(\emptyset) = \text{ag}_I$
2. fl_I hat die Hülleneigenschaften
3. fl_I erfüllt den Endlichkeitssatz (Beweis über Endlichkeitssatz für Modelle, analog AK).
4. Ableitbarkeitstheorem: Wenn $(H_1 \to H_2) \in \text{fl}_I(X)$, so $H_2 \in \text{fl}_I(X \cup \{H_1\})$.
5. Deduktionstheorem: Wenn $H_2 \in \text{fl}_I(X \cup \{X_1\})$,
   so $(H_1 \to H_2) \in \text{fl}_I$.
6. $\text{fl}_I(\text{ag}_I) \subseteq \text{ag}_I$, $\text{fl}(\text{ag}) \subseteq \text{ag}$

Beweis des Deduktionstheorems

Es sei $H_2 \in \text{fl}(X \cup \{H_1\})$ und $[I, g, f]$ ein Modell von X.

Behauptung: $\text{wert}_{I,g}(H_1 \to H_2, f) = W$

Fall1: $\text{wert}_{I,g}(H_1, f) = W \to [I, g, f]$ Modell von $X \cup \{H_1\}$. Es ist also $\text{wert}_{I,g}(H_2, f) = W$ nach Voraussetzung. Daraus folgt die Behauptung.

Fall2: $\text{wert}_{I,g}(H_1, f) = F \to \text{wert}_{I,g}((H_1 \to H_2), f) = W$.

Bemerkung: Die Relation $X \text{fol}_I H$ ist unentscheidbar, auch wenn X endlich ist. $(\emptyset \text{fol}_I H$ gdw. $\text{ag}_I H)$

3.8.2 Ableitbarkeit und Widerlegung

$X \subseteq$ AUSD, $H \in$ AUSD, wollen definieren $X \text{abl} H$.

Definition 3.8.2
$X \text{abl} H$

A) Wenn $H \in X$, so $X \text{abl} H$

I) 1. Wenn $X \text{abl} H_1$ und $X \text{abl} H_1 \to H_2$, so $X \text{abl} H_2$ (modus ponens)

$$\frac{\begin{array}{c} H_1 \\ H_1 \to H_2 \end{array}}{H_2}$$

2. Regel der vorderen Generalisierung

$$\frac{X\,\mathrm{abl}\,H_1\,(x) \rightarrow H_2}{X\,\mathrm{abl}\,\forall x H_1 \rightarrow H_2}$$

3. Regel der hinteren Generalisierung

$$\frac{X\,\mathrm{abl}\,H_1 \rightarrow H_2\,(x),\ \text{und } x \text{ nicht in } H_1.}{X\,\mathrm{abl}\,H_1 \rightarrow \forall x H_2}$$

4. Regel der vorderen Partikularisierung

$$\frac{X\,\mathrm{abl}\,H_1\,(x) \rightarrow H_2,\ x \text{ nicht in } H_2}{X\,\mathrm{abl}\,\exists x H_1 \rightarrow H_2}$$

5. Regel der hinteren Partikularsierung

$$\frac{X\,\mathrm{abl}\,H_1 \rightarrow H_2\,(x)}{X\,\mathrm{abl}\,H_1 \rightarrow \exists x H_2}$$

6. Regel der gebundenen Umbenennung
   Aus H entsteht H' durch gebundene Umbenennung, wenn gilt: es gibt Individuenvariablen x_k, x_l mit
   (a) x_k kommt in H gebunden vor
   (b) x_l kommt im Wirkungsbereich $H^\star$ von x_k in H nicht quantifizier und nicht frei vor,
   (c) $H^\star$ liegt in keinen Wirkungsbereich von x_l.
   (d) $H^\star$ entsteht aus H, indem in $Qx_kH^\star$ überall x_k durch x_l ersetzt wird

$$\frac{\begin{array}{c}X\,\mathrm{abl}\,H\\ H \text{ geht durch gebundene Umbenennung in } H' \text{ über}\end{array}}{X\,\mathrm{abl}\,H'}$$

Bsp.: $H \equiv y\forall\overbrace{xA^2xy}^{H^\star}$ $\qquad H' \equiv \exists y\forall zA^2zy.$ □

7. Termeinsetzung

$$\frac{\begin{array}{cl}X\,\mathrm{abl}\,H\,(x) & \\ T \text{ Term, wobei} & \text{alle Stellen in } H\text{, an denen } X \text{ steht, stehen in keinem Wirkungsbereich eines Quantors einer Variable, die in } T \text{ vorkommt}\end{array}}{X\,\mathrm{abl}\,H\,(X/_T)}$$

Wie im Aussagenkalkül, abla:

- $\mathrm{ab}\,(X) := \{H|X\mathrm{abl}H\}$
- $\mathrm{aba}\,(X) := \{H|X\mathrm{abla}H\}$

Satz 3.8.3 (Eigenschaften von ab **und** aba**)**

1. $\mathrm{ab}\,(\emptyset) = \mathrm{aba}\,(\emptyset) = \emptyset$;
2. ab und aba haben Hülleneigenschaften.
3. ab und aba erfüllen den Endlichkeitssatz.

4. Ableitbarkeitstheorem: $X\,\mathrm{abl}\,(H_1 \to H_2)$, so $X \cup \{H\}\,\mathrm{abl} H_2$.
5. Deduktionstheorem gilt nicht.
6.
   - Wenn $X \subseteq \mathrm{ag}_I$, so $\mathrm{ab}\,(X) \subseteq \mathrm{ag}_I$
   - Wenn $X \subseteq \mathrm{ag}_I$, so $\mathrm{aba}\,(X) \subseteq \mathrm{ag}_I$

Satz 3.8.4
Wenn für alle $H_1, H_2 \in$ AUSD gilt: $X\mathrm{abl}H_1 \to (H_2 \to H_1)$ und $X\mathrm{abl}H\,(x_j)$, so $X\mathrm{abl}\forall x_j H$.

Beweis: Es sei $H_0 \in$ AUSD, x_j kommt in H_0 nicht vor, $X\mathrm{abl}H_0$.

$$\frac{\begin{array}{c}X\mathrm{abl}H \to (H_0 \to H)\\ X\mathrm{abl}H\end{array}}{X\mathrm{abl}H_0 \to H\,(x_j)}\text{(nach Voraussetzung)}$$

hintere Generalisierung $\to X\mathrm{abl}(H_0 \to \forall x_j H)$, $X\mathrm{abl}H_0$, also $X\mathrm{abl}\forall x_j H$.

Definition 3.8.5
$\mathrm{Gen}\,(H)\,,\ H \in$ AUSD
$\mathrm{Gen}\,(H)$ ist einer der Ausdrücke, die aus H entstehen, wenn zuerst alle gebundenen Variablen nacheinander in nicht vorkommende Variablen umbenannt werden, dann alle vollfrei vorkommenden Variablen x mit $\forall x$ quantifiziert werden.

Beispiel:

$$H = \forall x\left(A^2yz \to B^2xy\right) \wedge C^1x.$$

$\to\ \forall n\left(A^2yz \to B^2ny\right) \wedge C^1x$: jetzt alle freien Variablen vollfrei

$$\to\ \forall z\forall y\forall n\left(\left(A^2yz \to B^2ny\right) \wedge C^2x\right)$$

□

Dual dazu Part (H).

Satz 3.8.6 (Ersatz für Deduktionstheorem)

Vor.:

$$X\mathrm{abl}\,(H' \to (H'' \to H')) \tag{3.8.5}$$
$$X\mathrm{abl}\,(H' \to H') \tag{3.8.6}$$
$$X\mathrm{abl}\,(H' \to (H'' \to H''')) \leftrightarrow ((H' \to H'') \to (H' \to H''')) \tag{3.8.7}$$
$$X\mathrm{abl}\,(H' \to (H'' \to H''')) \to (H'' \to (H' \to H''')) \tag{3.8.8}$$
$$X\mathrm{abl}\,(H' \to (H'' \to H''')) \leftrightarrow ((H' \wedge H'') \to H''') \tag{3.8.9}$$

Beh.: Wenn $(X \cup \{H_1\})\,\mathrm{abl}H_2$, so $X\mathrm{abl}\,(\mathrm{Gen}\,(H_1) \to H_2)$.

Bem.: Wenn H_1 Aussage, dann $\mathrm{Gen}\,(H_1) = H_1$.
Unter den Vorausetzungen (3.8.5)-(3.8.7) erfüllt abla das Deduktionstheorem.

Bew.: Durch Induktion über H_2.

Die syntaktische Charakterisierung des Folgerns, die wir im Aussagenkalkül durch die Gleichung

$$\mathrm{fl}(X) = \mathrm{aba}(\mathrm{abe}(\mathrm{axa}) \cup X)$$

vorgenommen haben, erfolgt ähnlich auch im Prädikatenkalkül. Man zeigt

Satz 3.8.7

$$\mathrm{fl}(X) = \mathrm{aba}(\mathrm{ag} \cup X)$$

Der Beweis verläuft ähnlich wie im Aussagenkalkül mit Hilfe des Endlichkeitssatzes für das Folgern. Es bleibt also ag syntaktisch zu charakterisieren. Dazu sei

$$\begin{aligned}\mathrm{AXA} = \{H \mid\ & H \text{ entsteht aus einem Axiom aus axa durch Ersetzen der} \\ & \text{Aussagenvariablen durch Ausdrücke aus AUSD}\}.\end{aligned}$$

Offenbar ist

$$\mathrm{AXA} \subseteq \mathrm{aga} \subseteq \mathrm{ag}.$$

Ferner sei

$$\begin{aligned}\mathrm{AXI} \;=\;& \{x_0 = x_0, x_0 = x_1 \to x_1 = x_0, x_0 = x_1 \wedge x_1 = x_2 \to x_0 = x_2\} \cup \\ & \{x_0 = x_1 \to A_i^j x_2 x_3 \cdots x_{k-1} x_0 x_{k+1} \cdots x_j \leftrightarrow A_i^j x_2 \cdots x_{k-1} x_1 x_{k+1} \cdots x_j \mid \\ & \hfill i \geq 0, k = 1, \ldots, j\} \cup \\ & \{x_0 = x_1 \to F_i^j(x_2, \ldots, x_k, x_0, x_{k+1}, \ldots, x_j) = F_i^j(x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_j) \mid \\ & \hfill i \geq 0, k = 1, \ldots, j\}\end{aligned}$$

und $\quad \mathrm{AX} := \mathrm{AXA} \cup \mathrm{AXI}.$

Man zeigt

Satz 3.8.8 (Axiomatisierbarkeit (Vollständigkeit) des PK 1)

$$\mathrm{ag} = \mathrm{ab}(\mathrm{AX})$$

Dabei ist die Widerspruchsfreiheit $\mathrm{ab}(\mathrm{AX}) \subseteq \mathrm{ag}$ leicht zu sehen, während die Vollständigkeit $\mathrm{ag} \subseteq \mathrm{ab}(\mathrm{AX})$ schwieriger zu beweisen ist.

Wir geben nun noch einige abgeleitete Schlußregeln für den Umgang mit Quantoren an:

- Quantoren–Einführung und –Beseitigung
  Voraussetzung: Die Individuenvariable x kommt vollfrei in $H \in \mathrm{AUSD}$ vor

  $$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, H(x)}{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\, H}$$

  (Wir erinnern daran, daß Schlußregeln mit fetten „Schlußstrichen" in beiden Richtungen gelten.)

  $$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, H(x)}{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\, H}\;, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\, H}{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\, H}$$

- Quantoren–Vertauschung

  $$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x \forall y\, H}{(X \cup \mathrm{AX})\mathrm{abl}\, \forall y \forall x\, H}\;, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x \exists y\, H}{(X \cup \mathrm{AX})\mathrm{abl}\, \exists y \exists x\, H}$$

  $$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x \forall y\, H}{(X \cup \mathrm{AX})\mathrm{abl}\, \forall y \exists x\, H}$$

- Quantoren–Verteilung

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\; (H_1(x) \wedge H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\, H_1 \wedge \forall x\, H_2}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\; (H_1(x) \wedge H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\, H_1 \wedge \exists x\, H_2}$$

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\; (H_1(x) \vee H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\, H_1 \vee \exists x\, H_2}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\, H_1 \vee \forall x\, H_2}{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\; (H_1(x) \vee H_2(x))}$$

- Quantoren–Verschiebung
Die Individuenvariable x komme in H_1 *nicht* vor:

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\; (H_1 \rightarrow H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\; (H_1 \rightarrow \forall x\, H_2)}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\; (H_1 \rightarrow H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\; (H_1 \rightarrow \exists x\, H_2)}$$

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\; (H_2(x) \rightarrow H_1)}{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\, H_2 \rightarrow H_1}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\; (H_2(x) \rightarrow H_1)}{(X \cup \mathrm{AX})\mathrm{abl}\; (\forall x\, H_2 \rightarrow H_1)}$$

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\; (H_1 \wedge H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\; (H_1 \wedge \forall x\, H_2)}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\; (H_1 \wedge H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\, H_1 \wedge \exists x\, H_2}$$

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\; (H_1 \vee H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\; (H_1 \vee \forall x\, H_2)}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\; (H_1 \vee H_2(x))}{(X \cup \mathrm{AX})\mathrm{abl}\, H_1 \vee \exists x\, H_2}$$

$$\frac{(X \cup \mathrm{AX})\mathrm{abl}\, \forall x\, \neg H}{(X \cup \mathrm{AX})\mathrm{abl}\, \neg\, \exists x\, H}\,, \quad \frac{(X \cup \mathrm{AX})\mathrm{abl}\, \exists x\, \neg H}{(X \cup \mathrm{AX})\mathrm{abl}\, \neg\, \forall x\, H}$$

Da es kein Entscheidungsverfahren für die Menge ag gibt, ag kann nur axiomatisiert werden als

$$\mathrm{ag} = \mathrm{ab(AX)},$$

können wir auch nicht durch ein algorithmisches Verfahren garantieren, daß eine Widerlegung für einen Ausdruck H gefunden wird, wenn er nicht allgemeingültig ist.

Wir gehen hier auf das *Widerlegen* ein, weil es eine große Rolle in der Wissensverarbeitung (in der künstlichen Intelligenz) spielt.

Im folgenden sei $X \subseteq \mathrm{AUSD}$ eine Menge von Aussagen ohne Identität, d. h. in denen das Gleichheitszeichen nicht vorkommt. Die Menge X möge das Wissen über ein Teilgebiet darstellen, also eine Art von Axiomensystem. Eine Vermutung sei durch eine Aussage H ohne Identität gegeben.

Die Aussage H folgt aus X ($H \in \mathrm{fl}(X)$), wenn jedes Modell von X H erfüllt, bzw. wenn $X \cup \{\neg H\}$ kein Modell hat. (Dabei spielen die Belegungen der Individuenvariablen keine Rolle, weil wir nur Aussagen betrachten.)

Zum Widerlegen brauchen wir einen syntaktischen Ableitungsbegriff, notiert durch $\vdash$, mit

$$X \vdash \bot \;\text{ gdw. } X \text{ kein Modell hat.}$$

Wir gehen vor wie im Aussagenkalkül und definieren

Definition 3.8.9

- Ausdrücke der Form $[\neg]A^i_j T_1 \cdots T_i$ (wobei A^i_j ein i-stelliges Attributensymbol ist und $T_1, \ldots, T_i$ Terme sind) werden Literal genannt.
- Als Klausel wird ein Literal oder eine Alternative von Literalen, bei der alle Individuenvariablen durch $\forall$ gebunden (generalisiert) sind, bezeichnet.

Die allgemeine Form einer Klausel ist also

$$\forall x_1 \cdots \forall x_k \; (\neg L_1 \vee \neg L_2 \vee \cdots \vee \neg L_n \vee L'_1 \vee \cdots \vee L'_m)$$

wobei die L_i, L'_j Literale und $x_1, \ldots, x_k$ alle vorkommenden Individuenvariablen sind. Als logisch äquivalente Schreibweise notiert man die Klausel wie folgt

$$L_1 \wedge L_2 \wedge \cdots \wedge L_n \;\rightarrow\; L'_1 \vee \cdots \vee L'_m$$

$$(\text{in Prolog:} \qquad L_1, \ldots, L_n \;\Rightarrow\; L'_1, \ldots, L'_m)$$

Es sei X eine Menge von Aussagen ohne Identität. Nach dem Endlichkeitssatz für Modelle hat X genau dann kein Modell, wenn eine endliche Teilmenge $X^\star = \{H_1, \ldots, H_k\} \subseteq X$ existiert, die kein Modell hat, d. h. genau dann, wenn die Einermenge $\{H^\star\}$ mit

$$H^\star = H_1 \wedge \cdots \wedge H_k$$

kein Modell hat.

Wir konstruieren zu $H^\star$ eine Menge K von Klauseln mit

$$\text{ef}\, H^\star \text{ gdw. } K \text{ hat kein Modell.}$$

Satz 3.8.10
Zu jeder Aussage H ohne Identität existiert eine Menge K von Klauseln mit

$$\text{ef}\, H^\star \text{ gdw. } K \text{ hat kein Modell.}$$

Beweis: Wir formen die Aussage H wie folgt semantisch äquivalent um:

1. Schritt: Die Zeichen $\rightarrow$, $\leftrightarrow$ eleminieren:

$$\begin{array}{lcl} H_1 \leftrightarrow H_2 & \sim & (H_1 \rightarrow H_2) \wedge (H_2 \rightarrow H_1) \\ H_1 \rightarrow H_2 & \sim & \neg H_1 \vee H_2 \end{array}$$

Betrachten wir als Beispiel

$$H \equiv \forall x \forall y\, (\exists z\, (Axz \vee Ayz) \rightarrow \exists z\, Bxyz);$$

wir erhalten nach dem ersten Schritt

$$H \sim \forall x \forall y\, (\neg \exists z\, (Axz \vee Ayz) \vee \exists z\, Bxyz)$$

2. Schritt: Das Zeichen $\neg$ wird vor die Attributenzeichen getrieben:

$$\begin{array}{rcl} \neg(H_1 \vee H_2) & \sim & \neg H_1 \wedge \neg H_2 \\ \neg(H_1 \wedge H_2) & \sim & \neg H_1 \vee \neg H_2 \\ \neg\neg H_1 & \sim & H_1 \\ \neg \forall x\, H_1 & \sim & \exists x\, \neg H_1 \\ \neg \exists x\, H_1 & \sim & \forall x\, \neg H_1 \end{array}$$

Im Beispiel erhalten wir

$$H \sim \forall x \forall y\, (\forall z\, (\neg Axz \wedge \neg Ayz) \vee \exists z\, Bxyz)$$

3. Schritt: Die Quantoren nach vorn ziehen:

$$\left.\begin{array}{lcl} Qx\,H_1(x) \wedge H_2 & \sim & Qx\ (H_1(x) \wedge H_2) \\ Qx\,H_1(x) \vee H_2 & \sim & Qx\ (H_1(x) \vee H_2) \end{array}\right\} \text{wobei } x \text{ nicht in } H_2 \text{ vorkommt}$$

$$\begin{array}{lcl} \forall x\,H_1(x) \wedge \forall x\,H_2(x) & \sim & \forall x\ (H_1(x) \wedge H_2(x)) \\ \exists x\,H_1(x) \vee \exists x\,H_2(x) & \sim & \exists x\ (H_1(x) \vee H_2(x)) \end{array}$$

Die Variable z komme weder in H_1 noch in H_2 vor

$$Q_1x\,H_1(x) \overset{\wedge}{\vee} Q_2x\,H_2(x) \quad \sim \quad Q_1xQ_2z\ \left(H_1(x) \overset{\wedge}{\vee} H_2\left({}^{x}\!/_{z}\right)\right)$$

Im Beispiel erhalten wir

$$\begin{array}{lcl} H & \sim & \forall x\forall y\,(\forall z\,(\neg Axz \wedge \neg Ayz) \vee \exists u\,Bxyu) \\ & \sim & \forall x\forall y\forall z\exists u\,((\neg Axz \wedge \neg Ayz) \vee Bxyu) \end{array}$$

4. Schritt: Den quantorenfreien Ausdruck in Form einer Konjunktion von Alternativen bringen

$$\begin{array}{lcl} (H_1 \wedge H_2) \vee H_3 & \sim & (H_1 \vee H_3) \wedge (H_2 \vee H_3) \\ H_1 \vee (H_2 \wedge H_3) & \sim & (H_1 \vee H_2) \wedge (H_1 \vee H_3) \end{array}$$

Im Beispiel:

$$H \sim \forall x\forall y\forall z\exists u\,((\neg Axz \vee Bxyu) \wedge (\neg Ayz \vee Bxyu))$$

Der jetzt erhaltene Ausdruck wird als pränexe Normalform ($\mathrm{PNf}(H)$) bezeichnet; bisher sind alle Umformungen semantisch äquivalent erfolgt, d. h. $\mathrm{ag}(H \sim \mathrm{PNf}(H))$.

5. Schritt: Elimination der $\exists$-Quantoren

Dieser Schritt führt von $H' = \mathrm{PNf}(H)$ nicht zu einem semantisch äquivalenten Ausdruck H'', sondern zu einem H'' mit

$$\mathrm{ef}\,H' \ \text{ gdw. } \mathrm{ef}\,H'',$$

was für unsere Zwecke ausreicht.

Sei $H = Q_1x_1 \cdots Q_nx_n\ \underbrace{H_0(x_1,\ldots,x_n)}_{\text{quantorenfrei}}$, Q_i sei das von links erste $\exists$

Fall 1: $i = 1$, $H \equiv \exists x_1 \ldots$

Wir nehmen eine (neue) Individuenkonstante a_j (nullstelliges Funktionszeichen) und setzen

$$H' \quad \equiv \quad Q_2x_2 \cdots Q_nx_n\,H_0\left[{}^{x_1}\!/_{a_j}\right]$$

Offenbar gilt $\mathrm{ef}\,H$ gdw. $\mathrm{ef}\,H'$

Fall 2: $i > 1$, $H \equiv \forall x_1 \cdots \forall x_{i-1}\exists x_iQ_{i+1}x_{i+1}\cdots$

Wir nehmen ein (neues) $(i-1)$-stelliges Funktionssymbol F_j^{i-1} her und setzen

$$H' \quad \equiv \quad \forall x_1 \cdots \forall x_{i-1}Q_{i+1}x_{i+1}\cdots Q_nx_n\,H_0\left[{}^{x_i}\!/_{F_j^{i+1}(x_1,\ldots,x_{i-1})}\right]$$

Diese Operation wird wiederholt bis alle $\exists$ eliminiert sind

Im Beispiel erhalten wir

$$H \approx \forall x \forall y \forall z\, ((\neg Axz \vee BxyF(x,y,z)) \wedge (\neg Ayz \vee BxyF(x,y,z)))$$

6. Schritt: Zerlegung in Klauseln

Es erfolgt eine Umbenennung der Variablen, so daß in jedem Konjunktionsglied verschiedene Variable sind.

$$\forall x\, (H_1(x) \wedge H_2(x) 0 \quad \sim \quad \forall x\, H_1 \wedge \forall y\, H_2 \left[{}^{x}\!/_{y}\right]$$

Im Beispiel:

$$H \approx \forall x \forall y \forall z\, (\neg Axz \vee BxyF(x,y,z)) \wedge \forall x' \forall y' \forall z'\, (\neg Ay'z' \vee Bx'y'F(x',y',z'))$$

Die Konjunktionsglieder liefern jetzt die Klauseln; d. h. in unserem Beispiel erhalten wir

$$\begin{array}{rlcl} K = & \{Axz & \rightarrow & BxyF(x,y,z), \\ & Ay'z' & \rightarrow & Bx'y'F(x',y',z')\} \end{array}$$

Bemerkung: Dies sind sogenannte HORN–Klauseln, d. h. sie haben nur ein positives Literal (auf der rechten Seite) (vgl. PROLOG).

Wir betrachten nun spezielle (syntaktische) Modelle und zeigen, daß diese zum Nachweis, daß eine Klauselmenge kein Modell hat, ausreichen.

Definition 3.8.11 (HERBRAND–Modell)
H sei eine Konjunktion von Klauseln. Wir setzen

$$\begin{array}{rcl} I_0 & = & \{a_0\} \cup \text{ Menge aller Konstantenzeichen, die in } H \text{ vorkommen} \\ I_{j+1} & = & I_j \cup \{F_k^n(t_1,\ldots,t_n) \mid F_k^n \text{ ist ein in } H \text{ vorkommendes Funkti-} \\ & & \qquad\qquad\qquad \text{onszeichen, } t_1,\ldots,t_n \in I_j\ \} \end{array}$$

$I_H = \bigcup_{j \geq 0} I_j$ ist eine Menge von Wörtern (Termen), die wir als Individuenbereich verwenden. Das Tripel $[I_H, g_H, f]$ heißt HERBRAND–Modell, wenn

$$g_H(a_i) = a_i \qquad \text{(für alle } a_i\text{, die in } H \text{ vorkommen)}$$

und

$$g_H(K_k^n)(t_1,\ldots,t_n) = F_k^n(t_1,\ldots,t_n) \qquad \text{(für alle } F_k^n\text{, die in } H \text{ vorkommen)}$$

ist.

In unserem Beispiel ist

$$\begin{array}{rcll} I_0 & = & \{a_0\} & \text{(in } K \text{ kommen keine Konstanten vor)} \\ I_1 & = & \{a_0, F(a_0,a_0,a_0)\} & \\ I_2 & = & \{a_0, F(a_0,a_0,a_0), F(F(a_0,a_0,a_0),a_0,a_0), \ldots\} & \end{array}$$

Satz 3.8.12
H sei eine Konjunktion von Klauseln. Dann gilt

$$\text{ef} H \quad \text{gdw. } H \text{ ein HERBRAND–Modell hat.}$$

Beweis: Es genügt zu zeigen, daß jeder erfüllbare Ausdruck ein HERBRAND–Modell hat. Es sei $[I, g, f]$ gegeben mit $\text{wert}_{I,g}(H, f) = W$, d. h. für jede Klausel

$$\forall x_1 \cdots \forall x_n\, H_0(x_1,\ldots,x_n)$$

gilt bei beliebiger Belegung $f' : \{x_1, \ldots, x_n\} \to I$

$$\mathrm{wert}_{I,g}(H_0, f') = W.$$

Entsprechend der Definition bestimmen wir I_H und g_H und vervollständigen g_H für Attributenzeichen wie folgt:

$$g_H(A^i_j)(t_1, \ldots, t_i) := \mathrm{wert}_{I,g}(A^i_j t_1 \cdots t_i, f)$$

Dabei hängt die rechte Seite (der zugeordnete Wahrheitswert) nicht von f ab, weil $A^i_j t_1 \cdots t_i$ keine Individuenvariablen enthält.

Es sei nun $f_H : X \to I_H$ eine Belegung und $A^i_j T_1 \cdots T_i$ ein Literal aus H_0. Dann gilt

$$\begin{aligned}
&\mathrm{wert}_{I_H,g_H}(A^i_j T_1 \cdots T_i, f_H) = \\
&= \; g_H(A^i_j)\,(\mathrm{element}_{I_H,g_H}(T_1, f_H), \ldots, \mathrm{element}_{I_H,g_H}(T_1, f_H)) \\
&= \; \mathrm{wert}_{I_H,g_H}\left(A^i_j T_1 \left[{}^{x_\gamma}\!/_{f_H(x_\gamma)}\right] \cdots T_i \left[{}^{x_\gamma}\!/_{f_H(x_\gamma)}\right], f\right)
\end{aligned}$$

wobei f eine beliebige I-Belegung ist.

Wir betrachten zu f_H die I-Belegung $f^\star$ mit

$$f^\star(x_\gamma) := \mathrm{element}_{I,g}\,(f_H(x_\gamma), f)$$

Die rechte Seite hängt von f nicht ab, weil $f_H(x_\gamma)$ ein Term ohne Individuenvariable ist. Ist z. B. $f_H(x_\gamma) = a_0$, so ist $\mathrm{element}_{I,g}\,(f_H(x_\gamma), f) = g(a_0)$. Nun ist

$$\begin{aligned}
\mathrm{wert}_{I,g}(A^i_j T_1 \cdots T_i, f^s tar) \;&=\; \mathrm{wert}_{I,g}\left(A^i_j T_1 \left[{}^{x_\gamma}\!/_{f_H(x_\gamma)}\right] \cdots T_i \left[{}^{x_\gamma}\!/_{f_H(x_\gamma)}\right], f\right) \\
&=\; \mathrm{wert}_{I_H,g_H}(A^i_j T_1 \cdots T_i, f_H)
\end{aligned}$$

folglich gilt für alle I_H-Belegungen f_H

$$\mathrm{wert}_{I_H,g_H}(H_0, f_H) = \mathrm{wert}_{I,g}(H_0, f^\star) = W,$$

denn alle Literale in H_0 haben bei $[I_H, g_H, f_H]$ denselben Wert wie bei $[I, g, f^\star]$; d. h. $\mathrm{wert}_{I_H,g_H}(\forall x_1 \cdots \forall x_n\, H_0, f_H) = W$, also hat H das HERBRAND–Modell $[I_H, g_H]$.

Der Test, ob eine Konjunktion von Klauseln ein HERBRAND–Modell besitzt, ist i. a. sehr aufwendig. Es gibt aber Fälle, wo man sofort sieht, daß kein Modell existiert:

$$H \equiv Aa_0 \wedge \neg Aa_0$$

d. h. als Klauselmenge geschrieben

$$\begin{array}{ccc} & & Aa_0 \\ Aa_0 & \to & \perp \end{array}$$

Die Schnittregel liefert hier sofort $\perp$.

Im Beispiel

$$H \equiv \forall y\, Aaf(y) \wedge \forall x\, \neg Axf(b)$$

bzw.

$$\begin{array}{ccc} & & Aaf(y) \\ Axf(b) & \to & \perp \end{array}$$

ist die Schnittregel nicht unmittelbar anwendbar, erst wenn man die Substitution ${}^{x}\!/_{a}$, ${}^{y}\!/_{b}$ ausgeführt hat, kommt man mit der Schnittregel zum Widerspruch $\perp$.

3.9 Unifikation

Definition 3.9.1
Eine Substitution σ ist eine Abbildung, die jeder Individuenvariablen einen Term zuordnet. Ist T ein Term, so bezeichne $T[\sigma]$ den Term, der entsteht, wenn simultan für jede Variable x_i der Term $\sigma(x_i)$ eingesetzt wird und $H[\sigma]$ bezeichnet den Ausdruck, der aus H in diesem Fall entsteht.

Eine Substitution σ heißt Unifikator für Ausdrücke H_1, H_2, wenn $H_1[\sigma] \equiv H_2[\sigma]$ ist.

Beispiel: $H_1 \equiv Aaxf(g(y)),\ H_2 \equiv Azf(z)f(v)$

	x	y	z	v
σ_1	$f(a)$	a	a	$g(a)$

$$H_1[\sigma_1] \equiv Aaf(a)f(g(a)) \equiv H_2[\sigma_1]$$

also σ_1 ist ein Unifikator für H_1, H_2.

	x	y	z	v
σ_2	$f(a)$	y	a	$g(y)$

$$H_1[\sigma_2] \equiv Aaf(a)f(g(y)) \equiv H_2[\sigma_2]$$

Auch σ_2 ist ein Unifikator für H_1, H_2, aber σ_2 ist allgemeiner als σ_1, weil eine Substitution σ_3 so existiert, daß

$$\sigma_3(\sigma_2(.)) = \sigma_1(.)$$

ist.

Definition 3.9.2 (allgemeinster Unifikator)
σ heißt allgemeinster Unifikator für H_1, H_2, wenn

1. σ ein Unifikator für H_1, H_2 ist
2. Zu jedem Unifikator σ' für H_1, H_2 eine Substitution $\sigma^\star$ mit

$$\sigma'(.) = \sigma^\star(\sigma(.))$$

   existiert.

3.9.1 Berechnung eines allgemeinsten Unifikators

Eingabe: $H_1 = A^i_j T_1 \cdots T_i$, $H_2 = A^i_j T'_1 \cdots T'_i$
zwei prädikative Ausdrücke mit dem gleichen Attributensymbol und disjunkten Variablenmengen

Ausgabe: allgemeinster Unifikator falls existent, „$\ominus$“ sonst.

PROCEDURE
$k := 0$; $M_0 := \{H_1, H_2\}$; $\sigma_0 = \mathrm{id}$
LOOP
IF $\mathrm{card}(M_k) = 1$ THEN RETURN σ_k END;
$T_k := \{t_1, t_2 | t_1, t_2$ bestimmen den von links ersten Unterschied in Ausdrücken von $M_k\}$;

IF Es gibt eine Variable y in T_k und einen Term t in T_k, in dem diese Variable nicht vorkommt
THEN

$$\sigma_{k+1}(x) = \begin{cases} t, & \text{falls } x = y \\ x, & \text{sonst} \end{cases}$$

$M_{k+1} := \sigma_{k+1}(M_k)$;
INC(k);
ELSE RETURN „⊖"
END
END;

Beispiele:

$$k = 0,\ M_0 = \{Aaxf(g(y)), Azf(z)f(v)\};\ \sigma_0 : \begin{array}{l} v \to v \\ x \to x \\ y \to y \\ z \to z \end{array}$$

$$\begin{array}{lcll}
T_0 & = & \{a, z\} & \\
\downarrow & & & \\
\sigma_1 & = & \begin{array}{l} v \to v \\ x \to x \\ y \to y \\ z \to a \end{array} & M_1 = \{Aaxf(g(y)), Aaf(a)f(v)\} \\
\downarrow & & & \\
T_1 & = & \{x, f(a)\} & \\
\sigma_2 & = & \begin{array}{l} v \to v \\ x \to f(a) \\ y \to y \\ z \to a \end{array} & M_2 = \{Aaf(a)f(g(y)), Aaf(a)f(v)\} \\
\downarrow & & & \\
T_2 & = & \{g(y), v\} & \\
\sigma_3 & = & \begin{array}{l} v \to g(y) \\ x \to f(a) \\ y \to y \\ z \to a \end{array} & M_3 = \{Aaf(a)f(g(y))\} \\
\downarrow & & & \\
\text{Stop} & & &
\end{array}$$

$$k = 0,\ M_0 = \{Af(a)g(x), Ayy\}$$

$$\begin{array}{lcll}
T_0 & = & \{f(a), y\} & \\
\sigma_1 & = & \begin{array}{l} x \to x \\ y \to f(a) \end{array} & M_1 = \{Af(a)g(x), Af(a)f(a)\} \\
T_1 & = & \{g(x), f(a)\} & \to \text{ enthält keine Variable} \\
 & & & \to ⊖
\end{array}$$

Also: Unifikation ermöglicht Anwendung der Schnittregel aber auch Vereinfachung von Klauseln!

Beispiel:

$$\begin{array}{lcll}
Ax \wedge Af(y) & \to & \perp & \\
 & & Af(g(a)) & \text{(Fakt)}
\end{array}$$

Unifizieren $\quad Ax \quad Af(y) \quad$ durch $\sigma : x \to f(y)$ und erhalten

$$\begin{array}{ccc} Af(y) & \to & \perp \\ & & Af(g(a)) \end{array}$$

Unifizieren: $\quad y \to g(a)$

$$\begin{array}{ccc} Af(g(a)) & \to & \perp \\ & & Af(g(a)) \end{array}$$

Cut liefert $\perp$

also ist die ursprüngliche Klauselmenge nicht erfüllbar und hat kein Modell.

Definition 3.9.3
$K_1 : L_1 \wedge \cdots \wedge L_n \to L'_1 \vee \cdots \vee L'_m$ und $K_2 : L^\star_1 \wedge \cdots \wedge L^\star_{n^\star} \to L''_1 \vee \cdots \vee L''_{m'}$ seien Klauseln mit disjunkten Variablenmengen.

1. Resolvente (Resolutionsregel)
   σ sei allgemeinster Unifikator von L'_μ und $L^\star_\gamma$. Die Klausel

   $$\sigma(L_1 \wedge \cdots \wedge L_n \wedge L^\star_1 \wedge \cdots \wedge L^\star_{\gamma-1} \wedge L^\star_{\gamma+1} \wedge \cdots \wedge L^\star_{n^\star} \to \\ L'_1 \vee \cdots \vee L'_{\mu-1} \vee L'_{\mu+1} \vee \cdots \vee L'_m \vee L''_1 \vee \cdots \vee L''_{m'})$$

   heißt Resolvente von K_1, K_2 bzgl. μ, γ und σ.

2. Ist σ ein allgemeinster Unifikator von L'_i, L'_j $(1 \leq i < j \leq m)$, so heißt

   $$\sigma(L_1 \wedge \cdots \wedge L_n \to L'_1 \vee \cdots \vee L'_{i-1} \vee L'_{i+1} \vee \cdots \vee L'_m)$$

   ein rechter Faktor von K_1.

3. Ist σ ein allgemeinster Unifikatorr von L'_i, L'_j $(1 \leq i < j \leq n)$, so ist

   $$\sigma(L_1 \wedge \cdots \wedge L_{i-1} \wedge L_{i+1} \wedge \cdots \wedge L_n \to L'_1 \vee \cdots \vee L'_m)$$

   ein linker Faktor von K_1.

Definition 3.9.4 ($Y \vdash H$)
Es sei Y eine Menge von Klauseln, H eine Klausel.

Anfangsschritt: Wenn $H \in Y$, so $Y \vdash H$

Induktionsschritt:

1. Wenn $Y \vdash K_1$ und $Y \vdash K_2$ und H ist Resolvente von K_1, K_2, so $Y \vdash H$.
2. Wenn $Y \vdash K$ und H ist rechter oder linker Faktor von K, so $Y \vdash H$.

Satz 3.9.5
Es sei Y eine Menge von Klauseln, die kein Modell hat. Dann ist $Y \vdash \perp$.

Beweisidee: Wenn Y kein Modell hat, so besitzt Y kein HERBRAND–Modell. Also gibt es Klauseln $K_1, \ldots, K_n \in Y$ und Substitutionen $\sigma_1, \ldots, \sigma_n$ derart, daß aus $\{K_1[\sigma_1], \ldots,$
$K_n[\sigma_n]\}$ aussagenlogisch (mit der Schnittregel) der Widerspruch $\perp$ abgeleitet werden kann. Aus einer solchen Ableitung konstruiert man eine Ableitung gemäß $\vdash$.[4]

Noch ein **Beispiel:**

$$
\begin{array}{rrcl}
K_1: & Ax \wedge Ab & \rightarrow & \perp \\
K_2: & Aa & \rightarrow & Ab \\
K_3: & Ab & \rightarrow & Aa \\
K_4: & & & Aa \vee Ay
\end{array}
$$

Resolution $K_1, K_2,\ x \rightarrow a$

$$
\begin{array}{rrcl}
 & Aa \wedge Ab & \rightarrow & \perp \\
 & Aa & \rightarrow & Ab \\
\cline{2-4}
K_5: & Aa & \rightarrow & \perp \\
\mathrm{Cut}(K_5, K_3): & Ab & \rightarrow & Aa \\
\cline{2-4}
K_6: & Ab & \rightarrow \perp &
\end{array}
$$

Resolution $K_4, K_6,\ y \rightarrow b$

$$
\begin{array}{rrcl}
 & & & Aa \vee Ab \\
\cline{2-4}
K_7: & & & Aa \\
\mathrm{Cut}(K_7, K_5): & Aa & \rightarrow & \perp \\
\cline{2-4}
 & & & \perp
\end{array}
$$

Literaturverzeichnis

[1] J. Rusza. Die Begriffswelt der Mathematik; Volk und Wissen Verlag, Berlin, 1975.

[2] D. Klaua. Elementare Axiome der Mengenlehre; WTB, Bd 81, Akademie-Verlag, Berlin, 1971.

[3] P. Bachmann. Mathematische Grundlagen der Informatik; Akademie-Verlag, 1992.

[4] Cordes/Kruse/Langendörfer/Rust. Prolog: Eine methodische Einführung; Vieweg Verlag.