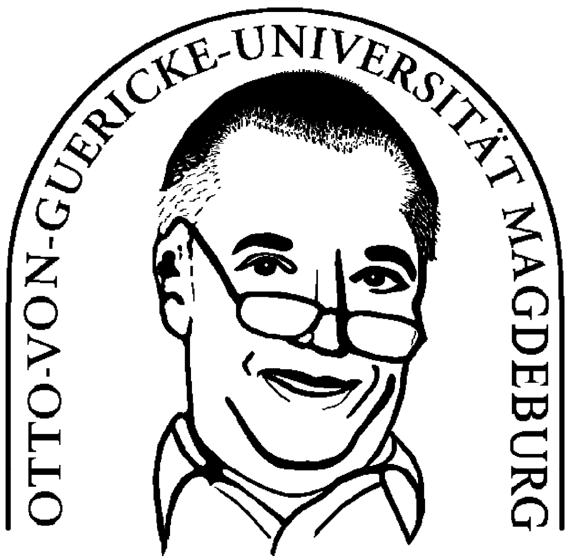


Logik-Vorlesungen

H. Hollatz

Versionsdatum: 24. Juni 2003

horst.hollatz.de — horst@hollatz.de

Vorwort

Diese Vorlesung halte ich seit dem Jahre 1985, dem Beginn des Studienganges Informatik an der damaligen Otto-von-Guericke-Hochschule in Magdeburg. Auf Drängen mehrerer Kollegen aus der Informatik habe ich im Sturmherbst des Jahres 1989 mit der Niederschrift begonnen. Im Jahre 1993 entschied ich mich unter dem Druck der neuen Medien, dem Manuskript die vorliegende Form zu geben.
Im Laufe der Jahre wurden die einzelnen Teile mehrfach überarbeitet. So gibt es seit dem Jahre 2000 Programme zu einigen Algorithmen (über meine www-Seite beziehbar); dabei wurde keine Vollständigkeit angestrebt.
Der mathematische Inhalt der Vorlesung ist weitgehend klassisch; er geht insbesondere auf eigene Mitschriften während des Studiums und meine nun mehr als drei Jahrzehnte währende Lehrtätigkeit zurück. Dankbar erinnere ich mich an die interessanten Logik-Vorlesungen, die K. SCHRÖTER in den 60-er Jahren an der Humboldt-Universität gehalten hat; seine Sicht und Darstellung haben die meine geprägt. Aus der von Schröter geführten Berliner Logikschule ging G. ASSER hervor, der Schröters Intensionen fortführte und in Teubner-Büchern zur Aussagen- und Prädikatenlogik eine schriftliche Form gegeben hat, die hier eingeflossen ist. Der hiermit vorliegende Text enthält das 4. Kapitel der Gesamtvorlesung.
Der Text ist kein Ersatz für die Vorlesung, was der geneigte Interessent beim Lesen bald merken wird. Neben der Vermittlung von grundlegendem, mathematischem Wissen besteht das Ziel der Einführung nicht vorrangig im Beschreiben und Üben mathematischer Techniken, sondern im Erlernen der mathematischen Denk- und Ausdrucksweise, treu dem Grundsatz: Nicht das Ziel ist das Leben, sondern der Weg, auch dann, wenn man das Ziel verfehlt. Das Wesen der Mathematik besteht nicht in ihren Resultaten, sondern in den Methoden, mit denen sie erreicht werden.
Von Studenten und Kollegen habe ich vielfache Unterstützung erhalten, wofür ich mich herzlich bedanke. Besonders möchte ich Frau Bianca Truthe hervorheben, die die Zeichnungen (einschließlich der Mathematiker-Übersicht auf der Zeitkarte) angefertigt, das gesamte Manuskript kritisch korrigierend studiert und wesentlich an der technischen Gestaltung mitgewirkt hat; fruchtbare Streitgespräche mit ihr haben zu Veränderungen der Darstellung geführt, die auch als Verbesserungen anzusehen sind. Die Übungsaufgaben wurden wesentlich von Frau Ute Förster zusammenge-

stellt; sie konnte dabei Sammlungen meiner anderen Übungsleiter verwenden, wie z. B. von Dr. Peter Szyler, Dr. Norbert Schieweck und Dr. Michael Schaper. Ich danke ihnen allen.

Magdeburg, im Juni 2003

Horst Hollatz

Inhaltsverzeichnis

Kapitel 1

Aussagenlogik

1.1. Aussagen

Menschen haben die Fähigkeit, Verhältnisse der Wirklichkeit in Aussagen zu formulieren. Wir wollen hier nicht die philosophischen Schwierigkeiten dieses Satzes diskutieren. Wir begnügen uns mit einem naiven Standpunkt: In gesprochenen Sätzen, in mathematischen, physikalischen, chemischen Formeln, in bildlichen Darstellungen drücken Menschen etwas aus, was sie Aussagen nennen. Solche Aussagen haben für den Menschen eine grundlegende Eigenschaft: Sie behaupten, dass sich gewisse Dinge der Wirklichkeit in gewisser Weise verhalten. Wenn sich die Dinge so wie behauptet verhalten, sprechen wir von einer wahren Aussage, andernfalls sagen wir: Die Aussage ist falsch. Formal sagen wir, dass eine Aussage dadurch von anderen Objekten unterschieden wird, dass ihr der Wert „wahr" oder „falsch" zugeordnet ist. Dabei gelten zwei wesentliche Prinzipien:

Prinzip der Zweiwertigkeit: Jede Aussage ist entweder wahr oder falsch.

Prinzip vom ausgeschlossenen Widerspruch: Es gibt keine Aussage, die sowohl wahr als auch falsch ist.

Damit gibt es zwei Klassen von Aussagen: Die Klasse W der wahren und die Klasse F der falschen Aussagen. Wenn eine Aussage A zur Klasse W gehört, sagen wir: Aussage A hat den Wahrheitswert W; entsprechend im anderen Falle. So hat die Aussage „2 ist die gerade Primzahl" den Wahrheitswert W, während die Aussage „11 ist eine gerade Zahl" den Wahrheitswert F hat. Ausdrücklich sei angemerkt: Die Frage, ob und wie man von einer Aussage entscheiden kann, welchen Wahrheitswert sie hat, bleibt offen. Aus dem täglichen Umgang mit Aussagen wissen wir, dass man mittels Bindewörtern neue Aussagen bilden kann. In dem noch aufzubauenden formalen Apparat werden die Bindewörter durch Operatoren modelliert. Ein solcher

Operator heißt **Aussagenfunktion**. Die üblichen sind folgende, falls A, B beliebige Aussagen darstellen:

Negation: nicht A,

Konjunktion: A und B,

Alternative: A oder B,

Implikation: wenn A, so B,

Äquivalenz: A genau dann, wenn B.

Die Negation ist eine einstellige Aussagenfunktion; die übrigen klassischen Aussagenfunktionen sind zweistellig. Die Alternative wird oft auch **Disjunktion** genannt. Allgemein ist eine n**-stellige Aussagenfunktion** eine Abbildung, die jedem n-Tupel von Aussagen genau eine Aussage zuordnet. Bei den obigen klassischen Aussagenfunktionen hängt der Wahrheitswert der Bildaussage aussschließlich von den Wahrheitswerten jener Aussagen ab, aus denen das Bild entstanden ist. Solche Aussagenfunktionen heißen **extensional**. Hier werden wir nur extensionale Aussagenfunktionen betrachten.
Zu mehrstelligen, extensionalen Aussagenfunktionen kommt man z. B. dadurch, dass man in Aussagen der Form „nicht A“, „A oder B“ usw. für A und B wieder Aussagen einsetzt, die ihrerseits aus klassischen Aussagenfunktionen aufgebaut sind. Dies nennt man **Superposition**. Zwei n-stellige Aussagenfunktionen α_1, α_2 heißen **logisch äquivalent**, wenn für alle n-Tupel $(A_1, \ldots, A_n)$ von Aussagen die beiden Aussagen $\alpha_1(A_1, \ldots, A_n)$ und $\alpha_2(A_1, \ldots, A_n)$ den gleichen Wahrheitswert haben. Die logische Gleichwertigkeit von Aussagen ist offensichtlich eine Äquivalenzrelation. Die Äquivalenzklassen abstrahieren von allen Eigenschaften der Aussagen bis auf ihren Wahrheitswert. Jeder n-stelligen, extensionalen Aussagenfunktion ist genau eine Funktion zugeordnet, die jedem n-Tupel von Wahrheitswerten genau einen Wahrheitswert zuordnet; diese Funktion heißt n**-stellige Wahrheitsfunktion**. Jede n-stellige Wahrheitsfunktion repräsentiert genau eine Äquivalenzklasse. So entsprechen den klassischen Aussagenfunktionen die folgenden Wahrheitsfunktionen:

- Negation $\rightarrow$ not: $\text{not}(W) = F$, $\text{not}(F) = W$,
- Konjunktion $\rightarrow$ and:

$$\text{and}(W, W) = W, \ \text{and}(W, F) = \text{and}(F, W) = \text{and}(F, F) = F,$$

- Alternative $\rightarrow$ or: $\text{or}(F, F) = F$, $\text{or}(W, W) = \text{or}(W, F) = \text{or}(F, W) = W$,

- Implikation $\to$ seq:

$$\text{seq}(W,F)=F,\ \text{seq}(W,W)=\text{seq}(F,W)=\text{seq}(F,F)=W,$$

- Äquivalenz $\to$ äq: äq$(W,W)=$ äq$(F,F)=W$, äq$(W,F)=$ äq$(F,W)=F$.

Sehr gebräuchlich zur Darstellung von Wahrheitsfunktionen sind **Wahrheitstafeln**, die wir bereits als Operationstafeln in der Algebra kennengelernt haben:

A	not A
W	F
F	W

,

A	B	and(A,B)
W	W	W
W	F	F
F	W	F
F	F	F

,

A	B	or(A,B)
W	W	W
W	F	W
F	W	W
F	F	F

,

A	B	seq(A,B)
W	W	W
W	F	F
F	W	W
F	F	W

,

A	B	äq(A,B)
W	W	W
W	F	F
F	W	F
F	F	W

.

Entsprechend ist der Superposition von Aussagenfunktionen eine Superposition von Wahrheitsfunktionen zugeordnet, z. B. entspricht der Aussage

- (Wenn A, so B) genau dann, wenn (wenn nicht B, so nicht A)

die Wahrheitsfunktion

- äq(seq(A,B),seq(not B,not A)).

Zu jeder natürlichen Zahl n gibt es genau 2^n n-Tupel von Wahrheitwerten; jedem n-Tupel kann man W oder F zuordnen; damit gibt es genau 2^{2^n} n-stellige Wahrheitsfunktionen, die wir mit Φ_k^n $(1 \leqq k \leqq 2^{2^n})$ bezeichnen. Bei einer lexikographischen Ordnung stellen wir stets W vor F, so dass damit die Wahrheitsfunktionen geordnet sind.

1.2. Ausdrücke

Um Aussagen einer mathematischen Untersuchung zugänglich zu machen, ist eine strenge formale Definition des Begriffes Aussage als mathematisches Objekt nötig. Zur formalen Darstellung von Ausdrücken benutzen wir folgende Grundzeichen (atomare Zeichen):

- das Zeichen $\neg$, das wir einstelligen Funktor nennen,
- die Zeichen $\wedge, \vee, \rightarrow, \leftrightarrow$, die wir zweistellige Funktoren nennen,
- die technischen Zeichen (,),
- eine Menge var von Zeichen, die durch $p, q, r, s, t, \ldots$ (eventuell mit Indices) repräsentiert sind und Variable genannt werden.

Anstelle des Wortes Funktor findet man oft auch die Bezeichnung Junktor. Die Menge aller Grundzeichen nennt man **Alphabet**. Sie besteht bis auf die technischen Zeichen aus der Menge fun aller Funktoren und der Menge var aller Variablen. Eine Variable nennt man auch **Aussagenvariable, Wahrheitsvariable, boolesche Variable**. Die Bezeichnung der Zeichen ergibt sich aus ihrer späteren Verwendung. Eine beliebige Aneinanderreihung von Zeichen der obigen Art nennen wir ein Wort. Anstelle von Funktor findet man auch die Bezeichnung Junktor. Bei gegebenem Wort w bezeichnen wir mit $\mathsf{var}(w)$ die Menge aller im Wort w vorkommenden Variablen und mit $\mathsf{fun}(w)$ die Menge aller in w vorkommenden Funktoren. Die meisten der durch Aneinanderreihung erzeugten Wörter werden uns „sinnlos“ erscheinen. Aus ihnen haben wir mittels einer geeigneten Definition solche Ausdrücke zu selektieren, von denen wir im weiteren Fortgang der Untersuchungen erkennen werden, dass sie als Hilfsmittel zur formalen Wiedergabe von Sachverhalten dienen können. Mit einer induktiven Definition sagen wir nun, wann ein Wort ein **Ausdruck** sein soll:

1. Atomare Ausdrücke: Jede Variable ist ein Ausdruck.
2. Abgeleitete Ausdrücke: Sind A, B Ausdrücke, so sind die folgenden Wörter Ausdrücke:

   $$\neg A,\ (A \wedge B),\ (A \vee B),\ (A \rightarrow B),\ (A \leftrightarrow B).$$

3. Ein Wort A ist genau dann ein Ausdruck, wenn es eine natürliche Zahl n gibt, so dass man das Wort durch n-malige Anwendung von 2. aus den Variablen gewinnen kann.

Mittels dieser induktiven Definition kann man in endlich vielen Schritten von jedem aus den Grundzeichen aufgebauten Wort entscheiden, ob es ein Ausdruck ist oder nicht. Die Anzahl solcher Schritte nennt man **Ausdrucksstufe**.Es sei etwa das Wort

$$((p \wedge q) \rightarrow r) \rightarrow ((p \rightarrow (q \rightarrow r)))$$

gegeben. In der folgenden Tabelle geben wir an, auf welche Arten das Wort in die Form $(A \rightarrow B)$ bzw. $(A \wedge B)$ aufgespalten werden kann:

	(	A		B	)
1	(	$(p$	$\wedge$	$q) \to r) \to ((p \to (q \to r))$	)
2	(	$(p \wedge q)$	$\to$	$r) \to ((p \to (q \to (q \to r))$	)
3	(	$(p \wedge q) \to r)$	$\to$	$((p \to (q \to r))$	)
4	(	$(p \wedge q) \to r) \to ((p$	$\to$	$(q \to r))$	)
5	(	$(p \wedge q) \to r) \to ((p \to (q$	$\to$	$r))$	)

Wir haben zu untersuchen, in welchen Fällen A oder B kein Ausdruck ist. Man sieht leicht, dass im Falle 1 A kein Ausdruck ist; in den anderen Fällen stellt man durch Aufspalten von B fest, dass B kein Ausdruck ist. Dagegen ist

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

ein Ausdruck. Für das automatische Identifizieren von Ausdrücken ist es besser, über eine explizite Charakterisierung von Ausdrücken zu verfügen. Eine solche ist die folgende.

1.1. Satz: *Ein Wort A ist genau dann ein Ausdruck, wenn die folgenden Bedingungen simultan erfüllt sind:*

1. *Das Wort A beginnt mit einer Variablen oder mit $\neg$ oder mit $($.*
2. *Auf eine Variable oder $)$ folgt in A nichts, oder $)$ oder ein zweistelliger Funktor.*
3. *Auf $($ oder einen Funktor folgt in A eine Variable oder $\neg$ oder $($.*
4. *Die Häufigkeiten des Auftretens von zweistelligen Funktoren in A, von $($ und von $)$ stimmen überein.*
5. *An jeder Stelle in A, an der $($ steht gilt: Es beginnt ein Teilwort B, in dem die Häufigkeit des Auftretens von $($ gleich der Häufigkeit des Auftretens von $)$ ist, und in dem kürzestens derartigen Teilwort B ist dies gleich der Häufigkeit des Auftretens von zweistelligen Funktoren.*

Mit dieser expliziten Charakterisierung eines Ausdrucks entscheidet man sofort, dass das obige Wort kein Ausdruck ist. Zur Einsparung von Klammern vereinbaren wir, dass beim Aufschreiben von Ausdrücken die Außenklammern weggelassen werden dürfen; außerdem soll folgende Trennungsreihenfolge gelten: $\leftrightarrow, \to, \vee, \wedge$. Im Interesse einer besseren Lesbarkeit verwenden wir beim Notieren von Ausdrücken anstelle der runden Klammern auch eckige und geschweifte. Hiernach können wir den letzten Ausdruck auch in der Form

$$(p \wedge q \to r) \to [p \to (q \to r)]$$

schreiben.
Für die Auswertung von Ausdrücken auf dem Rechner ist es sicherlich zweckmäßig,

eine klammerfreie Schreibweise von Ausdrücken zu verwenden. Hier darf man zwischen einer Präfix- und einer Postfixnotation wählen. Als Grundzeichen werden neben den Variablen nur noch Zeichen F_k^n für n-stellige Funktoren benötigt. In dieser Schreibweise lautet die induktive Definition von Ausdrücken in der Präfixnotation folgendermaßen.

1. Jede Variable ist ein Ausdruck.

2. Sind $A_1, \ldots, A_m$ Ausdrücke und ist F_k^m ein m-stelliger Funktor, so ist auch $F_k^m A_1 \ldots A_m$ ein Ausdruck.

3. Zu jedem Ausdruck A gibt es eine natürliche Zahl n derart, dass man ihn durch n-malige Anwendung von 2. aus den Variablen gewinnen kann.

Wir bezeichnen etwa die obigen Funktoren mit N, K, A, C, E. Dann schreibt sich z. B. der Ausdruck $\neg(\neg p \wedge \neg q) \leftrightarrow p \vee q$ in der Form $ENKNpNqApq$. Ohne Beweis bemerken wir noch, dass sich bei dieser Schreibweise leicht entscheiden lässt, ob ein Ausdruck vorliegt. Dazu ordnet man einem aus Variablen und Funktoren aufgebauten Wort eine endliche Zahlenfolge zu: Jeder Variablen wird die Zahl 1 und jedem n-stelligen Funktor die Zahl $1-n$ zugeordnet. Sodann bilde man von rechts nach links zu dieser Zahlenfolge die zugehörige Partialsummenfolge. Man kann zeigen, dass ein gegebenes Wort genau dann ein Ausdruck ist, wenn die zugordnete endliche Partialsummenfolge mit der Zahl 1 beginnt und nur positive Zahlen enthält.
Es sei im folgenden $\mathscr{L}$ die Menge aller Ausdrücke. Eine Abbildung α, die jeder Variablen genau einen Wahrheitswert W oder F zuordnet, heißt **Belegung** der Variablen mit Wahrheitswerten. Bei einer Belegung wird also stets allen Variablen ein Wahrheitswert zugeordnet, unabhängig davon, ob sie in einem Ausdruck vorkommen oder nicht. Bei gegebener Belegung α können wir jedem Ausdruck $A \in \mathscr{L}$ einen **Wahrheitswert** $\text{ww}(A, \alpha)$ zuordnen; dieser wird induktiv definiert:

1. Atomare Wahrheitswerte: Für jede Variable p gilt: $\text{ww}(p, \alpha) = \alpha(p)$.

2. Abgeleitete Wahrheitswerte: Sind A, B Ausdrücke, so ist

$$\begin{aligned}
\text{ww}(\neg A, \alpha) &= \text{not ww}(A, \alpha), \\
\text{ww}(A \wedge B, \alpha) &= \text{and}(\text{ww}(A, \alpha), \text{ww}(B, \alpha)), \\
\text{ww}(A \vee B, \alpha) &= \text{or}(\text{ww}(A, \alpha), \text{ww}(B, \alpha)), \\
\text{ww}(A \rightarrow B, \alpha) &= \text{seq}(\text{ww}(A, \alpha), \text{ww}(B, \alpha)), \\
\text{ww}(A \leftrightarrow B, \alpha) &= \text{äq}(\text{ww}(A, \alpha), \text{ww}(B, \alpha)).
\end{aligned}$$

Für jeden Ausdruck kann der Wert nach dieser Definition in endlich vielen Schritten berechnet werden; er hängt nur von den Werten jener Variablen ab, die im Ausdruck wirklich vorkommen. Es gilt das

1.2. Koinzidenzlemma der Aussagenlogik: *Für jeden Ausdruck A und je zwei Belegungen α_1, α_2 mit $\alpha_1(p) = \alpha_2(p)$ für alle $p \in \mathsf{var}(A)$ gilt* $\mathsf{ww}(A, \alpha_1) = \mathsf{ww}(A, \alpha_2)$.

Über $\mathrm{ww}(A, \alpha)$ entspricht jedem Ausdruck A eine Superposition von klassischen Wahrheitsfunktionen und umgekehrt. So gilt z. B.

$$\mathrm{ww}(p \to q \leftrightarrow \neg q \to \neg p, \alpha) = \text{äq}(\text{seq}(\alpha(p), \alpha(q)), \text{seq}(\text{not}\alpha(q), \text{not}\alpha(p))).$$

Das gibt uns das Recht, den einstelligen Funktor $\neg$ als Negation, den Funktor $\wedge$ als Konjunktion, den Funktor $\vee$ als Alternative (Disjunktion), $\to$ als Implikation und $\leftrightarrow$ als Äquivalenz zu bezeichnen. Wir werden diese Bezeichnungen auch für solche Ausdrücke verwenden, die ausschließlich den entsprechenden Funktor enthalten. Wir nennen einen Ausdruck A **erfüllbar** , wenn es eine Belegung α mit $\mathrm{ww}(A, \alpha) = W$ gibt und sagen: α erfüllt A. Mit $\mathsf{erf}(\mathscr{L}, \alpha)$ bzw. $\mathsf{erf}(\alpha)$ bezeichnen wir die Menge aller Ausdrücke, die durch die Belegung α erfüllt werden. Durch Rückgang auf die Definition erhält man z. B.

$$\neg A \in \mathsf{erf}(\alpha) \iff A \notin \mathsf{erf}(\alpha)$$

$$(A \wedge B) \in \mathsf{erf}(\alpha) \iff A \in \mathsf{erf}(\alpha) \text{ und } B \in \mathsf{erf}(\alpha),$$
$$(A \vee B) \in \mathsf{erf}(\alpha) \iff A \in \mathsf{erf}(\alpha) \text{ oder } B \in \mathsf{erf}(\alpha),$$
$$(A \to B) \in \mathsf{erf}(\alpha) \iff \text{aus } A \in \mathsf{erf}(\alpha) \text{ folgt } B \in \mathsf{erf}(\alpha),$$
$$(A \leftrightarrow B) \in \mathsf{erf}(\alpha) \iff A \in \mathsf{erf}(\alpha) \text{ genau dann, wenn } B \in \mathsf{erf}(\alpha).$$

Mit $\mathsf{erf}(\mathscr{L})$ bezeichnen wir die Menge aller erfüllbaren Ausdrücke, d. h. die Vereinigung aller Mengen $\mathsf{erf}(\mathscr{L}, \alpha)$. In $\mathsf{erf}(\mathscr{L})$ gibt es eine wichtige Teilmenge, nämlich die Menge aller jener Ausdrücke, die von jeder Belegung erfüllt werden. Diese Ausdrücke nennt man allgemeingültig. Genau: Ein Ausdruck A heißt **allgemeingültig**, wenn bei jeder Belegung α gilt:

$$\mathrm{ww}(A, \alpha) = W.$$

Mit $\mathsf{ag}(\mathscr{L})$ bezeichnen wir die Menge aller allgemeingültigen Ausdrücke. Daneben gibt es noch unerfüllbare und neutrale Ausdrücke. Ein Ausdruck A heißt **unerfüllbar**, wenn bei jeder Belegung α gilt

$$\mathrm{ww}(A, \alpha) = F.$$

Es sei $\mathsf{uf}(\mathscr{L})$ die Menge aller unerfüllbaren Ausdrücke. Schließlich nennen wir einen Ausdruck A **neutral**, wenn zwei Belegungen α_1, α_2 existieren mit

$$\mathrm{ww}(A, \alpha_1) = W, \quad \mathrm{ww}(A, \alpha_2) = F.$$

Entsprechend sei $\mathsf{nt}(\mathscr{L})$ die Menge aller neutralen Ausdrücke. Wenn aus dem Zusammenhang klar ist, welche Ausdrucksmenge $\mathscr{L}$ der Untersuchung zugrunde liegt, lassen wir sie bei diesen Teilmengen weg. Offenbar ist jeder allgemeingültige Ausdruck auch erfüllbar: $\mathsf{ag} \subset \mathsf{erf}$. Auch jeder neutrale Ausdruck ist erfüllbar: $\mathsf{nt} \subset \mathsf{erf}$. Die Menge der erfüllbaren Ausdrücke zerfällt in zwei elementfremde Teilmengen, die allgemeingültigen und die neutralen Ausdrücke:

$$\mathsf{erf} = \mathsf{ag} \cup \mathsf{nt}, \quad \mathsf{ag} \cap \mathsf{nt} = \emptyset.$$

Ein Ausdruck A ist genau dann allgemeingültig, wenn $\neg A$ unerfüllbar ist:

$$\mathsf{uf} = \{\, A \in \mathscr{L} \mid \neg A \in \mathsf{ag} \,\}, \quad \mathsf{ag} = \{\, A \in \mathscr{L} \mid \neg A \in \mathsf{uf} \,\}$$

oder einfach

$$\mathsf{ag} = \neg \mathsf{uf}.$$

Ein Ausdruck A ist genau dann erfüllbar, wenn der Ausdruck $\neg A$ nicht allgemeingültig ist:

$$\mathsf{erf} = \{\, A \in \mathscr{L} \mid \neg A \notin \mathsf{ag} \,\}$$

oder

$$\mathsf{erf} = \neg\, (\mathscr{L} \setminus \mathsf{ag})\,.$$

1.3. Satz: *Für allgemeingültige bzw. erfüllbare Ausdrücke gelten die folgenden Beziehungen.*

1. $(A \wedge B) \in \mathsf{ag} \Longleftrightarrow A \in \mathsf{ag}$ *und* $B \in \mathsf{ag}$.
2. *Wenn* $A \in \mathsf{ag}$ *oder* $B \in \mathsf{ag}$, *so ist* $(A \vee B) \in \mathsf{ag}$.
3. *Wenn* $(A \rightarrow B) \in \mathsf{ag}$, *so gilt: Aus* $A \in \mathsf{ag}$, *folgt* $B \in \mathsf{ag}$.
4. *Wenn* $(A \leftrightarrow B) \in \mathsf{ag}$, *so folgt:* $A \in \mathsf{ag} \Longleftrightarrow B \in \mathsf{ag}$.
5. *Aus* $(A \wedge B) \in \mathsf{erf}$ *folgt* $A \in \mathsf{erf}$ *und* $B \in \mathsf{erf}$.
6. $(A \vee B) \in \mathsf{erf}$ *genau dann, wenn* $A \in \mathsf{erf}$ *oder* $B \in \mathsf{erf}$.

Beweis: Sämtliche Eigenschaften zeigt man durch Rückgang auf die Definition. Beispielhaft wählen wir die 3. Eigenschaft aus. Es sei $(A \rightarrow B) \in \mathsf{ag}, A \in \mathsf{ag}$. Nehmen wir an, dass $B \notin \mathsf{ag}$ gilt. Dann gibt es eine Belegung α mit $\mathrm{ww}(B,\alpha) = F$. Wegen $\mathrm{ww}(A,\alpha) = W$ folgt damit aus der Wertetabelle für die Implikation, dass $\mathrm{ww}(A \rightarrow B),\alpha) = F$ sein muss, was der Voraussetzung widerspricht. In analoger

Weise verifiziert man die anderen Beziehungen. ♣

Die dritte Eigenschaft hat eine besondere Bedeutung: Man nennt sie **Abtrennungsregel**, weil sie formal gesprochen wie folgt interpretiert werden kann: Aus einem als allgemeingültig erkannten Ausdruck der Form $(A \to B)$ kann man den Ausdruck A abtrennen, falls dieser allgemeingültig ist und erhält so den allgemeingültigen Ausdruck B:

$$(A \to B) \in \mathsf{ag}, A \in \mathsf{ag} \quad \Longrightarrow \quad B \in \mathsf{ag}.$$

Ein wichtiges Mittel zur Produktion neuer Ausdrücke ist die **Einsetzungsregel**: Es seien A, B Ausdrücke und $p \in \mathsf{var}(A)$. Wir sagen, dass der Ausdruck A' durch Einsetzung von B anstelle von p aus dem Ausdruck A entsteht, wenn A' gleich jenem Ausdruck ist, den man dadurch erhält, dass man die Variable p an allen Stellen ihres Auftretens im Ausdruck A durch den Ausdruck B ersetzt, in Zeichen: $A' = A(p|B)$.

1.4. Satz: *Bei der Einsetzungsregel ist die Allgemeingültigkeit erblich:*
Wenn $A \in \mathsf{ag}$ *und* $B \in \mathscr{L}$*, so gilt* $A(p|B) \in \mathsf{ag}$.

Beweis: Es sei α eine beliebige Belegung der Variablen, A und B seien Ausdrücke, p eine in A vorkommende Variable. Wir konstruieren aus α eine neue Belegung α'; sie soll die Variable p mit $\mathrm{ww}(B, \alpha)$ belegen und alle übrigen Variablen in gleicher Weise wie α. Dann gilt offenbar

$$\mathrm{ww}(A(p|B), \alpha) = \mathrm{ww}(A, \alpha').$$

Nun ist aber A allgemeingültig, woraus $\mathrm{ww}(A, \alpha') = W$ folgt, also

$$\mathrm{ww}(A(p|B), \alpha) = W.$$

Da α eine beliebige Belegung war, folgt $A(p|B) \in \mathsf{ag}$. ♣

Natürlich kann man die Einsetzungsregel mehrfach oder simultan anwenden. Alle entstehenden Ausdrücke sind allgemeingültig, sofern nur der erste es war.

1.3. Allgemeingültige Ausdrücke

Die im letzten Abschnitt definierte Menge $\mathscr{L}$ aller Ausdrücke ist innerhalb der Aussagenlogik das abstrakte Analogon für die Menge aller Aussagen einer Theorie. Um dieses glaubwürdig zu untermauern, wollen wir zeigen, dass wichtige Beziehungen zwischen Aussagen sich in abstrakten Relationen zwischen Ausdrücken wiederfinden. In der Mathematik und anderen Wissenschaften verwendete Aussagen und

Schlussweisen haben ihre Widerspiegelung in Eigenschaften und Relationen zwischen Ausdrücken. So entspricht dem Satz „Jede Aussage ist entweder wahr oder falsch“ die Tatsache, dass der Ausdruck $p \vee \neg p$ allgemeingültig ist:

$$(p \vee \neg p) \in \mathsf{ag}(\mathscr{L}).$$

Wegen der Einsetzungsregel kann man für die Variable p jeden Ausdruck A einsetzen und erhält, dass der Ausdruck $A \vee \neg A$ allgemeingültig ist. Das Prinzip vom ausgeschlossenen Widerspruch ist durch den allgemeingültigen Ausdruck $\neg(p \wedge \neg p)$ repräsentiert.
Eine erste, sehr bekannte Beziehung zwischen Aussagen ist die Tatsache, dass man mit verschiedenen Aussagen das gleiche meinen kann; man sagt, die entsprechenden Aussagen sind semantisch äquivalent. Die semantische Äquivalenz können wir in der Aussagenlogik leicht modellieren: Wir sagen, dass zwei Ausdrücke A und B **semantisch äquivalent** sind (in Zeichen $A \cong B$), wenn der Ausdruck $A \leftrightarrow B$ allgemeingültig ist:

$$A \cong B \quad \Longleftrightarrow \quad (A \leftrightarrow B) \in \mathsf{ag},$$

d. h. wenn für jede Belegung α gilt:

$$\mathrm{ww}(A, \alpha) = \mathrm{ww}(B, \alpha).$$

Man sieht, dass die semantische Äquivalenz eine Äquivalenzrelation ist. Zwei allgemeingültige Ausdrücke sind sicher semantisch äquivalent, ebenso zwei unerfüllbare:

$$A, B \in \mathsf{ag} \quad \Longrightarrow \quad A \cong B,$$

$$A, B \in \mathsf{uf} \quad \Longrightarrow \quad A \cong B.$$

Umgekehrt kann zu einem allgemeingültigen Ausdruck nur ein allgemeingültiger semantisch äquivalent sein; entsprechendes gilt bei einem unerfüllbaren:

$$A \in \mathsf{ag}, A \cong B \quad \Longrightarrow \quad B \in \mathsf{ag},$$

$$A \in \mathsf{uf}, A \cong B \quad \Longrightarrow \quad B \in \mathsf{uf}.$$

Möglichkeiten, semantisch äquivalente Ausdrücke zu produzieren, erschließen sich insbesondere dadurch, dass man untersucht, wie sich die semantische Äquivalenz und die Funktoren vertragen.

1.5. Satz: *Zwischen der semantischen Äquivalenz und den Funktoren gelten folgende Beziehungen:*

1. *Die Funktoren* $\wedge, \vee, \leftrightarrow$ *sind hinsichtlich der semantischen Äquivalenz kommutativ und assoziativ, d. h. z. B. :*

   $$p \wedge q \cong q \wedge p, \quad p \wedge (q \wedge r) \cong (p \wedge q) \wedge r.$$

2. *Die Funktoren* $\wedge, \vee$ *sind idempotent:*

   $$p \wedge p \cong p, \quad p \vee p \cong p.$$

3. *Es gelten die de Morganschen Regeln bzgl. der Funktoren* $\neg, \wedge, \vee$*:*

   $$\neg(p \wedge q) \cong \neg p \vee \neg q, \quad \neg(p \vee q) \cong \neg p \wedge \neg q.$$

4. *Die Funktoren* $\wedge, \vee$ *sind gegeneinander distributiv:*

   $$p \wedge (q \vee r) \cong (p \wedge q) \vee (p \wedge r),$$

   $$p \vee (q \wedge r) \cong (p \vee q) \wedge (p \vee r).$$

5. *Der Funktor* $\rightarrow$ *ist rechtsdistributiv bzgl. aller zweistelligen Funktoren, z. B.*

   $$p \rightarrow (q \wedge r) \cong (p \rightarrow q) \wedge (p \rightarrow r).$$

6. *Es gilt die* **Prämissenverschmelzung***:*

   $$p \rightarrow (p \rightarrow q) \cong p \rightarrow q.$$

7. *Es gilt die* **Prämissenvertauschung***:*

   $$p \rightarrow (q \rightarrow r) \cong q \rightarrow (p \rightarrow r).$$

8. *Es gilt die* **Prämissenverbindung***:*

   $$p \rightarrow (q \rightarrow r) \cong (p \wedge q) \rightarrow r.$$

9. *Jede Implikation* $A \rightarrow B$*, in der* A *eine Konjunktion ist, kann als Alternative von Implikationen dargestellt werden:*

   $$p \wedge q \rightarrow r \cong (p \rightarrow r) \vee (q \rightarrow r).$$

10. *Jede Implikation* $A \rightarrow B$*, in der* A *eine Alternative ist, kann als Konjunktion von Implikationen dargestellt werden:*

    $$p \vee q \rightarrow r \cong (p \rightarrow r) \wedge (q \rightarrow r).$$

11. *Die doppelte Verneinung eines Ausdrucks ist zum Ausdruck semantisch äquivalent:*

$$\neg\neg p \cong p.$$

Die Beweise dieser Aussagen erhält man durch Aufstellen der entsprechenden Wahrheitstafeln.
Ein wichtiger Beweistrick in der Mathematik ist die **Kontraposition** (der indirekte Beweis): Um eine Implikation zu beweisen, nimmt man an, dass die Behauptung falsch ist und schließt daraus, dass mindestens eine der Voraussetzungen nicht erfüllt sein kann. Dieses Prinzip widerspiegelt sich in

$$p \to q \cong \neg q \to \neg p.$$

Außerdem gilt:

$$p \wedge q \cong \neg(p \to \neg q),$$

$$p \vee q \cong \neg p \to q \cong (p \to q) \to q,$$

$$p \leftrightarrow q \cong (p \to q) \wedge (q \to p) \cong \neg[(p \to q) \to \neg(q \to p)].$$

Hiermit ist gezeigt, dass sich alle Standardfunktoren mittels $\neg$ und $\to$ äquivalent ausdrücken lassen. Durch Rückgang auf die Wahrheitsfunktionen folgt: Durch die Wahrheitsfunktionen not und seq können alle Standardwahrheitsfunktionen ausgedrückt werden. Andererseits sind die Standardfunktoren auch durch $\neg$ und $\wedge$, aber auch durch $\neg$ und $\vee$ semantisch äquivalent ausdrückbar. Dazu braucht man nur zu zeigen, dass $\to$ sowohl durch $\neg$ und $\wedge$ als auch durch $\neg$ und $\vee$ ausdrückbar ist:

$$\neg(p \wedge \neg q) \cong p \to q \cong \neg p \vee q.$$

Aus diesen Überlegungen folgt insbesondere, dass wir die Funktorenmenge unserer Sprache z. B. auf die beiden Funktoren $\neg$ und $\wedge$ reduzieren dürfen, ohne die Aussagekraft der Sprache zu ändern.
Zu jedem Ausdruck darf man einen allgemeingültigen konjunktiv hinzufügen und einen unerfüllbaren alternativ, denn

$$A \in \mathsf{ag} \quad \Longrightarrow \quad A \wedge B \cong B,$$

$$A \in \mathsf{uf} \quad \Longrightarrow \quad A \vee B \cong B.$$

Die Äquivalenzen dürfen wir auch von rechts nach links lesen: In einer Konjunktion darf man einen allgemeingültigen Ausdruck semantisch äquivalent weglassen. In einer Alternative darf man einen unerfüllbaren Ausdruck semantisch äquivalent

streichen.
Jede semantische Äquivalenz für eine Implikation der Form $A \to B$ liefert zwei allgemeingültige Implikationen, denn aus $A \cong B$ folgt, dass $(A \leftrightarrow B) \in \mathsf{ag}$, was $(A \to B) \in \mathsf{ag}$ und $(B \to A) \in \mathsf{ag}$ nach sich zieht. Aus jeder allgemeingültigen Implikation folgt eine Schlussregel. Ist nämlich der Ausdruck $A \to B$ allgemeingültig, so gilt wegen der Abtrennungsregel für allgemeingültige Ausdrücke: Wenn $A \in \mathsf{ag}$, so $B \in \mathsf{ag}$. Wir geben einige allgemeingültige Implikationen und ihre entsprechenden Schlussregeln an.

1. **Selbstimplikation**: $p \to p \in \mathsf{ag}$.
2. **Prämissenbelastung**: $p \to (q \to p) \in \mathsf{ag}$.
   Schlussregel:
   $$A \in \mathsf{ag} \quad \Longrightarrow \quad B \to A \in \mathsf{ag}.$$
3. **Prämissenverschmelzung**: $(p \to (p \to q)) \to (p \to q) \in \mathsf{ag}$.
   Schlussregel:
   $$A \to (A \to B) \in \mathsf{ag} \quad \Longrightarrow \quad A \to B \in \mathsf{ag}.$$
4. **Prämissenvertauschung**: $[p \to (q \to r)] \to [q \to (p \to r)] \in \mathsf{ag}$.
   Schlussregel:
   $$A \to (B \to C) \in \mathsf{ag} \quad \Longrightarrow \quad B \to (A \to C) \in \mathsf{ag}.$$
5. **Abtrennung**: $p \to [(p \to q) \to q] \in \mathsf{ag}$.
   Schlussregeln:
   $$\begin{aligned} A \in \mathsf{ag} &\Longrightarrow (A \to B) \to B \in \mathsf{ag}, \\ A, A \to B \in \mathsf{ag} &\Longrightarrow B \in \mathsf{ag}. \end{aligned}$$
6. **Gewöhnlicher Kettenschluss**: $(p \to q) \to [(q \to r) \to (p \to r)] \in \mathsf{ag}$.
   Schlussregeln:
   $$\begin{aligned} A \to B \in \mathsf{ag} &\Longrightarrow (B \to C) \to (A \to C) \in \mathsf{ag}, \\ A \to B, B \to C \in \mathsf{ag} &\Longrightarrow A \to C \in \mathsf{ag}, \\ A \to B, B \to C, A \in \mathsf{ag} &\Longrightarrow C \in \mathsf{ag}. \end{aligned}$$
7. **Schließen aus einer Konjunktion**: $p \wedge q \to p \in \mathsf{ag}$.
   Schlussregel:
   $$A \wedge B \in \mathsf{ag} \quad \Longrightarrow \quad A \in \mathsf{ag}.$$

8. **Schließen auf eine Konjunktion**: $(p \to q) \to [(p \to r) \to (p \to q \wedge r)] \in \mathsf{ag}$. Schlussregel:

$$A \to B, A \to C, A \in \mathsf{ag} \quad \Longrightarrow \quad B \wedge C \in \mathsf{ag}.$$

1.4. Aussagenlogische Normalformen

Es sei var_n eine Menge von n Variablen:

$$\mathsf{var}_n = \{ p_1, \ldots, p_n \} .$$

Eine **Elementarkonjunktion** K ist ein Ausdruck der Form

$$A_1 \wedge A_2 \wedge \ldots \wedge A_n$$

mit $A_i = p_i$ oder $A_i = \neg p_i$. Eine Elementarkonjunktion über n Variable ist demnach ein konjunktiver Ausdruck, in dem jede Variable genau einmal entweder selbst oder negiert vorkommt. Im Falle $n = 3$ gibt es die folgenden 8 Elementarkonjunktionen über p, q, r:

$$K_1(p,q,r) = (p \wedge q \wedge r), \quad K_2(p,q,r) = (p \wedge q \wedge \neg r),$$

$$K_3(p,q,r) = (p \wedge \neg q \wedge r), \quad K_4(p,q,r) = (p \wedge \neg q \wedge \neg r),$$
$$K_5(p,q,r) = (\neg p \wedge q \wedge r), \quad K_6(p,q,r) = (\neg p \wedge q \wedge \neg r),$$
$$K_7(p,q,r) = (\neg p \wedge \neg q \wedge r), \quad K_8(p,q,r) = (\neg p \wedge \neg q \wedge \neg r).$$

Insbesondere gibt es genau 2^n verschiedene Elementarkonjunktionen. Eine Elementarkonjunktion ist genau dann wahr, wenn jede negiert auftretende Variable mit F und alle anderen mit W belegt sind. Folglich gibt es zu jeder gegebenen Belegung α der Variablen aus var_n genau eine Elementarkonjunktion, die bei der Belegung α den Wert W annimmt. Diese kann man sofort angeben: Im Falle $\alpha(p_i) = W$ wird die Variable selbst und im Falle $\alpha(p_i) = F$ wird die negierte Variable in die Elementarkonjunktion aufgenommen. Umgekehrt gibt es zu jeder Elementarkonjunktion K genau eine Belegung α der Variablen aus var_n, so dass K den Wert W hat und alle anderen den Wert F. Dazu wird jede in K negiert vorkommende Variable mit F und jede andere mit W belegt. Jene Elementarkonjunktion, die bei gegebener Belegung α den Wert W annimmt, heißt **verifizierte Elementarkonjunktion**. Da es zu jeder Belegung α genau eine durch α verifizierte Elementarkonjunktion gibt, ist die Alternative über alle 2^n Elementarkonjunktionen allgemeingültig; die Konjunktion über zwei verschiedene Elementarkonjunktionen ist unerfüllbar. Somit repräsentieren die Elementarkonjunktionen über var_n alle möglichen Belegungen dieser Variablen.

Dual zur Elementarkonjunktion definieren wir zu var_n eine **Elementaralternative** als alternativen Ausdruck, in dem jede Variable genau einmal entweder selbst oder negiert auftritt. Eine Elementaralternative hat genau dann den Wert F, wenn jede negiert auftretende Variable mit dem Wert W und alle anderen mit dem Wert F belegt sind. Bei gegebener Belegung α nimmt genau eine Elementaralternative den Wert F an. Man nennt diese die durch α **falsifizierte Elementaralternative**; es ist gerade jene Elementaralternative $A_1 \vee \ldots \vee A_n$ mit $A_i = p_i$, falls $\alpha(p_i) = F$ und $A_i = \neg p_i$, falls $\alpha(p_i) = W$. Umgekehrt gibt es zu jeder Elementaralternative A über var_n genau eine Belegung α mit $\mathrm{ww}(A, \alpha) = F$. Somit ist die konjunktive Verknüpfung aller 2^n Elementaralternativen über var_n unerfüllbar; die alternative Verknüpfung von je zwei verschiedenen Elementaralternativen ist stets allgemeingültig. Es sei nun $\bigwedge(\mathsf{var}_n)$ die Menge aller Elementarkonjunktionen über var_n und entsprechend $\bigvee(\mathsf{var}_n)$ die Menge aller Elementaralternativen. Als **alternative Normalform** bezeichnet man die alternative Verknüpfung von beliebigen, verschiedenen Elementarkonjunktionen über var_n. Zur formalen Abschließung nehmen wir als alternative Normalform noch den unerfüllbaren Ausdruck

$$(p_1 \wedge \neg p_1) \vee \ldots \vee (p_n \wedge \neg p_n)$$

hinzu. Indem wir alle Elementarkonjunktionen durchnummerieren, hat eine alternative Normalform die Form

$$K_{l_1}(\mathsf{var}_n) \vee \ldots \vee K_{l_r}(\mathsf{var}_n)$$

mit $1 \leqq l_1 < \ldots < l_r \leqq 2^n$. Analog verstehen wir unter einer **konjunktiven Normalform** die konjunktive Verknüpfung aller Elemente einer beliebigen Teilmenge von $\bigvee(\mathsf{var}_n)$, wobei wir zur formalen Abschließung als konjunktive Normalform noch den allgemeingültigen Ausdruck

$$(p_1 \vee \neg p_1) \wedge \ldots \wedge (p_n \vee \neg p_n)$$

hinzunehmen. Damit hat eine konjunktive Normalform die Gestalt

$$A_{l_1}(\mathsf{var}_n) \wedge \ldots \wedge A_{l_r}(\mathsf{var}_n)$$

mit $1 \leqq l_1 < \ldots < l_r \leqq 2^n$, wobei die gleiche Nummerierung wie bei den Elementarkonjunktionen verwendet wurde. Da jeder Teilmenge von $\bigvee(\mathsf{var}_n)$ genau eine konjunktive Normalform entspricht, gibt es genau 2^{2^n} konjunktive und auch 2^{2^n} alternative Normalformen über var_n.

1.6. Repräsentantensatz für alternative Normalformen: *Jede n-stellige Wahrheitsfunktion wird durch genau eine alternative Normalform repräsentiert.*

Beweis: Es gibt gleichviel n-stellige Wahrheitsfunktionen und alternative Normalformen über var_n. Daher genügt es zu zeigen, dass nicht zwei verschiedene alternative Normalformen N_1, N_2 die gleiche Wahrheitsfunktion repräsentieren. Es sei also $K(\mathsf{var}_n)$ eine Elementarkonjunktion aus N_1, die nicht in N_2 vorkommt. Es gibt eine Belegung α, durch die K verifiziert wird; daraus ergibt sich

$$\mathrm{ww}(N_1, \alpha) = W.$$

Nun erteilt aber α jeder anderen Elementarkonjunktion den Wert F, also muss

$$\mathrm{ww}(N_2, \alpha) = F$$

sein. ♣

Wir wollen nun die eine Wahrheitsfunktion repräsentierende alternative Normalform ermitteln. Offenbar nimmt eine alternative Normalform N über var_n genau dann bei einer gewissen Belegung α den Wert W an, wenn α verifizierende Belegung einer in N vorkommenden Elementarkonjunktion ist. Die durch N repräsentierte Wahrheitsfunktion ordnet also genau jenen n-Tupeln $(w_1, \ldots, w_n)$ von Wahrheitswerten den Wert W zu, für die die durch $\alpha(p_i) = w_i,\ i = 1, \ldots, n$ definierte Belegung verifizierende Belegung einer Elementarkonjunktion aus N ist. Daher erhält man bei gegebener Wahrheitsfunktion Φ die sie repräsentierende alternative Normalform, indem man alle jene Elementarkonjunktionen alternativ verknüpft, deren verifizierende Belegung α die Bedingung $\Phi(\alpha(p_1), \ldots, \alpha(p_n)) = W$ erfüllt. Ist somit $\Phi(w_1, \ldots, w_n) = W$, so gehört zur alternativen Normalform die Elementarkonjunktion $A_1 \wedge \ldots \wedge A_n$ mit $A_i = p_i$, falls $w_i = W$ und $A_i = \neg p_i$, falls $w_i = F$ $(i = 1, \ldots, n)$.

Beispiele: Die 3-stellige Wahrheitsfunktion, die genau den Tripeln

$$(W,W,W), (W,F,W), (F,F,F)$$

den Wert W und den anderen den Wert F zuordnet, lautet

$$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r).$$

Die alternative Normalform

$$(\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$$

repräsentiert jene 3-stellige Wahrheitsfunktion, die den Tripeln

$$(F,W,W), (F,F,W), (F,F,F)$$

den Wert W und den übrigen 5 Tripeln den Wert F zuordnet.

Mit analogen Betrachtungen zeigt man den

1.7. Repräsentantensatz für konjunktive Normalformen: *Jede n-stellige Wahrheitsfunktion wird durch genau eine konjunktive Normalform repräsentiert.*

Die konjunktive Normalform

$$(p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r)$$

repräsentiert jene 3-stellige Wahrheitsfunktion, die den Tripeln

$$(F, F, W), (F, W, F), (W, F, W)$$

den Wert F und den übrigen den Wert W zuordnet. Die 3-stellige Wahrheitsfunktion, die den Tripeln

$$(W, W, W), (W, W, F), (W, F, F), (F, F, W)$$

den Wert F und den übrigen den Wert W zuordnet, wird durch die konjunktive Normalform

$$(\neg p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \wedge (p \vee q \vee \neg r)$$

repräsentiert.

1.8. Satz: *Jede alternative Normalform über* var_n *ist zur Negation genau einer konjunktiven Normalform über* var_n *semantisch äquivalent.*

Beweis: Die Negation einer Elementarkonjunktion ist zu genau einer Elementaralternative semantisch äquivalent:

$$\neg(A_1 \wedge A_2 \wedge \ldots \wedge A_n) \cong (\neg A_1 \vee \neg A_2 \vee \ldots \vee \neg A_n),$$

wobei doppelte Verneinungen weggelassen werden. Für eine beliebige alternative Normalform

$$K_{l_1} \vee K_{l_2} \vee \ldots \vee K_{l_r}, \quad K_{l_i} = (A_{i1} \wedge \ldots \wedge A_{in})$$

folgt:

$$\begin{aligned} K_{l_1} \vee \ldots \vee K_{l_r} &\cong \neg(\neg K_{l_1} \wedge \ldots \wedge \neg K_{l_r}) \\ &\cong \neg((\neg A_{11} \vee \ldots \vee \neg A_{1n}) \wedge \ldots \wedge (\neg A_{r1} \vee \ldots \vee \neg A_{rn})). \end{aligned}$$

Damit ist die geforderte semantische Äquivalenz hergestellt. ♣

1.9. Satz: *Jede n-stellige Wahrheitsfunktion kann mittels der Wahrheitsfunktionen not, and, or ausgedrückt werden.*

Dieser Satz ist unmittelbare Folge der Repräsentantensätze. Er rechtfertigt übrigens, dass man die Anfragen an Datenbanken meist nur mittels „nicht“, „und“, „oder“ formulieren darf.

1.10. Satz: *Zu jedem Ausdruck A mit genau n Variablen gibt es genau eine alternative und genau eine konjunktive Normalform über n Variablen, die zu A semantisch äquivalent sind.*

Beweis: Jeder Ausdruck wird durch eine n-stellige Wahrheitsfunktion repräsentiert. Aus der vollständigen Wertetafel der repräsentierenden Wahrheitsfunktion kann man unmittelbar nach den obigen Überlegungen die entsprechende alternative bzw. konjunktive Normalform aufstellen. ♣

Beispiel: Wir suchen die alternative Normalform zu dem Ausdruck

$$p \lor \neg q \lor r.$$

Die zugeordnete Wahrheitstafel lautet

p	q	r	$p \lor \neg q \lor r$
W	W	W	W
W	W	F	W
W	F	W	W
W	F	F	W
F	W	W	W
F	W	F	F
F	F	W	W
F	F	F	W

.

Daraus erhalten wir die alternative Normalform

$$\begin{aligned}&(p \land q \land r) \lor (p \land q \land \neg r) \lor (p \land \neg q \land r) \lor (p \land \neg q \land \neg r)\\ &\lor (\neg p \land q \land r) \lor (\neg p \land \neg q \land r) \lor (\neg p \land \neg q \land \neg r)\end{aligned}$$

und sehen, dass sie bedeutend länger ist als der ursprüngliche Ausdruck. Trotzdem hat dieser Satz grundlegende Bedeutung. Durch die semantisch äquivalente Überführung eines Ausdrucks in eine Normalform wird das automatische Verifizieren von Ausdrücken wesentlich erleichtert, da die entsprechende Normalform standardisiert ist und damit ihre Untersuchung mit einfachen, leicht überschaubaren Algorithmen erfolgen kann.

1.5. Resolventenmethode

In vielen Fällen ist es für die Untersuchung eines gegebenen Ausdrucks nicht erforderlich, ihn in eine Normalform zu überführen. Wir betrachten wieder nur Ausdrücke über einer Menge var_n mit n Variablen: $\mathsf{var}_n = \{ p_1, \ldots, p_n \}$. Einen alternativen Ausdruck nennt man **einfach**, wenn jede Variable p_i höchstens einmal vorkommt oder höchstens einmal negiert vorkommt. Insbesondere brauchen in einer einfachen Alternative nicht alle betrachteten Variablen aufzutreten; außerdem darf mit einer Variablen p_i auch $\neg p_i$ in einer einfachen Alternative vorkommen. Analog nennen wir einen konjunktiven Ausdruck einfach. Offenbar ist eine einfache Alternative genau dann allgemeingültig, wenn eine vorkommende Variable auch negiert vorkommt. Entsprechend ist eine einfache Konjunktion genau dann unerfüllbar, wenn eine vorkommende Variable auch negiert vorkommt. So ist z. B. die einfache Alternative

$$p \vee q \vee r \vee \neg p$$

allgemeingültig, wogegen die einfache Konjunktion

$$p \wedge \neg q \wedge r \wedge q$$

unerfüllbar ist.
Wir sagen, dass sich ein Ausdruck in **alternativer Standardform** befindet, wenn er eine Alternative von einfachen Konjunktionen ist. Entsprechend befindet sich ein Ausdruck in **konjunktiver Standardform**, wenn er eine Konjunktion von einfachen Alternativen ist.

1.11. Satz: *Jeden Ausdruck kann man in eine semantisch äquivalente alternative bzw. konjunktive Standardform überführen.*

Beweis: Der Beweis soll nur skizziert werden. Jeden Ausdruck kann man zunächst semantisch äquivalent in einen solchen überführen, der neben den Variablen nur noch die Funktoren $\neg, \wedge, \vee$ enthält. Sodann kann er durch Ausnutzen von Kommutativität, Distributivität, Idempotenz und den de Morgan'schen Regeln sowohl in eine konjunktive als auch in eine alternative Standardform semantisch äquivalent überführt werden. ♣
An der Standardform eines Ausdrucks kann man sofort die Allgemeingültigkeit bzw. Unerfüllbarkeit des Ausdrucks feststellen: Tritt bei der konjunktiven Standardform in jeder einfachen Alternative eine Variable nebst ihrer Negation auf, ist der Ausdruck allgemeingültig, andernfalls nicht. Tritt bei der alternativen Standardform in jeder einfachen Konjunktion eine Variable nebst ihrer Negation auf, ist der Ausdruck unerfüllbar, andernfalls nicht.
Beispiel: Wir wollen den indirekten Beweis

$$(p \to q) \leftrightarrow [(p \wedge \neg q) \to \neg p]$$

als allgemeingültig verifizieren. Dabei können wir den Prozess der Herleitung der konjunktiven Standardform abbrechen, wenn sich ein offensichtlich allgemeingültiger Ausdruck ergibt.

Unter Ausnutzung von

$$(A \to B) \cong (\neg A \vee B)$$

erhalten wir den zum indirekten Beweis semantisch äquivalenten Ausdruck

$$(\neg p \vee q) \leftrightarrow (\neg(p \wedge \neg q) \vee \neg p).$$

Auf der rechten Seite dieser Äquivalenz wenden wir eine de Morgan'sche Regel, die doppelte Verneinung, Assoziativität, Kommutativität und Idempotenz an:

$$\begin{aligned}\neg(p \wedge \neg q) \vee \neg p &\cong (\neg p \vee \neg\neg q) \vee \neg p \\ &\cong (\neg p \vee q) \vee \neg p \cong \neg p \vee q \vee \neg p \\ &\cong \neg p \vee \neg p \vee q \cong \neg p \vee q.\end{aligned}$$

Damit haben wir den Ausdruck für den indirekten Beweis in den dazu semantisch äquivalenten Ausdruck

$$(\neg p \vee q) \leftrightarrow (\neg p \vee q)$$

überführt, der aber offensichtlich allgemeingültig ist.
Als zweites Beispiel sei die alternative Standardform

$$p \vee (\neg p \wedge \neg q) \vee (\neg p \wedge q)$$

in eine konjunktive Standardform zu überführen. Unter Ausnutzung der Distributivität, Idempotenz und Kommutativität erhalten wir folgende Kette von semantischen Äquivalenzen:

$$p \vee (\neg p \wedge \neg q) \vee (\neg p \wedge q) \cong p \vee ((\neg q \vee q) \wedge \neg p) \cong (p \vee \neg p) \wedge (p \vee q \vee \neg q).$$

Jede einfache Alternative enthält eine Variable und ihre Negation; also ist der ursprüngliche Ausdruck allgemeingültig.
Unter dem **Erfüllbarkeitsproblem** versteht man die Aufgabe, von einem gegebenen Ausdruck zu entscheiden, ob er erfüllbar ist oder nicht. Dabei bedeutet das Wort „entscheiden" die Anwendung eines Algorithmus, der bei Eingabe eines beliebigen Ausdrucks nach endlich vielen Schritten (Operationen) ausgibt, ob der eingegebene Ausdruck erfüllbar ist oder nicht. Das Erfüllbarkeitsproblem hat in der Komplexitätstheorie große Bedeutung. Vielen mathematischen Aufgaben kann man Ausdrücke aus einer gewissen Sprache zuordnen, so dass das Auffinden eines Algorithmus für die Lösung der Aufgabe äquivalent zum Erfüllbarkeitsproblem für die entsprechende Ausdrucksmenge ist. Das Erfüllbarkeitsproblem der Aussagenlogik gehört zur

Klasse der sog. NP-vollständigen Probleme. Das sind solche Aufgaben, für die man keinen (deterministischen) Algorithmus kennt, dessen Operationszahl polynomial von der Anzahl der Eingabeinformationen abhängt. Um die Erfüllbarkeit eines Ausdrucks festzustellen, kann man z. B. einfach den Wert des Ausdrucks systematisch für alle möglichen Belegungen berechnen und aufhören, wenn man den Wert W erhalten hat. Da es bei n auftretenden Variablen 2^n verschiedene Belegungen gibt, ist dies ein exponentieller Algorithmus: Die Operationszahl hängt exponentiell von der Inputlänge ab, die hier die Variablenanzahl ist. Es scheint, dass es keinen besseren Algorithmus hinsichtlich Operationsaufwand gibt. Wohl aber gibt es Methoden, die sich besser auf Rechnern realisieren lassen als die systematische Suche. Ein solches Verfahren ist die **Resolventenmethode**, die nun betrachtet werden soll.

Wir setzen voraus, dass der gegebene Ausdruck in konjunktiver Standardform vorliegt. In der Standardform kommt es weder auf die Reihenfolge der einfachen Alternativen noch auf die Reihenfolge der Variablen in jeder einfachen Alternative an. Wir können daher eine einfache Alternative durch die Menge der in ihr auftretenden Variablen und negierten Variablen darstellen. Genauer: Jede Menge von Variablen und negierten Variablen definiert genau eine einfache Alternative und umgekehrt. Eine solche Menge nennen wir **Klausel** . Es sei bemerkt, dass eine Klausel eine Menge darstellt, also insbesondere keine Variable oder negierte Variable mehrfach in ihr auftreten kann. Eine konjunktive Standardform ist damit durch eine Klauselmenge dargestellt, wobei die Elemente gerade die Klauseln aus der Standardform sind. Es sei etwa

$$A = (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (q \vee \neg q).$$

Die Klauseln von A sind die Mengen

$$\{\, p, \neg q, r \,\},\; \{\, \neg p, q, \neg r \,\},\; \{\, q, \neg q \,\},$$

und die Klauselmenge von A lautet

$$\mathscr{K}(A) = \{\, \{\, p, \neg q, r \,\}, \{\, \neg p, q, \neg r \,\}, \{\, q, \neg q \,\} \,\}.$$

Die leere Menge fassen wir auch als Klausel auf und bezeichnen sie als leere Klausel. Wegen der Beziehung zwischen den konjunktiven Standardformen und ihren Klauselmengen können wir auch jeder Klauselmenge einen Wert bei einer Belegung α zuordnen, indem wir

$$\mathrm{ww}(\mathscr{K}(A), \alpha)) = \mathrm{ww}(A, \alpha)$$

setzen. Eine Klausel erhält dabei genau dann den Wert W, wenn mindestens eine ihrer Variablen oder negierten Variablen mit W bzw. F belegt wird. Eine Klauselmenge erhält genau dann den Wert W, wenn alle ihre Klauseln den Wert W haben.

Offenbar ist eine konjunktive Standardform genau dann erfüllbar, wenn ihre zugeordnete Klauselmenge erfüllbar ist. Auch die semantische Äquivalenz überträgt sich von den konjunktiven Standardformen auf die ihnen zugeordneten Klauselmengen.
Es sei A eine Klauselmenge. Eine Klausel K heißt **Resolvente** von A, wenn sie die folgenden beiden Bedingungen erfüllt:

1. Die Klausel K ist nicht allgemeingültig und nicht Element von A.

2. Es gibt eine Variable p und zwei verschiedene, nicht allgemeingültige Klauseln K_1, K_2 in A mit $p \in K_1, \neg p \in K_2$ und

$$K = K_1 \setminus \{ p \} \cup K_2 \setminus \{ \neg p \}.$$

Für die Klauselmenge

$$A = \{ p, \neg p, q, r \}, \{ \neg p, \neg q, r \}, \{ q, r \}, \{ \neg r \}, \{ q \}$$

gibt es die folgenden Resolventen:

$$\{ \neg p, r \}, \{ \neg p, \neg q \}.$$

Zentrale Feststellung ist nun der

1.12. Satz: *Ist A eine Klauselmenge und K eine Resolvente von A, so sind A und $A \cup \{ K \}$ semantisch äquivalent: $A \cong A \cup \{ K \}$.*

Beweis: Zunächst ist klar, dass eine Belegung α, die $A \cup \{ K \}$ erfüllt, auch A erfüllen muss, da die den Klauselmengen A und $\{ K \}$ entsprechenden Ausdrücke in dem $A \cup \{ K \}$ entsprechenden Ausdruck konjunktiv verknüpft sind. Es sei umgekehrt α eine Belegung, die A erfüllt und etwa mit $K_1, K_2 \in A, p \in K_1, \neg p \in K_2$:

$$K = K_1 \setminus \{ p \} \cup K_2 \setminus \{ \neg p \}.$$

Wegen $\text{ww}(K_1, \alpha) = \text{ww}(K_2, \alpha) = W$ muss es eine von p verschiedene Variable geben, so dass deren Belegung mindestens eine der beiden Klauseln K_1 und K_2 erfüllt. Diese Variable kommt auch in K vor, also gilt $\text{ww}(K, \alpha) = W$. ♣
Aus dieser Grundtatsache folgern wir sofort: Eine Klauselmenge A ist unerfüllbar, falls sie eine leere Resolvente hat. Eine leere Resolvente von A existiert genau dann, wenn A zwei Klauseln der Form $\{ p \}, \{ \neg p \}$ enthält.
Setzen wir nun

$$\mathsf{Res}(A) = A \cup \{ K \mid K \text{ ist Resolvente von } A \},$$

so können wir diese Mengenbildung iterieren, wobei im nullten Schritt alle allgemeingültigen Klauseln aus A entfernt werden:

$$\mathsf{Res}^0(A) = A \setminus \{\, K \in A \mid K \text{ ist allgemeingültig} \,\},$$

Falls $\mathsf{Res}^0 \neq \emptyset$, so

$$\mathsf{Res}^{r+1}(A) = \mathsf{Res}(\mathsf{Res}^r(A)),\ r = 0, 1, 2, \ldots.$$

Diese Iteration kann natürlich nur dann ausgeführt werden, wenn die nach dem nullten Schritt noch vorhandene Klauselmenge Elemente enthält, denn andernfalls ist A allgemeingültig. Nach der obigen Grundtatsache sind alle entstehenden Klauselmengen semantisch äquivalent. Andererseits enthält A nur endlich viele Variable. Daher gibt es auch nur endlich viele Resolventen, und die Iteration kann nur endlich oft zu einer neuen Menge führen. Es gibt somit ein l mit

$$\mathsf{Res}^{l+1}(A) = \mathsf{Res}^l(A) = \mathsf{Res}^*(A).$$

Die Klauselmenge $\mathsf{Res}^*(A)$ heißt die **Resolution** der Klauselmenge A.

1.13. Resolventensatz: *Eine Klauselmenge ist genau dann unerfüllbar, wenn ihre Resolution die leere Klausel enthält.*

Beweis: Wir haben nur zu beweisen, dass die Bedingung notwendig ist, denn wegen

$$A \cong \mathsf{Res}^*(A)$$

folgt aus $\emptyset \in \mathsf{Res}^*(A)$, dass die Klauselmenge A unerfüllbar ist.
Es sei A eine unerfüllbare Klauselmenge. Durch Induktion über die Anzahl n der in A auftretenden Variablen zeigen wir, dass $\emptyset \in \mathsf{Res}^*(A)$ sein muss. Im Falle $n = 0$ ist nichts zu beweisen, da in diesem Falle A nur die leere Klausel enthält. Als Induktionsvoraussetzung nehmen wir an, dass für jede unerfüllbare Klauselmenge B mit höchstens n Variablen $\emptyset \in \mathsf{Res}^*(B)$ gilt. Es sei nun A eine Klauselmenge mit $n+1$ Variablen und p eine beliebige, in A vorkommende Variable. Aus der Klauselmenge A bilden wir die folgenden beiden Klauselmengen A_1 und A_2: A_1 entstehe aus A dadurch, dass aus A alle Klauseln gestrichen werden, die $\neg p$ enthalten; in der Restmenge wird in allen Klauseln die Variable p gestrichen. Die Menge A_2 entstehe aus A in umgekehrter Weise: Es werden in A alle jene Klauseln gestrichen, die die Variable p enthalten und in der Restmenge wird aus jeder Klausel $\neg p$ entfernt. Die Klauselmengen A_1, A_2 sind nicht leer. Angenommen, A_1 ist leer. Dann enthält jede Klausel von A $\neg p$ und jede Belegung α mit $\alpha(p) = F$ erfüllt A, was aber nach Voraussetzung nicht sein kann. Entsprechend zeigt man, dass auch A_2 nicht leer ist. Wir

zeigen als nächstes, dass A_1 und A_2 unerfüllbar sind. Angenommen, es gibt eine Belegung α, die A_1 erfüllt. Dann erfüllt die Belegung α', die der Variablen p den Wert F und allen anderen den gleichen Wert wie α zuordnet, offenbar den Ausdruck A, was aber nicht sein kann, da A als unerfüllbar vorausgesetzt ist. Analog folgt, dass A_2 unerfüllbar ist. Da A_1 und A_2 jeweils höchstens n Variable enthalten, können wir auf sie die Induktionsvoraussetzung anwenden: Es gilt also $\emptyset \in \mathsf{Res}^*(A_1)$ und $\emptyset \in \mathsf{Res}^*(A_2)$. Wir fügen nun die Variable p in alle Elemente aus A_1, in denen sie gestrichen wurde, wieder ein. Dann ist $\mathsf{Res}^*(A_1) \subseteqq \mathsf{Res}^*(A)$ und daher $\{\, p \,\} \in \mathsf{Res}^*(A)$ oder $\emptyset \in \mathsf{Res}^*(A)$. Im zweiten Falle sind wir fertig. Im ersten Falle wird in A_2 die negierte Variable $\neg p$ an den alten Stellen wieder eingefügt und wir erhalten analog zu oben, dass $\{\, \neg p \,\} \in \mathsf{Res}^*(A)$ oder $\emptyset \in \mathsf{Res}^*(A)$. Beide Klauseln zusammen liefern im ersten Falle die leere Resolvente. ♣

Beispiel: Wir wenden die Resolventenmethode auf

$$A = \{\, \{\, p, \neg q, \neg r \,\}, \{\, \neg p, q, r \,\}, \{\, p, r \,\}, \{\, \neg r \,\} \,\}$$

an. Durch die obige Iteration erhalten wir die folgenden Klauselmengen:

$$\begin{aligned}
&\mathsf{Res}^1(A) = A \cup \{\, \{\, p, \neg q \,\}, \{\, \neg p, q \,\}, \{\, p \,\}, \{\, q, r \,\} \,\},\\
&\mathsf{Res}^2(A) = \mathsf{Res}^1(A) \cup \{\, \{\, q \,\} \,\},\\
&\mathsf{Res}^3(A) = \mathsf{Res}^2(A) \cup \{\, \{\, p, \neg r \,\} \,\},\\
&\mathsf{Res}^4(A) = \mathsf{Res}^3(A) \cup \{\, \{\, q, \neg r \,\}, \{\, p, q \,\} \,\},\\
&\mathsf{Res}^5(A) = \mathsf{Res}^4(A) = \mathsf{Res}^*(A).
\end{aligned}$$

Das Iterationsende zeigt an, dass der zugeordnete Ausdruck

$$(p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee r) \wedge \neg r$$

erfüllbar, aber nicht allgemeingültig ist.

Für eine wichtige Teilmenge von konjunktiven Standardformen gibt es einen polynomialen Algorithmus. Eine Klausel K, die bis auf höchstens eine Ausnahme nur negierte Variable enthält, heißt **Hornklausel** (nach dem Logiker A. HORN benannt). Entsprechend nennt man eine konjunktive Standardform **Hornausdruck** oder Hornformel, falls die zugeordnete Klauselmenge nur Hornklauseln enthält. Wegen

$$\neg p \vee q \cong p \to q$$

lässt sich jeder Hornausdruck als Konjunktion von Implikationen schreiben, z. B.

$$\begin{aligned}
&(\neg p \vee q) \wedge (\neg p \vee \neg r \vee s) \wedge (\neg p \vee \neg q) \wedge r \wedge \neg s\\
&\cong (p \to q) \wedge (p \wedge r \to s) \wedge (p \wedge q \to 0) \wedge (1 \to r) \wedge (s \to 0).
\end{aligned}$$

Hierin steht 0 für einen beliebigen unerfüllbaren und 1 für einen allgemeingültigen Ausdruck.
Für eine Horn-Klauselmenge A können wir nach dem folgenden Horn-Algorithmus die Erfüllbarkeit entscheiden, indem wir versuchen, direkt eine erfüllende Belegung α zu konstruieren.

1. Streiche in A alle allgemeingültigen Klauseln. Falls danach A leer ist, stoppe: A ist allgemeingültig.

2. Setze $\alpha(p) = W$ für alle p mit $\{ p \} \in A$.

3. Solange eine Klausel $K \in A$ existiert, in der alle negiert auftretenden Variablen belegt sind, führe aus: Wenn K eine unnegierte, unbelegte Variable enthält, so belege sie mit W; wenn K keine unnegierte Variable enthält, so stoppe: Der Ausdruck ist unerfüllbar.

4. Belege alle nicht belegten Variablen mit F und stoppe: Der Ausdruck ist erfüllbar.

1.14. Satz: *Für jede Horn-Klauselmenge A mit genau n Variablen gilt: Wenn der Ausdruck A erfüllbar ist, liefert der Horn-Algorithmus nach höchstens n Belegungsschritten eine erfüllende Belegung. Wenn A unerfüllbar ist, stoppt der Algorithmus mit dieser Ausgabe.*

Beweis: Es ist klar, dass der Algorithmus nach höchstens n Schritten endet. Wir können uns auf den Fall beschränken, dass die vorgegebene Horn-Klauselmenge keine allgemeingültigen Klauseln enthält. Für eine erfüllende Belegung muss jede Hornklausel den Wert W haben. Es sei H eine beliebige Hornklausel aus A. Enthält H nur eine Variable, so hat H nach Schritt 2 den Wert W. Hat H die Form $\{ \neg p_1, \ldots, \neg p_r, p \}$, so sind entweder alle Variablen durch Schritt 3 mit W belegt (der Wert von H ist damit gleich W) oder aber in Schritt 4 wird eine negiert vorkommende Variable mit F belegt, wodurch H auch den Wert W erhält. Wenn H die Form $\{ \neg p_1, \ldots, \neg p_r \}$ hat, wird in Schritt 3 korrekt gestoppt, falls $p_1, \ldots, p_r$ mit W belegt sind. Sollte auch noch Schritt 4 ausgeführt werden, erhält H dadurch den Wert W.
♣

1.6. Ableitbarkeit

Einen Ausdruck können wir mit folgenden Methoden auf Allgemeingültigkeit untersuchen: Zu allen möglichen Belegungen der auftretenden Variablen mit Wahrheitswerten berechnen wir den Wert des Ausdrucks. Das entspricht dem Aufstellen einer vollständigen Wertetabelle. Wir können den Ausdruck in n Variablen auch in seine konjunktive Normalform überführen. Entsteht dabei die Normalform

$$(p_1 \vee \neg p_1) \wedge (p_2 \vee \neg p_2) \wedge \ldots \wedge (p_n \vee \neg p_n),$$

so ist der gegebene Ausdruck allgemeingültig, andernfalls nicht. Als drittes können wir den vorgelegten Ausdruck in eine konjunktive Standardform überführen. Enthält jede entstandene einfache Alternative eine Variable und ihre Negation, so ist der Ausdruck allgemeingültig, andernfalls nicht. Schließlich können wir auch Schlussregeln anwenden. Ein Ausdruck ist genau dann allgemeingültig, wenn er mit Hilfe gewisser Schlussregeln aus einer Menge bereits als allgemeingültig erkannter Ausdrücke abgeleitet werden kann. In der klassischen Aussagenlogik verwendet man meist die Abtrennungs- und die Einsetzungsregel. Diese werden rein formal angewendet. Danach definiert die Abtrennungsregel den formalen Übergang von einem Ausdruck A und einem Ausdruck $A \to B$ zum Ausdruck B. Entsprechend definiert die Einsetzungsregel den formalen Übergang von einem Ausdruck A zu einem Ausdruck $A' = A(p|B)$, den man aus A dadurch erhält, dass man für die in A vorkommende Variable p an allen Stellen einen gegebenen Ausdruck B einsetzt. Diese Regeln werden unabhängig davon benutzt, ob ein allgemeingültiger Ausdruck vorliegt oder nicht. Wir wissen aber, dass sie stets von allgemeingültigen zu allgemeingültigen Ausdrücken führen. Es sei nun $\mathscr{X} \subseteqq \mathscr{L}$ eine beliebige Menge von Ausdrücken. Unter $\mathsf{Ab}(\mathscr{X})$ wollen wir die Menge aller aus den Elementen von $\mathscr{X}$ ableitbaren Ausdrücke verstehen. Wir sagen, dass der Ausdruck A aus $\mathscr{X}$ ableitbar ist, d. h. $A \in \mathsf{Ab}(\mathscr{X})$, wenn er durch endlich oftmalige Anwendung von Abtrennungs- und Einsetzungsregel aus Ausdrücken der Menge $\mathscr{X}$ erhalten werden kann. Dies impliziert, dass die Elemente der Ableitungsmenge $\mathsf{Ab}(\mathscr{X})$ induktiv definiert sind.

1. Jeder Ausdruck $A \in \mathscr{X}$ ist aus $\mathscr{X}$ ableitbar: $\mathscr{X} \subseteqq \mathsf{Ab}(\mathscr{X})$.

2. Abtrennungsregel: Sind die Ausdrücke A und $A \to B$ aus $\mathscr{X}$ ableitbar, so auch der Ausdruck B:

$$A, A \to B \in \mathsf{Ab}(\mathscr{X}) \quad \Longrightarrow \quad B \in \mathsf{Ab}(\mathscr{X}).$$

3. Einsetzungsregel: Für jeden Ausdruck B gilt: Wenn der Ausdruck A aus $\mathscr{X}$ ableitbar ist, so auch der Ausdruck $A(p|B)$, d. h. es gilt:

$$A \in \mathsf{Ab}(\mathscr{X}), p \in \mathsf{var}(A), B \in \mathscr{L} \quad \Longrightarrow \quad A(p|B) \in \mathsf{Ab}(\mathscr{X}).$$

4. Weitere, aus $\mathscr{X}$ ableitbare Ausdrücke gibt es nicht.

Im Sinne dieser Definition sind aus $\mathscr{X}$ zur Stufe 0 alle Elemente aus $\mathscr{X}$ ableitbar. Zur Stufe $n+1$ sind neben allen n-stufig ableitbaren Ausdrücken genau jene Ausdrücke ableitbar, die man mittels Abtrennungs- und Einsetzungsregel aus den n-stufig ableitbaren Ausdrücken gewinnen kann. Ein Ausdruck A ist genau dann aus $\mathscr{X}$ ableitbar, wenn es eine natürliche Zahl n gibt, so dass A n-stufig aus $\mathscr{X}$ ableitbat ist. Damit ist die Ableitungsmenge $\mathsf{Ab}(\mathscr{X})$ die kleinste Menge von Ausdrücken, die bezüglich der Einsetzungs- und Abtrennungsregel abgeschlossen ist. Außerdem gilt die Monotonie: Wenn $\mathscr{X}_1 \subseteqq \mathscr{X}_2$, so gilt $\mathsf{Ab}(\mathscr{X}_1) \subseteqq \mathsf{Ab}(\mathscr{X}_2)$.

1.15. Endlichkeitssatz für die Ableitbarkeit: *Jeder aus einer Menge $\mathscr{X}$ von Ausdrücken ableitbare Ausdruck ist bereits aus einer endlichen Teilmenge $\mathscr{X}^*$ von $\mathscr{X}$ ableitbar.*

Beweis: Wir beweisen diesen Satz durch Induktion über die Ableitungsstufe. Ist $A \in \mathscr{X}$, so kann man $\mathscr{X}^* = \{A\}$ setzen und A ist aus $\mathscr{X}^*$ 0-stufig ableitbar.
Als 1. Induktionsvoraussetzung haben wir: Der Ausdruck A gehe durch die Abtrennungsregel aus den Ausdrücken $B \in \mathsf{Ab}(\mathscr{X}_1^*)$ und $B \to A \in \mathsf{Ab}(\mathscr{X}_2^*)$ hervor, wobei $\mathscr{X}_1^*$ und $\mathscr{X}_2^*$ endliche Teilmengen von $\mathscr{X}$ sind. Wegen der Monotonie sind dann B und $B \to A$ aus $\mathscr{X}_1^* \cup \mathscr{X}_2$ ableitbar, also durch Anwendung der Abtrennungsregel auch der Ausdruck A. Die 2. Induktionsvoraussetzung lautet: Der Ausdruck A gehe mittels Einsetzungsregel aus dem Ausdruck B hervor und B sei aus einer endlichen Menge $\mathscr{X}_0^* \subseteqq \mathscr{X}$ ableitbar. Dann ist wegen der Einsetzungsregel A auch aus $\mathscr{X}_0^*$ ableitbar. ♣
Wir bemerken, dass man aus der leeren Menge nichts ableiten kann. Außerdem gilt $\mathsf{Ab}(\{p\}) = \mathscr{L}$, was bereits mit der Einsetzungsregel allein folgt.

1.16. Erblichkeit der Allgemeingültigkeit: *Aus einer Menge von allgemeingültigen Ausdrücken kann man nur allgemeingültige Ausdrücke ableiten:*

$$\mathscr{X} \subseteqq \mathsf{ag} \quad \Longrightarrow \quad \mathsf{Ab}(\mathscr{X}) \subseteqq \mathsf{ag}.$$

Abschließend soll noch ein Problem betrachtet werden, das in analoger Form in jeder mathematischen Theorie steht. Bekanntlich ist $\mathsf{Ab}(\mathsf{ag}) = \mathsf{ag}$. Kann man die Menge aller allgemeingültigen Ausdrücke aus einer einzigen endlichen Menge ableiten? Dies ist das **Axiomatisierbarkeitsproblem** für aussagenlogische Ausdrücke:
Gibt es eine endliche Menge – ein **Axiomensystem** –, deren ableitbare Ausdrücke genau alle allgemeingültigen sind?
In einfacherer Form haben wir das Axiomatisierbarkeitsproblem bereits in der Algebra studiert, z. B. bei Vektorräumen. Dort haben wir gezeigt, dass man Vektorräume aus einer beliebigen Basis erzeugen kann. Die Suche nach erzeugenden Elementen bei algebraischen Strukturen ist dort das sachgemäße Axiomatisierbarkeitsproblem.

Für die allgemeingültigen Ausdrücke wird es durch das folgende Axiomensystem, das man Axa nennt, gelöst.
Axa:

1. Prämissenbelastung: $p \to (q \to p)$.

2. Satz von CH. S. PEIRCE: $((p \to q) \to p) \to p$.

3. Kettenschluss: $(p \to q) \to [(q \to r) \to (p \to r)]$.

4. Konjunktion: $(p \wedge q) \to p$, $(p \wedge q) \to q$, $(p \to q) \to [(p \to r) \to (p \to q \wedge r)]$.

5. Alternative: $p \to (p \vee q)$, $q \to (p \vee q)$, $(p \to r) \to [(q \to r) \to (p \vee q \to r)]$.

6. Äquivalenz:

$$(p \to q) \to [(q \to p) \to (p \leftrightarrow q)],\ (p \leftrightarrow q) \to (p \to q),\ (p \leftrightarrow q) \to (q \to p).$$

7. Kontraposition: $(p \to q) \to (\neg q \to \neg p)$.

8. Doppelte Verneinung: $p \to \neg\neg p$, $\neg\neg p \to p$.

Es sei erwähnt, dass man das Axiomensystem Axa in folgender Weise abändern darf, wobei das abgeänderte zu Axa äquivalent ist: Anstelle des Satzes von Peirce und des Kettenschlusses verwende man den Kettenschluss

$$(p \to (q \to r)) \to ((p \to q) \to (p \to r)).$$

1.17. Axiomatisierbarkeit allgemeingültiger Ausdrücke: *Ein Ausdruck ist genau dann allgemeingültig, wenn er mit Abtrennungs- und Einsetzungsregel aus* Axa *abgeleitet werden kann.*

Wegen seines großen Umfangs wird hier auf einen Beweis verzichtet.
Da ein Ausdruck A genau dann allgemeingültig ist, wenn $\neg A$ unerfüllbar ist, folgt

1.18. Axiomatisierbarkeit unerfüllbarer Ausdrücke: *Jeder unerfüllbare Ausdruck der Aussagenlogik kann aus einer endlichen Menge von Ausdrücken abgeleitet werden.*

Für das effektive Durchführen von Ableitungen gibt es keine allgemein tragfähigen Regeln. Für einige allgemeingültige Ausdrücke wollen wir das Ableiten aus Axa explizit ausführen. Als erstes soll die Prämissenverschmelzung

$$[p \to (p \to q)] \to (p \to q)$$

aus Axa abgeleitet werden. Dies werden wir mit dem Kettenschluss tun, der überhaupt beim Ableiten eine herausragende Stellung einnimmt. Wir wenden den Kettenschluss so an, dass die letzte Implikation in ihm gerade die Prämissenverschmelzung ist, und die davor stehenden Implikationen durch geeignete Einsetzungen so gewählt werden, dass sie ableitbar sind, um sie dann abtrennen zu können. Damit die letzte Implikation $p \rightarrow r$ im Kettenschluss zur Prämissenverschmelzung wird, müssen wir im Kettenschluss für q einen noch unbekannten Ausdruck A, für p den Ausdruck $p \rightarrow (p \rightarrow q)$ und für r den Ausdruck $p \rightarrow q$ einsetzen. Die beiden abzutrennenden Prämissen aus dem Kettenschluss lauten danach

$$[p \rightarrow (p \rightarrow q)] \rightarrow A, \quad A \rightarrow (p \rightarrow q),$$

wobei für A ein solcher Ausdruck gefunden werden muss, dass beide Ausdrücke ableitbar sind. Die „Kunst“ besteht nun darin, einen solchen Ausdruck zu finden. Günstig wäre es, durch eine geeignete Einsetzung Ausdrücke zu erhalten, die sich als Axiome aus Axa verifizieren lassen. Wir wollen etwa, dass der obige zweite Ausdruck $A \rightarrow (p \rightarrow q)$ die Form des Satzes von Peirce hat. Dazu müssen wir im Satz von Peirce für die Variable p den Ausdruck $p \rightarrow q$ einsetzen. Hiernach lautet der Satz von Peirce:

$$\{\, [(p \rightarrow q) \rightarrow q] \rightarrow (p \rightarrow q) \,\} \rightarrow (p \rightarrow q).$$

Folglich nehmen wir für A die Prämisse dieses Ausdrucks:

$$A = [(p \rightarrow q) \rightarrow q] \rightarrow (p \rightarrow q)$$

und der Ausdruck $A \rightarrow (p \rightarrow q)$ stimmt mit dem Satz von Peirce überein. Mit diesem A lautet der erste Ausdruck

$$[p \rightarrow (p \rightarrow q)] \rightarrow \{\, [(p \rightarrow q) \rightarrow q] \rightarrow (p \rightarrow q) \,\},$$

der mit dem Kettenschluss übereinstimmt, wenn man dort für q den Ausdruck $p \rightarrow q$ und für r die Variable q einsetzt. Damit haben wir die Prämissenverschmelzung aus dem Satz von Peirce und dem Kettenschluss abgeleitet:

$$[p \rightarrow (p \rightarrow q)] \rightarrow (p \rightarrow q) \in \mathsf{Ab}(\mathsf{Axa}).$$

Setzen wir hier für q die Variable p ein, so erhalten wir den Ausdruck

$$[p \rightarrow (p \rightarrow p)] \rightarrow (p \rightarrow p).$$

In diesem ist die Prämisse ableitbar, denn sie ergibt sich aus der Prämissenbelastung, indem dort für q die Variable p eingesetzt wird. Also ist auch die Selbstimplikation ableitbar:

$$p \rightarrow p \in \mathsf{Ab}(\mathsf{Axa}).$$

Um einen weiteren Kunstgriff zu illustrieren, leiten wir die Prämissenvertauschung

$$[p \to (q \to r)] \to [q \to (p \to r)]$$

ab. Wieder verwenden wir den Kettenschluss: Wir haben für q einen noch unbekannten Ausdruck A, für p den Ausdruck $p \to (q \to r)$ und für r den Ausdruck $q \to (p \to r)$ in den Kettenschluss einzusetzen. Dabei ist A so zu wählen, dass die beiden Ausdrücke

$$[p \to (q \to r)] \to A, \quad A \to [q \to (p \to r)]$$

als ableitbar zu erkennen sind. Nach vielen Fehlversuchen erkennt man, dass es nicht gelingt. Daher probieren wir eine abgeschwächte Variante. Wir versuchen, für A einen solchen Ausdruck zu finden, dass der erste Ausdruck bereits als ableitbar erkannt ist und der zweite allgemeingültig wird, so dass für ihn dann die Ableitbarkeit noch nachgewiesen werden muss. Für den ersten Ausdruck bietet sich an, ihm die Form des Kettenschlusses zu geben. Dazu haben wir im Kettenschluss für q den Ausdruck $q \to r$ einzusetzen:

$$[p \to (q \to r)] \to \{\, [(q \to r) \to r] \to (p \to r) \,\}\,.$$

Hieraus lesen wir einen Ausdruck für A ab:

$$A = [(q \to r) \to r] \to (p \to r).$$

Damit ist noch der Ausdruck

$$\{\, [(q \to r) \to r] \to (p \to r) \,\} \to [q \to (p \to r)]$$

abzuleiten. Eine kleine Probe zeigt uns, dass er allgemeingültig ist, also ein Ausdruck entstanden ist, der ableitbar sein muss. Auch hierfür verwenden wir wieder den Kettenschluss, indem wir in ihm simultan für p die Variable q, für q den Ausdruck $(q \to r) \to r$ und für r den Ausdruck $p \to r$ einsetzen. Die Prämisse $p \to q$ lautet dann

$$q \to [(q \to r) \to r]$$

und die Conclusio nimmt die Form

$$\{\, [(q \to r) \to r] \to (p \to r) \,\} \to [q \to (p \to r)]$$

an, so dass nur noch die neue Prämisse abzuleiten ist, was wiederum mit dem Kettenschluss passieren soll, jetzt jedoch wieder so, dass sie in der letzten Conclusio $p \to r$

erscheint. Dazu haben wir für die Variable q einen noch unbekannten Ausdruck A, für r den Ausdruck

$$(q \to r) \to r$$

und für p die Variable q einzusetzen. Nun haben wir den Ausdruck A so zu bestimmen, dass uns die Ableitung der beiden Ausdrücke

$$q \to A, \quad A \to [(q \to r) \to r]$$

gelingt. Dazu wenden wir nochmals den obigen Kunstgriff an. Wir nehmen für A den Ausdruck $(q \to r) \to q$. Dann geht der Ausdruck $q \to A$ in den Ausdruck

$$q \to [(q \to r) \to q]$$

über, der gerade die Prämissenbelastung darstellt. Nun ist noch der Ausdruck

$$[(q \to r) \to q] \to [(q \to r) \to r]$$

abzuleiten. Auch hier macht der Kettenschluss den Anfang: Wir haben in ihm für q einen noch unbekannten Ausdruck A, für p den Ausdruck $(q \to r) \to q$ und für r den Ausdruck $(q \to r) \to r$ einzusetzen. Damit verbleibt die Ableitung der beiden Ausdrücke

$$[(q \to r) \to q] \to A, \quad A \to [(q \to r) \to r]$$

mit einem geeignet gewählten Ausdruck A. Wir wollen dem ersten Ausdruck die Form des Kettenschlusses geben. Dazu ist

$$A = (q \to r) \to [(q \to r) \to r]$$

zu wählen. Unsere beiden Ausdrücke lauten dann

$$\begin{aligned}
&[(q \to r) \to q] \to \{\, (q \to r) \to [(q \to r) \to r] \,\}\,, \\
&\{\, (q \to r) \to [(q \to r) \to r] \,\} \to [(q \to r) \to r].
\end{aligned}$$

Der erste stimmt mit dem Kettenschluss überein, wenn man dort offensichtliche Einsetzungen vornimmt. Der zweite ist die Prämissenverschmelzung. Damit ist die Prämissenvertauschung aus Axa abgeleitet. Auf dem Ableitungsweg haben wir noch weitere Ausdrücke als ableitbar erkannt:

$$\begin{aligned}
&[(p \to q) \to p] \to [(p \to q) \to q], \\
&p \to [(p \to q) \to q], \\
&\{\, [(p \to q) \to q] \to (p \to r) \,\} \to \{\, p \to (r \to q) \,\}\,, \\
&\{\, (p \to q) \to r \,\} \to \{\, (q \to p) \to r \,\}\,.
\end{aligned}$$

Aus diesen Ableitungen wird klar, mit welchen Schwierigkeiten man es zu tun hat, wenn man die Ableitung eines Ausdruck A explizit auszuführen hat: Man versucht, einen bereits als ableitbar erkannten Ausdruck durch simultane Einsetzung in eine solche Implikation zu überführen, aus der man A durch (eventuell mehrfache) Abtrennung gewinnen kann. Die dabei abgetrennten Ausdrücke sind danach als ableitbar zu verifizieren. Dafür gibt es zwei Möglichkeiten. Im ersten Falle findet man einen schon als ableitbar erkannten Ausdruck, der nach einer geeigneten simultanen Einsetzung in den abzuleitenden Ausdruck übergeht. Im zweiten Falle hat man die Prozedur mit dem neuen Ausdruck zu wiederholen. Diese Vorgehensweise ist solange fortzusetzen, bis kein zweiter Fall mehr eintritt. Auf diesem Wege muss man sich natürlich bei jedem abzuleitenden Ausdruck davon überzeugen, ob er überhaupt ableitbar sein kann. Im Falle des Axiomensystems Axa bedeutet dies: Man suche nach einer Belegung, die den Ausdruck nicht erfüllt. Stößt man bei dieser Suche auf einen Widerspruch, ist der Ausdruck allgemeingültig und damit aus Axa ableitbar.

1.7. Anwendungen in der Automatentheorie

Eine Anwendung der Aussagenlogik betrifft den mathematischen Schaltkreisentwurf, wozu hier einige Bemerkungen gemacht werden sollen. Dazu wird zunächst unser Automatenbegriff aus der Algebra etwas spezialisiert. In einem Automaten $\mathscr{R} = (K, \Sigma, T, \sigma, \lambda)$ seien das Eingabealphabet Σ und das Ausgabealphabet T jeweils Produktmengen:

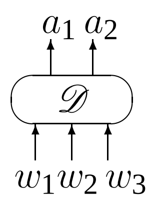
$$\Sigma = \Sigma_1 \times \Sigma_2 \times \cdots \times \Sigma_n, \quad T = T_1 \times T_2 \times \cdots \times T_m.$$

Bei Eingabe eines n-Tupels $(s_1, \ldots, s_n)$ aus der Menge Σ möge der Automat ein m-Tupel $(t_1, \ldots, t_m)$ aus T ausgeben. Wir nehmen ferner an, dass $K = \emptyset$ gilt, d. h. es gibt keine Zustände im Automaten (speicherloser Automat). Entsprechend gibt es auch keine Überführungsfunktion σ, so dass sich das definierende 5-Tupel auf ein Tripel $\mathscr{R} = (\Sigma, T, \lambda)$ reduziert. Besonders wichtig ist der Spezialfall, dass alle Mengen Σ_j und T_i aus einem zweielementigen Alphabet $\{0, 1\}$ bestehen. Solche Automaten lassen sich einerseits leicht realisieren und andererseits kann man den allgemeinen Fall theoretisch auf diesen reduzieren, in dem man die Ein- und Ausgaben dual codiert. Dieser Spezialfall soll hier studiert werden. Zur i-ten Komponente t_i der Ausgabe $(t_1, \ldots, t_m)$ gehört eine Funktion λ_i von n Argumenten, wobei bei Eingabe von $(s_1, \ldots, s_n)$ gerade $\lambda_i(s_1, \ldots, s_n) = t_i$ gilt. Wir nennen λ_i die durch die Ausgabe t_i des Automaten $\mathscr{R}$ realisierte Wahrheitsfunktion: $\lambda = (\lambda_1, \ldots, \lambda_m)$. Als Beispiel betrachten wir den Dualadder $\mathscr{D}$ mit einem Tripel (w_1, w_2, w_3) als Eingabe und einem Paar (a_1, a_2) als Ausgabe, wobei durch die Ausgabe die folgenden beiden Wahrheitsfunktionen realisiert sein mögen:

w_1	w_2	w_3	λ_1	λ_2
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

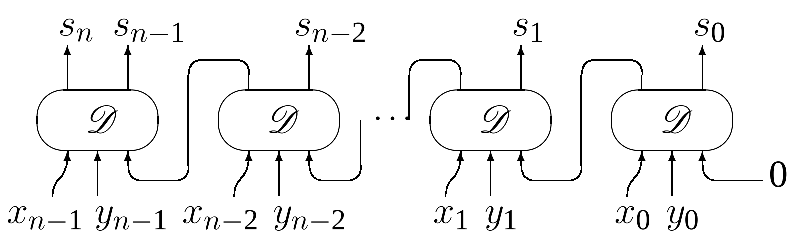
.

Den Dualadder können wir wie folgt darstellen:



.

Wir schalten nun n solcher Dualadder in folgender Weise:



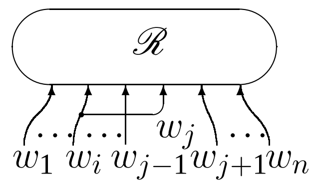
Man überlegt sich leicht, dass dieser Automat bei Eingabe zweier n-stelliger Dualzahlen

$$x = x_{n-1}x_{n-2}\dots x_1x_0, \quad y = y_{n-1}y_{n-2}\dots y_1y_0$$

als Ausgabe ihre Summe liefert: $s = x + y$, wobei s eine $(n+1)$-stellige Dualzahl ist:

$$s = s_ns_{n-1}\dots s_1s_0.$$

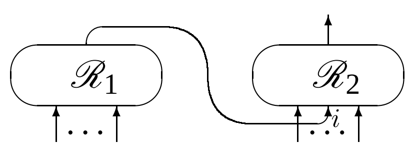
Von praktischer Bedeutung ist die Verknüpfung speicherloser Automaten zu logischen Netzen. Wir beschränken uns hier auf solche Netze, die aus Automaten mit nur einem Ausgang aufgebaut sind. Die logischen Netze werden durch die beiden folgenden Operationen geknüpft: Für einen Automaten $\mathscr{R}$ mit n Eingängen sei $[\mathscr{R}]_{ij}$ für $i < j$ jener Automat mit $n-1$ Eingängen, der aus $\mathscr{R}$ dadurch entsteht, dass die beiden Eingänge i und j zusammengelegt werden:



Wenn $\mathscr{R}$ die n-stellige Wahrheitsfunktion φ realisiert, so realisiert $[\mathscr{R}]_{ij}$ die $(n-1)$-stellige Wahrheitsfunktion ψ, die gemäß

$$\psi(w_1,\dots,w_i,\dots,w_{j-1},w_{j+1},\dots,w_n) = \varphi(w_1,\dots,w_{j-1},w_i,w_{j+1},\dots,w_n)$$

gegeben ist.
Für die zweite Operation seien zwei speicherlose Automaten $\mathscr{R}_1$, $\mathscr{R}_2$ mit n_1 bzw. n_2 Eingängen und je einem Ausgang gegeben. Aus diesen beiden bilden wir den Automaten $\mathscr{R}_1 \to_i \mathscr{R}_2$, indem wir den Ausgang von $\mathscr{R}_1$ zum i-ten Eingang von $\mathscr{R}_2$ machen. Die Operation $\to_i$ verbindet also den Ausgang des ersten Automaten mit dem i-ten Eingang des zweiten Automaten:



Dabei entsteht ein Automat mit n_1+n_2-1 Eingängen und genau einem Ausgang. Wenn zum Automaten $\mathscr{R}_1$ die n_1-stellige Wahrheitsfunktion φ_1, zum Automaten $\mathscr{R}_2$ die n_2-stellige Wahrheitsfunktion φ_2 gehört, so wird die Verknüpfung $\mathscr{R}_1 \to_i \mathscr{R}_2$ durch die (n_1+n_2-1)-stellige Wahrheitsfunktion ψ repräsentiert, die durch

$$\begin{aligned}&\psi(w_1,\dots,w_{n_1},v_1,\dots,v_{i-1},v_{i+1},\dots,v_{n_2})\\&=\varphi_2(v_1,\dots,v_{i-1},\varphi_1(w_1,\dots,w_{n_1}),v_{i+1},\dots,v_{n_2})\end{aligned}$$

gegeben ist.
Wir stellen uns nun vor, dass wir endlich viele Typen $\mathscr{E}_1,\dots,\mathscr{E}_l$ von Elementarautomaten haben und nehmen an, dass von jedem Typ beliebig viele Exemplare von Automaten vorhanden sind. Die Automaten des Typs $\mathscr{E}_\lambda$ realisieren alle die gleiche Wahrheitsfunktion ε_λ. Ein $(\mathscr{E}_1,\dots\mathscr{E}_l)$-Netz ist dann ein logisches Netz, das induktiv aus Automaten der Typen $\mathscr{E}_1,\dots,\mathscr{E}_l$ aufgebaut ist, wobei nur die Operationen $[\cdot]_{ij}$ und $\to_i$ verwendet wurden. Jedes solche logische Netz realisiert dann eine Wahrheitsfunktion, die Superposition der Funktionen $\varepsilon_1,\dots,\varepsilon_l$ ist und umgekehrt. Eine Superposition der Funktionen $\varepsilon_1,\dots,\varepsilon_l$ kann auf verschiedene Weise durch ein $(\mathscr{E}_1,\dots,\mathscr{E}_l)$-Netz realisiert werden. Zwei Netze mit gleicher Funktion heißen äquivalent. Über diesen Netzen kann man insbesondere folgende Probleme untersuchen:

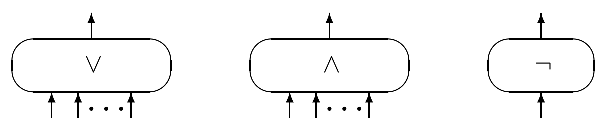
- **Analyseproblem**: Für ein gegebenes Netz ist die dadurch realisierte Wahrheitsfunktion zu ermitteln.

- **Synteseproblem**: Bei gegebener Wahrheitsfunktion ist ein die Funktion realisierendes Netz zu bestimmen. Dabei ist zunächst zu prüfen, ob die gegebene Wahrheitsfunktion durch die Funktionen $\varepsilon_1, \ldots, \varepsilon_l$ superponiert werden kann. Dieses Lösbarkeitsproblem kommt daher, dass die Wahrheitsfunktion oft in einer Form gegeben ist, die eine Umsetzung in eine Superposition der Funktionen $\varepsilon_1, \ldots, \varepsilon_l$ erfordert.

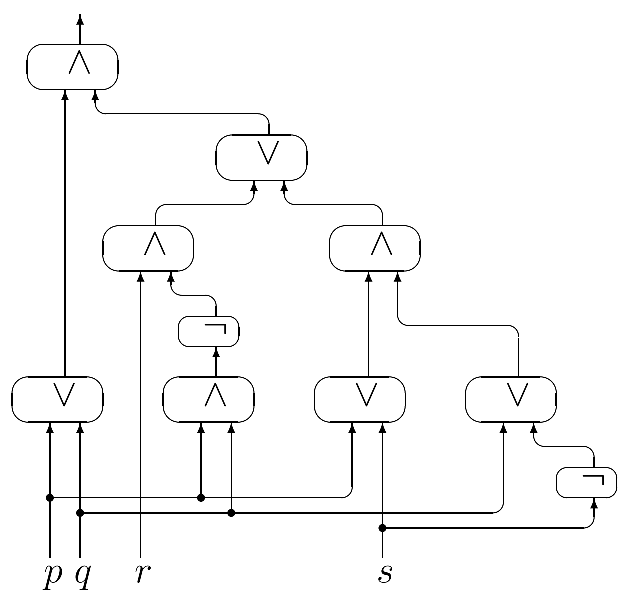
- **Äquivalenzproblem**: Von zwei gegebenen Netzen ist zu ermitteln, ob sie die gleiche Wahrheitsfunktion realisieren oder nicht. Hierfür interessieren direkte Methoden.

- **Optimierungsproblem**: Unter allen Netzen, die eine gegebene Wahrheitsfunktion realisieren, ist ein solches zu bestimmen, das in einem gewissen Sinne optimal ist. Ein solches optimales Netz könnte z. B. an die Aufgabe gebunden sein, den Gesamtpreis als Summe der Preise für die eingesetzten Elementarautomaten zu minimieren.

Beispiel: Für eine einfache Alternative, einfache Konjunktion und die Negation benutzen wir Symbole der folgenden Form



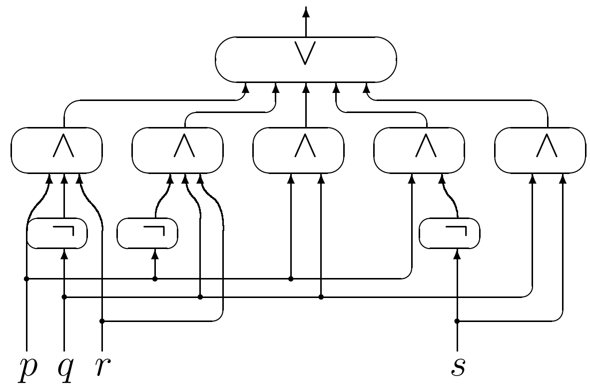
Dem Ausdruck $(p \vee q) \wedge (\neg(p \wedge q) \wedge r \vee (p \vee s) \wedge (q \vee \neg s))$ entspricht das folgende logische Netz:



Durch „Ausmultiplizieren" des Ausdrucks erhält man den semantisch äquivalenten

$$p \wedge \neg q \wedge r \vee \neg p \wedge q \wedge r \vee p \wedge q \vee p \wedge \neg s \vee q \wedge s$$

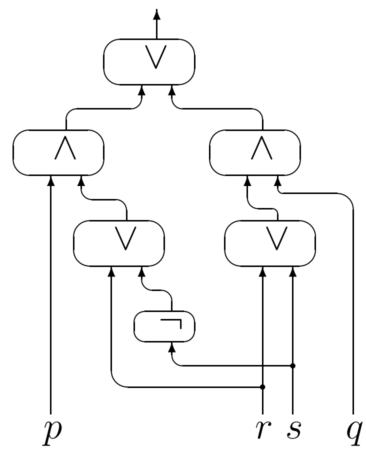
und damit das logisch gleichwertige Netz



Mittels äquivalenter Umformungen lässt sich der Ausdruck auf

$$p \wedge (r \vee \neg s) \vee q \wedge (r \vee s)$$

reduzieren, wozu das nebenstehende logische Netz gehört:



Beim logischen Netz für den Dualadder wird die Übertragungsfunktion λ_1 durch

$$X(p,q,r) = p \wedge q \vee ((p \vee q) \wedge r)$$

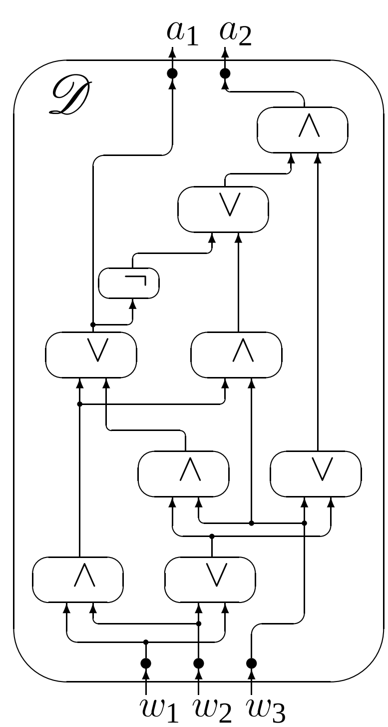
repräsentiert. Aus der Wahrheitstafel entnehmen wir, dass

$$\lambda_2(w_1, w_2, w_3) = \text{not}(\lambda_1(w_1, w_2, w_3))$$

für alle jene Eingaben gilt, die verschieden von $(0,0,0)$ und $(1,1,1)$ sind. Folglich wird λ_2 durch den Ausdruck

$$(p \wedge q \wedge r \vee \neg X(p,q,r)) \wedge (p \vee q \vee r)$$

repräsentiert. Damit stellt z. B. das nebenstehende Netz einen Dualadder dar:



Kapitel 2

Prädikatenlogik

2.1. Aussageformen

Die Betrachtungen in diesem Abschnitt sollen die Einführung einer ausdrucksstärkeren Sprache, als es die Aussagenlogik ist, motivieren. Für die Modellierung grundlegender Sachverhalte in Mathematik und Informatik ist die Aussagenlogik nicht ausreichend. So bilden sich sehr einfache Formulierungen innerhalb der Aussagenlogik nicht adäquat ab, z. B. „Die reelle Zahl x ist kleiner als die reelle Zahl y“ oder „$x^2 + y^2 = z^2$“. Ein solches sprachliches Gebilde nennt man **Aussageform**. In einer Aussageform kommen sog. freie Variable vor, für die man Namen von Objekten der Wirklichkeit oder des Denkens einzusetzen hat, um die Aussageform zu einer Aussage zu machen. Aus dem Zusammenhang ist dabei stets klar, aus welchem Bereich (Universum) die Variablen Werte annehmen dürfen. Zu jeder Aussageform gibt es eine wohlbestimmte Anzahl von freien Variablen, die in ihr vorkommen. Diese Anzahl nennt man **Stellenzahl** der Aussageform. Wir sprechen von einer n-stelligen Aussageform A, wenn in A genau n verschiedene freie Variable vorkommen. Die Aussagen selbst sind dann 0-stellige Aussageformen. Die Aussageform „x ist Element der Menge M“ wird z. B. zu einer Aussage, wenn man für x eine natürliche Zahl (genauer den Namen für eine natürliche Zahl) und für M eine Teilmenge der natürlichen Zahlen einsetzt, so dass etwa die Aussage „4 ist Element der natürlichen Zahlen“ oder auch „ $5 \in \{2,4,6,8\}$“ entstehen könnte. Den Bereich, aus dem eine freie Variable in einer Aussageform Werte annehmen darf, nennt man **Universum** U. Wir betrachten hier nur den sog. einsortigen Fall, d. h. sämtliche Variable dürfen nur Werte aus genau einem vorgegebenen Universum annehmen. Die Aussageform

„Der Punkt p liegt auf der Geraden g“

wird nicht modellierbar sein, da p und g aus verschiedenen Universen zu wählen sind.

Durch aussagenlogische Verbindung mit „nicht“, „und“, „oder“, „wenn, so“ und „genau dann, wenn“ lassen sich aus Aussageformen neue mit höherer Stelligkeit bilden. Man kann aber auch aus einer n-stelligen Aussageform eine solche mit niederer Stelligkeit bilden. Das kann z. B. dadurch geschehen, dass man für gewisse Variable Werte einsetzt; die betreffende Variable wird konstant gesetzt. Außerdem kann man durch **Quantifizierung** aus einer n-stelligen Aussageform eine $(n-1)$-stellige gewinnen. Dazu sei $A(x)$ eine Aussageform mit der freien Variablen x. Indem wir zu der Aussageform „für jedes $x \in U$ gilt $A(x)$“ oder „es gibt ein $x \in U$“ übergehen, haben wir eine neue Aussageform gewonnen mit einer um 1 niedrigeren Stelligkeit. Durch die Quantifizierung „für jedes $x \in U$“ bzw. „es gibt ein $x \in U$“ wird die freie Variable x gebunden und es entsteht aus der n-stelligen Aussageform eine $(n-1)$-stellige. So wird z. B. aus der zweistelligen Aussageform „$x < y$“ die einstellige Aussageform „Für jedes $x \in \mathbb{R}$ gilt: $x < y$“ und daraus schließlich die Aussage „Zu jedem $x \in \mathbb{R}$ gibt es ein $y \in \mathbb{R}$ mit $x < y$“. Aussageformen sind in folgendem Sinne extensional: Beim Übergang von einer Aussageform zu einer Aussage hängt der Wahrheitswert der entstandenen Aussage ausschließlich von der Belegung der Variablen mit Werten aus dem Universum U ab und nicht davon, welchen „Sinn“ die Aussageform hat. Dies erlaubt uns den folgenden Abstraktionsprozess: Zu jeder n-stelligen Aussageform $A(x_1, \ldots, x_n)$, in der die freien Variablen x_i nur Werte aus einem gegebenen Universum U annehmen dürfen, existiert eine n-stellige Relation R in U. Dabei gilt $(\xi_1, \ldots, \xi_n) \in R$, falls die Aussage $A(\xi_1, \ldots, \xi_n)$ wahr ist und andernfalls $(\xi_1, \ldots, \xi_n) \notin R$. So ist der Aussageform „$x < y$“ in $U = \mathbb{N}$ die $<$-Relation im Bereich der natürlichen Zahlen zugeordnet. Die Relation R_U^n mit $R_U^n = U^n$ nennen wir n-stellige All-Relation und die Relation $R_U^\emptyset$ mit $R_U^\emptyset = \emptyset$ heißt n-stellige Leer-Relation. Für die formale Abschließung brauchen wir noch eine 0-stellige All-Relation und eine 0-stellige Leer-Relation. Die 0-stellige All-Relation bezeichnen wir mit W und die 0-stellige Leer-Relation mit F. Dies sind nur Zeichen für uns.
Es sei A eine n-stellige Aussageform und x eine freie Variable in A: $A = A(x)$. Dem Übergang von der n-stelligen Aussageform $A(x)$ zu der $(n-1)$-stelligen Aussageform $A' =$„für jedes x gilt $A(x)$“ bzw. $A' =$„es gibt ein x mit $A(x)$“ entspricht der Übergang von einer n-stelligen Relation R_A zu einer $(n-1)$-stelligen Relation $R_{A'} = \mathrm{Om}(R_A)$ bzw. $R_{A'} = \mathrm{Ex}(R_A)$. Den klassischen Quantifizierungen entsprechen damit Funktionen Om und Ex, die nach Fixierung einer Variablen x_i jeder n-stelligen Relation R eine $(n-1)$-stellige Relation $\mathrm{Om}(R)$ bzw. $\mathrm{Ex}(R)$ zuordnen. Dabei gilt

$$(\xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_n) \in \mathrm{Om}(R)$$

genau dann, wenn für alle $\xi \in U$ gilt

$$(\xi_1, \ldots, \xi_{i-1}, \xi, \xi_{i+1}, \ldots, \xi_n) \in R.$$

Entsprechend gilt

$$(\xi_1, \dots, \xi_{i-1}, \xi_{i+1}, \dots, \xi_n) \in \mathrm{Ex}(R)$$

genau dann, wenn ein $\xi \in U$ existiert mit

$$(\xi_1, \dots, \xi_{i-1}, \xi, \xi_{i+1}, \dots, \xi_n) \in R.$$

Insbesondere ordnet die Funktion Om der 1-stelligen All-Relation den Wert W und jeder anderen 1-stelligen Relation den Wert F zu. Die Funktion Ex ordnet der 1-stelligen leeren Relation den Wert F zu und jeder anderen 1-stelligen Relation den Wert W. Unter den n-stelligen Relationen gibt es natürlich Relationen R, für die $\mathrm{Om}^n(R) = W$ gilt. Solche n-stelligen Relationen nennt man **allgemeingültig**; sie haben als Urbild Aussageformen, die bei jeder Belegung der freien Variablen mit Werten aus dem Universum zu einer wahren Aussage werden. Im Hinblick auf Anwendungen werden wir neben Relationssymbolen auch Operationssymbole in den Aussageformen zulassen.

2.2. Ausdrücke einer Sprache erster Stufe

Eine Sprache erster Stufe ist durch das folgende Alphabet festgelgt:

- Eine Menge von Funktoren $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists$,
- eine Menge var von Variablen $x, y, z, u, v, \dots$ (eventuell mit Indices),
- runde Klammern (,) und das Komma,
- eine (evtl. leere) Menge von Konstantensymbolen $a, b, c, \dots$ (eventuell mit Indices),
- für jedes $n \geqq 1$ eine (evtl. leere) Menge von n-stelligen Relationssymbolen $P, Q, R, \dots$ (evtl. mit Indices),
- für jedes $n \geqq 1$ eine (evtl. leere) Menge von n-stelligen Operationssymbolen $f, g, h \dots$ (evtl. mit Indices).

Die letzten 3 Symbolmengen bilden die sog. **Signatur** S der Sprache, die restlichen bezeichnen wir mit $\mathscr{A}$, so dass $\mathscr{A}^S = \mathscr{A} \cup S$ das gesamte Alphabet darstellt. Bis auf die Quantoren $\forall, \exists$ kennen wir die Funktoren bereits aus der Aussagenlogik. Der Quantor $\forall$ steht für die Quantifizierung einer Aussageform $A(x)$ zur Aussageform „für jedes x gilt $A(x)$“; entsprechend steht der Quantor $\exists$ für die Quantifizierung „es

gibt ein“.
Jede endliche Aneinandereihung von Zeichen unseres Alphabets heißt **Wort** . Die Menge aller Wörter über $\mathscr{A}^S$ bezeichnen wir mit $\mathscr{A}_S^*$; man nennt sie **Sprache**.

2.1. Satz: *Die Menge $\mathscr{A}_S^*$ aller Wörter über dem Alphabet $\mathscr{A}^S$ ist abzählbar.*

Beweis: Zum Beweis verwenden wir die sog. **Gödelnummerierung**. Zunächst ist das Alphabet abzählbar. Wir ordnen jedem Zeichen z aus dem Alphabet einen Index $\lambda(z)$ in der Weise zu, dass verschiedene Zeichen auch verschiedene Indices erhalten. Es sei p_n die n-te Primzahl in aufsteigender Reihenfolge. Jedem Wort $w = w_1 w_2 \dots w_l$ ordnen wir die Zahl $g(w) = p_1^{\lambda(w_1)} \dots p_l^{\lambda(w_l)}$, die **Gödelnummer** des Wortes w bezüglich der betrachteten Nummerierung des Alphabetes, zu. Damit sind offenbar alle Wörter umkehrbar eindeutig auf eine Teilmenge der natürlichen Zahlen abgebildet. ♣

Die Gödelnummerierung ist in dem Sinne universell, dass jedes formale System $(S_1, S_2, \dots, S_n, \dots)$ mit abzählbaren Mengen S_i eine Gödelnummerierung hat. Damit entspricht jedem System von wahren Sätzen über einem höchstens abzählbaren, formalen System $(S_1, S_2, \dots, S_n, \dots)$ mit abzählbaren Mengen S_i umkehrbar eindeutig ein System von wahren Sätzen über natürliche Zahlen. Kurzum: Die Theorie der natürlichen Zahlen ist so reichhaltig, dass sie alle wahren Sätze über solchen Systeme bereits enthält.
Um aus den Wörtern die Ausdrücke aussondern zu können, definieren wir zunächst induktiv, was ein S-**Term** sein soll.

1. (Atomare Terme:) Die Variablen und die Konstantensymbole sind S-Terme.

2. (Abgeleitete Terme:) Sind $t_1, \dots, t_m$ S-Terme und f ein m-stelliges Operationssymbol aus der Signatur S, so ist auch $f(t_1, \dots, t_m)$ ein S-Term.

3. Zu jedem Term t gibt es eine natürliche Zahl n so, dass man durch n-malige Anwendung von 2. den Term aus atomaren Termen gewinnen kann.

Mit $\mathscr{T}^S$ bezeichnen wir die Menge aller Terme über einer Signatur S. Die Terme sind also gerade jene Wörter, die z. B. auf den rechten und linken Seiten von mathematischen Gleichungen auftreten.
Wir sagen, dass in einem Wort w die Variable x **abs-frei** vorkommt, wenn sie in w vorkommt, aber nicht $\forall x$ oder $\exists x$ vorkommt, d. h. wenn die Variable x zwar vorkommt, aber nicht quantifiziert auftritt. Nach dieser kleinen Vorbereitung können wir induktiv einen S-Ausdruck definieren.

1. Die atomaren Ausdrücke sind die relationalen: Sind $t_1, \dots, t_m$ S-Terme und ist R ein m-stelliges Relationssymbol aus S, so ist $Rt_1 \dots t_m$ ein Ausdruck.

2. Abgeleitete Ausdrücke:

   - Aussagenlogische Ausdrücke: Sind A und B zwei S-Ausdrücke, so sind auch

     $$\neg A,\ (A \wedge B),\ (A \vee B),\ (A \to B),\ (A \leftrightarrow B)$$

     S-Ausdrücke.

   - Quantifizierte Ausdrücke: Ist $A(x)$ ein S-Ausdruck, in dem die Variable x abs-frei vorkommt, so sind auch $\forall x A(x)$ und $\exists x A(x)$ Ausdrücke.

3. Zu jedem Ausdruck A gibt es eine natürliche Zahl n, so dass A durch n-malige Anwendung von 2. aus den atomaren Ausdrücken gewonnen werden kann.

Die Menge aller Ausdrücke bezeichnen wir mit $\mathscr{L}^S$; sie ist die zur Signatur S gehörende Sprache erster Stufe. Eine Sprache, die nur n Variable $x_1, \ldots, x_n$ verwendet, wird mit $\mathscr{L}_n^S$ bezeichnet. Wir bemerken noch, dass der Hinweis auf die Signatur gelegentlich weggelassen wird, sofern klar ist, welche Signatur gemeint sein soll oder aber die Signatur unwichtig ist.
Bei der Notierung von Ausdrücken benutzen wir analog zur Aussagenlogik vereinfachende Schreibweisen. Außerdem werden wir oft bei einem relationalen Ausdruck mit einem zweistelligen Relationssymbol anstelle der Präfixnotation Rxy die in der Mathematik übliche Schreibweise xRy verwenden. Um die Lesbarkeit von Ausdrücken zu unterstützen, verwenden wir anstelle der runden Klammern beim Notieren von Ausdrücken und Termen auch die eckigen und die geschweiften Klammern; desweiteren setzen wir gelegentlich auch Klammern an Stellen, wo sie eigentlich nicht stehen dürften. Ein einfaches Beispiel für Ausdrücke ist die Theorie der Äquivalenzrelationen. Wir setzen dazu $S = \{R\}$, wobei R ein zweistelliges Relationssymbol sein soll. Die Axiome für eine Äquivalenzrelation lauten dann

$$\begin{aligned}&\forall x xRx,\ \forall x \forall y (xRy \to yRx),\\ &\forall x \forall y \forall z [(xRy \wedge yRz) \to xRz].\end{aligned}$$

Es sei A ein Ausdruck, in dem die Variable x quantifiziert vorkommt. Nach der induktiven Ausdrucksdefinition beginnt unmittelbar hinter dieser Stelle ein Teilausdruck B von A, in dem die Variablen x abs-frei vorkommt. Diesen Teilausdruck nennt man **Wirkungsbereich** der Quantifizierung von x im Ausdruck A. So gehört z. B. im Ausdruck

$$\forall x[\neg \exists y(yPx \to yQf(x)) \wedge g(a, f(y))Qf(x)]$$

zur Quantifizierung $\exists y$ der Variablen y der Wirkungsbereich $(yPx \to yQf(x))$. Man sagt, dass eine Variable x in einem Ausdruck A **gebunden** vorkommt, wenn sie an einer Stelle quantifiziert vorkommt. Schließlich kommt eine Variable x im Ausdruck A **rel-frei** vor, wenn sie an einer Stelle vorkommt, die nicht zum Wirkungsbereich einer Quantifizierung von x gehört. Enthält der Ausdruck A keine rel-freien Variablen, heißt er **abgeschlossen** oder kurz **Aussage**. Falls im Ausdruck A die Variable x abs-frei vorkommt, schreiben wir $A(x)$. In einem Term t kommt natürlich jede vorkommende Variable x abs-frei vor. Analog zur Aussagenlogik ist hier $A(x|t)$ jener Ausdruck, der aus $A(x)$ dadurch entsteht, dass für die Variable x an allen Stellen ein Term $t \in \mathscr{T}^S$ eingesetzt wird. In einem solchen Term können Variable auftreten, die bereits im Ausdruck $A(x)$ vorkommen. Da x eine abs-freie Variable ist, dürfen die im Term t vorkommenden Variablen nach der Einsetzung in A nicht gebunden sein. Wir nennen daher eine Termeinsetzung $A(x|t)$ **zulässig**, wenn keine in t vorkommende Variable im Ausdruck $A(x|t)$ gebunden vorkommt. Speziell spricht man von einer abs-freien Umbenennung, falls der Term t eine Variable ist. Für den Ausdruck

$$\forall y(yPx \to yQx)$$

ist der Übergang zum Ausdruck

$$\forall y(yPf(z,a) \to yQf(z,a))$$

eine zulässige Termeinsetzung während der Term $h(y)$ zu keiner zulässigen Termeinsetzung führt.
In einem Term $t(x)$ kann für die vorkommende Variable x ein beliebiger Term eingesetzt werden, was schon aus der induktiven Termdefinition folgt.
Neben der abs-freien Umbenennung kann man auch gebunden umbenennen. Dazu sei x eine Variable, die im Ausdruck A gebunden vorkommt. Man sagt, dass der Ausdruck A durch **gebundene Umbenennung** in den Ausdruck A' übergeht, wenn man A' aus A dadurch gewinnen kann, dass für die Variable x an einer Quantifizierungsstelle und an allen Stellen des zugehörenden Wirkungsbereiches eine andere Variable y eingesetzt wird. Dabei heißt die gebundene Umbenennung **zulässig**, wenn die folgenden Bedingungen erfüllt sind:

- Die Variable y darf im Wirkungsbereich der Quantifizierung von x nicht vorkommen.

- Falls die Variable y im Ausdruck A quantifiziert vorkommt, darf der Wirkungsbereich der Quantifizierung von x nicht im Wirkungsbereich der Quantifizierung von y liegen.

Illustrieren wir die Situation an einem Beispiel. Gegeben sei der Ausdruck

$$\forall x \exists y[yPx \to \exists z(zPx \wedge xQx_0)] \wedge xQz.$$

Indem wir hier die Variable x in x_1 gebunden umbenennen, entsteht der neue Ausdruck

$$\forall x_1 \exists y[yPx_1 \to \exists z(zPx_1 \wedge x_1 Q x_0)] \wedge xQz,$$

was eine zulässige gebundene Umbennenung darstellt. Würden wir die Variable x in x_0 umbenennen, wäre die ehemals freie Variable nun gebunden, was unzulässig ist. Würden wir die Variable x in y umbenennen, entstünde ein Wort, das keinen Ausdruck darstellt.

Von einem Ausdruck A kann man durch eine Folge gebundener Umbenennungen stets zu einem Ausdruck A' übergehen, in dem alle in A rel-freien Variablen sogar abs-frei vorkommen. Alle in A' abs-freien Variablen können am Anfang quantifiziert werden. Verwendet man dafür den All-Quantor, so spricht man von der **All-Quantifizierten** $\mathsf{All}(A')$; wird der Ex-Quantor verwendet, spricht man von der **Ex-Quantifizierten** $\mathsf{Ex}(A')$. Ein Ausdruck A heißt **aussagenlogisch einfach**, falls er mit aussagenlogischen Methoden nicht zerlegbar ist, d. h. falls er ein relationaler Ausdruck ist oder mit einem Quantorsymbol beginnt, dessen Wirkungsbereich der gesamte Ausdruck ist. Zwischen den Aussagen aus der Aussagenlogik und den S-Ausdrücken gibt es folglich einen engen Zusammenhang: Jedem S-Ausdruck A ist in folgender Weise ein aussagenlogischer Ausdruck, seine aussagenlogische Struktur $\mathsf{ausl}(A)$ zugeordnet:

- Jedem quantifizierten Teilausdruck von A, der nicht zum Wirkungsbereich einer anderen Quantifizierung gehört, wird eine Aussagenvariable zugeordnet, so dass gleichen quantifizierten Teilausdrücken die gleiche Aussagenvariable und verschiedenen quantifizierten Teilausdrücken auch verschiedene Aussagenvariable zugeordnet sind.

- Jedem relationalen Teilausdruck aus A, der nicht im Wirkungsbereich einer Quantifizierung auftritt, wird eine noch nicht verwendete Aussagenvariable zugeordnet, wobei gleichen relationalen Teilausdrücken nur eine Aussagenvariable zuzuordnen ist.

Als Beispiel wählen wir den Ausdruck

$$A = (\exists x xPy \wedge xQy) \to [\neg \exists x xPy \vee \forall y(yQy \to xPy)].$$

Die aussagenlogische Struktur von A liefert uns den aussagenlogischen Ausdruck

$$\mathsf{ausl}(A) = (p \wedge q) \to (\neg p \vee r).$$

Der Ausdruck A entsteht aus $\mathsf{ausl}(A)$, indem wir

$$p = \exists x xPy, \quad q = xQy, \quad r = \forall y(yQy \to xPy)$$

setzen.

2.3. Interpretation der Terme und Ausdrücke

Es seien eine Signatur S und eine nichtleere Trägermenge U gegeben.
Eine S-**Interpretation** in U ist eine Abbildung ω mit folgenden Eigenschaften:

- Für jedes Konstantensymbol $a \in S$ ist $\omega(a)$ ein Element aus U.
- Für jedes m-stellige Relationssymbol P ist $\omega(P)$ eine m-stellige Relation auf U.
- Für jedes n-stellige Operationssymbol f ist $\omega(f)$ eine n-stellige Operation auf U.

Für $\omega(a), \omega(P), \omega(f)$ schreiben wir abkürzend $a^\omega, P^\omega, f^\omega$. Dann ist

$$\mathscr{U} = (U; \{\, a^\omega \mid a \in S \,\}; \{\, f^\omega \mid f \in S \,\}; \{\, P^\omega \mid P \in S \,\})$$

eine algebraische Struktur, wie sie aus der Algebra bekannt ist; wir nennen sie einfach S-Algebra $\mathscr{U}$. Insbesondere können wir die Begriffe Homomorphismus, Isomorphismus und den Homomorphiesatz hier verwenden. Die Ausdrücke unserer Sprache $\mathscr{L}^S$ sollen nun in einer S-Algebra $\mathscr{U}$ interpretiert und ihnen ein Wahrheitswert zugewiesen werden. Dazu gehen wir schrittweise vor. Unter einer **Belegung** der Variablen mit Elementen aus U verstehen wir eine Abbildung α, die jeder Variablen $x \in \mathscr{A}$ genau ein $\alpha(x) = x^\alpha \in U$ zuordnet. Mit Hilfe einer Belegung α können wir induktiv jeden Term $t \in \mathscr{T}^S$ in der S-Algebra $\mathscr{U}$ interpretieren, indem wir die Interpretation ω in natürlicher Weise auf Terme ausdehnen.

1. Atomare Werte:
   - Ist der Term $t \in \mathscr{T}^S$ eine Variable x, so gilt $\omega(t, \alpha) = x^\alpha$.
   - Ist der Term t ein Konstantensymbol $a \in S$, so ist $\omega(t, \alpha) = a^\omega$.
2. Abgeleitete Werte:
   - Für einen Term $f(t_1, \ldots, t_n) \in \mathscr{T}^S$ gilt

     $$\omega(f(t_1, \ldots, t_n), \alpha) = f^\omega(\omega(t_1, \alpha), \ldots, \omega(t_n, \alpha)).$$
3. Zu jedem Term $t \in \mathscr{T}^S$ gibt es eine natürliche Zahl m, so dass der Wert $\omega(t, \alpha)$ durch m-malige Anwendung von 2. aus den atomaren Werten erhalten werden kann.

Damit ist für jeden Term $t \in \mathscr{T}^S$ die Größe $\omega(t,\alpha)$ bei jeder Belegung α ein wohlbestimmtes Element aus dem Träger U. Als Beispiel seien etwa

$$S = \{\, a, f, g, P, Q \,\}, \quad \mathscr{U} = (\mathbb{N}; 1; +, \cdot; \leqq, >).$$

Für den Term $t = f\,\{\, x, g[f(y,a), f(y,a)]\,\}$ erhält man bei einer beliebigen Belegung α:

$$\omega(t,\alpha) = x^\alpha + (y^\alpha + a^\omega)^2 = x^\alpha + (y^\alpha + 1)^2,$$

woraus man leicht den Wert berechnen kann. Die Frage, wie sich der Wert eines Terms bei einer homomorphen Abbildung der S-Algebra $\mathscr{U}$ verändert, wird durch den nächsten Satz geklärt.

2.2. Wertübertragung bei homomorphen Abbildungen: *Es seien*

$$\mathscr{U}_1 = (U_1, \omega_1), \quad \mathscr{U}_2 = (U_2, \omega_2)$$

homomorphe S-Algebren, φ ein Homomorphismus von $\mathscr{U}_1$ auf $\mathscr{U}_2$, α eine Belegung aus U_1 und α^φ die in U_2 induzierte Belegung, d. h. $x^{\alpha^\varphi} = \varphi(x^\alpha)$.
Dann gilt für jeden Term $t \in \mathscr{T}^S :\ \varphi(\omega_1(t,\alpha)) = \omega_2(t,\alpha^\varphi)$.

Beweis: Den Beweis dieser Aussage führen wir induktiv über den Termaufbau. Es sei α eine beliebige Belegung aus U_1. Ist t eine Variable x, so folgt

$$\varphi(\omega_1(t,\alpha)) = \varphi(x^\alpha) = x^{\alpha^\varphi} = \omega_2(t,\alpha^\varphi).$$

Ist t ein Konstantensymbol a, so schließen wir

$$\varphi(\omega_1(t,\alpha)) = \varphi(a^{\omega_1}) = a^{\omega_2} = \omega_2(t,\alpha^\varphi).$$

Damit ist der Induktionsanfang abgeschlossen.
Angenommen, für die Terme $t_1,\ldots,t_n$ ist die Behauptung richtig. Es sei f ein beliebiges n-stelliges Operationssymbol. Für den Term $t = f(t_1,\ldots,t_n)$ erhalten wir dann:

$$\begin{aligned}
\varphi(\omega_1(t,\alpha)) &= \varphi[f^{\omega_1}(\omega_1(t_1,\alpha),\ldots,\omega_1(t_n,\alpha))] \\
&= f^{\omega_2}[\varphi(\omega_1(t_1,\alpha)),\ldots,\varphi(\omega_1(t_n,\alpha))] \\
&= f^{\omega_2}(\omega_2(t_1,\alpha^\varphi),\ldots,\omega_2(t_n,\alpha^\varphi)) \\
&= \omega_2(t,\alpha^\varphi).
\end{aligned}$$

Damit gilt die Behauptung für alle Terme. ♣
Für eine beliebige Belegung α bezeichnen wir mit $\alpha^{x_1,\ldots,x_r}_{\xi_1,\ldots,\xi_r}$ diejenige Belegung, die der Variablen x_i den Wert ξ_i zuordnet ($i = 1,\ldots,r$) und sonst mit α übereinstimmt.
Die Verhältnisse zwischen dem Wert eines Terms vor und nach einer Termeinsetzung werden durch den folgenden Satz geklärt.

2.3. Wertübertragung bei Termeinsetzungen in Termen: *Es seien ω eine S-Interpretation in U und $\bar{t}(x)$ ein S-Term, in dem die Variable x vorkommt. Dann gilt für jeden S-Term t und jede Belegung α:*

$$\omega(\bar{t}(x|t),\alpha) = \omega(\bar{t}(x),\alpha^x_{\omega(t,\alpha)}).$$

Der induktive Beweis dieses Satzes über den Termaufbau von $\bar{t}(x)$ kann sehr leicht vom Leser geführt werden.
Wir können nun induktiv einem gegebenen S-Ausdruck A in einer S-Algebra $\mathscr{U}$ bei einer Belegung α der Variablen mit Werten aus U einen Wahrheitswert $\mathrm{ww}_{\mathscr{U}}(A,\alpha)$ zuordnen.

1. Relationale Ausdrücke:
   Für m beliebige Terme $t_1,\ldots,t_m \in \mathscr{T}^S$ und jedes m-stellige Relationssymbol R ist

$$\begin{aligned}\mathrm{ww}_{\mathscr{U}}(Rt_1\ldots t_m,\alpha) &= R^\omega\omega(t_1,\alpha)\ldots\omega(t_m,\alpha)\\ &= \begin{cases} W, \text{ falls } (\omega(t_1,\alpha),\ldots,\omega(t_m,\alpha)) \in R^\omega, \\ F, \text{ sonst.}\end{cases}\end{aligned} .$$

2. Abgeleitete Wahrheitswerte:

   - Aussagenlogische Ausdrücke: Für alle $A,B \in \mathscr{L}^S$ ist

$$\begin{aligned}\mathrm{ww}_{\mathscr{U}}(\neg A,\alpha) &= \mathrm{not}(\mathrm{ww}_{\mathscr{U}}(A,\alpha)),\\ \mathrm{ww}_{\mathscr{U}}(A\wedge B,\alpha) &= \mathrm{and}(\mathrm{ww}_{\mathscr{U}}(A,\alpha),\mathrm{ww}_{\mathscr{U}}(B,\alpha)),\\ \mathrm{ww}_{\mathscr{U}}(A\vee B,\alpha) &= \mathrm{or}(\mathrm{ww}_{\mathscr{U}}(A,\alpha),\mathrm{ww}_{\mathscr{U}}(B,\alpha)),\\ \mathrm{ww}_{\mathscr{U}}(A\rightarrow B,\alpha) &= \mathrm{seq}(\mathrm{ww}_{\mathscr{U}}(A,\alpha),\mathrm{ww}_{\mathscr{U}}(B,\alpha)),\\ \mathrm{ww}_{\mathscr{U}}(A\leftrightarrow B,\alpha) &= \mathrm{äq}(\mathrm{ww}_{\mathscr{U}}(A,\alpha),\mathrm{ww}_{\mathscr{U}}(B,\alpha)).\end{aligned}$$

   - Quantifizierte Ausdrücke: Für jeden Ausdruck $A(x) \in \mathscr{L}^S$ ist

$$\mathrm{ww}_{\mathscr{U}}(\forall x A(x),\alpha) = \begin{cases} W, & \text{falls für alle } \xi \in U \text{ gilt}\\ & \quad \mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_\xi) = W,\\ F, & \text{sonst.}\end{cases}$$

$$\mathrm{ww}_{\mathscr{U}}(\exists x A(x),\alpha) = \begin{cases} W, & \text{falls ein } \xi \in U \text{ existiert mit}\\ & \quad \mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_\xi) = W,\\ F, & \text{sonst.}\end{cases}$$

3. Zu jedem Ausdruck A existiert eine natürliche Zahl n, so dass man seinen Wahrheitswert mittels n-maliger Anwendung von 2. aus den atomaren Wahrheitswerten gewinnen kann.

Damit ist jedem S-Ausdruck A bezüglich einer S-Algebra $\mathscr{U}$ bei jeder Belegung α ein wohlbestimmter Wahrheitswert zugeordnet. Zwei S-Ausdrücke heißen **logisch äquivalent**, wenn sie bei jeder Interpretation und jeder Belegung den gleichen Wahrheitswert haben. Es ist klar, dass die Ausdrücke

$$\begin{aligned} A \wedge B &\text{ und } \neg(\neg A \vee \neg B), \\ A \rightarrow B &\text{ und } \neg A \vee B, \\ A \leftrightarrow B &\text{ und } \neg(A \vee B) \vee \neg(\neg A \vee \neg B), \\ \forall x A(x) &\text{ und } \neg \exists x \neg A(x) \end{aligned}$$

logisch äquivalent sind. Wir können daher im Alphabet auf die Funktoren $\wedge, \rightarrow, \leftrightarrow$ und den Quantor $\forall$ verzichten, ohne die Ausdrucksstärke der Sprache einzuschränken. Insbesondere können bei den induktiven Definitionen die entsprechenden Regeln weggelassen werden, so dass bei induktiven Beweisen nur noch die Regeln für $\neg, \vee, \exists$ nachgewiesen werden müssen.

2.4. Koinzidenzlemma: *Es sei ω_1 eine S_1-Interpretation in U, ω_2 eine S_2-Interpretation in U und $S = S_1 \cap S_2$. Dann gilt für jeden S-Term t, jeden S-Ausdruck A und jede Belegung α in U:*

- *Falls die in t auftretenden Symbole $s \in S$ gleich interpretiert werden, d. h. $s^{\omega_1} = s^{\omega_2}$ gilt, so ist $\omega_1(t,\alpha) = \omega_2(t,\alpha)$.*
- *Falls die in A auftretenden Symbole aus S gleich interpretiert werden, so ist mit den S-Algebren $\mathscr{U}_1 = (U,\omega_1) und \mathscr{U}_2 = (U,\omega_2)$*

$$ww_{\mathscr{U}_1}(A,\alpha) = ww_{\mathscr{U}_2}(A,\alpha).$$

Beweis: Der Beweis wird induktiv über den Termaufbau bzw. über die Ausdrucksstufe geführt. Führen wir zunächst den Beweis für Terme. Für den Induktionsanfang sei t ein Konstantensymbol a. Nach der Wertdefinition gilt dann $\omega_i(t,\alpha) = a^{\omega_i}$ und nach Voraussetzung ist $a^{\omega_1} = a^{\omega_2}$, womit wir die Gleichungskette

$$\omega_1(t,\alpha) = a^{\omega_1} = a^{\omega_2} = \omega_2(t,\alpha)$$

erhalten. Ist t eine Variable x, so folgt für jede Belegung α

$$\omega_1(t,\alpha) = x^{\alpha} = \omega_2(t,\alpha).$$

Es seien $t_1,\ldots,t_n$ Terme und f ein n-stelliges Operationssymbol; nach Induktionsvoraussetzung sei ferner

$$\omega_1(t_i,\alpha) = \omega_2(t_i,\alpha), \quad i = 1,\ldots,n.$$

Mit der Voraussetzung $f^{\omega_1} = f^{\omega_2}$ und der Induktionsvoraussetzung schließen wir:

$$\begin{aligned}\omega_1(t,\alpha) &= f^{\omega_1}(\omega_1(t_1,\alpha),\ldots,\omega_1(t_n,\alpha)\\ &= f^{\omega_1}(\omega_2(t_1,\alpha),\ldots,\omega_2(t_n,\alpha))\\ &= f^{\omega_2}(\omega_2(t_1,\alpha),\ldots,\omega_2(t_n,\alpha))\\ &= \omega_2(t,\alpha)\end{aligned}$$

Damit ist die erste Behauptung bewiesen.
Für die zweite Behauptung haben wir einen induktiven Beweis über die Ausdrucksstufe auszuführen. Ist A ein relationaler Ausdruck:

$$A = Rt_1 \ldots t_m,$$

so erhalten wir mit der Voraussetzung und der schon bewiesenen 1. Behauptung

$$\begin{aligned}\mathrm{ww}_{\mathscr{U}_1}(Rt_1\ldots t_m,\alpha) &= R^{\omega_1}\omega_1(t_1,\alpha)\ldots\omega_1(t_m,\alpha)\\ &= R^{\omega_2}\omega_2(t_1,\alpha)\ldots\omega_2(t_m,\alpha)\\ &= \mathrm{ww}_{\mathscr{U}_2}(Rt_1\ldots t_m,\alpha).\end{aligned}$$

Für den Induktionsschritt haben wir die Fälle $\neg A, A \vee B, \exists x A(x)$ zu untersuchen.
Fall $\neg A$: Mit der Induktionsvoraussetzung folgt

$$\begin{aligned}\mathrm{ww}_{\mathscr{U}_1}(\neg A,\alpha) &= \mathrm{not}(\mathrm{ww}_{\mathscr{U}_1}(A,\alpha))\\ &= \mathrm{not}(\mathrm{ww}_{\mathscr{U}_2}(A,\alpha))\\ &= \mathrm{ww}_{\mathscr{U}_2}(\neg A,\alpha).\end{aligned}$$

Fall $A \vee B$: Mit der Induktionsvoraussetzung ergibt sich sofort

$$\begin{aligned}\mathrm{ww}_{\mathscr{U}_1}(A\vee B,\alpha) &= \mathrm{or}(\mathrm{ww}_{\mathscr{U}_1}(A,\alpha),\mathrm{ww}_{\mathscr{U}_1}(B,\alpha))\\ &= \mathrm{or}(\mathrm{ww}_{\mathscr{U}_2}(A,\alpha),\mathrm{ww}_{\mathscr{U}_2}(B,\alpha))\\ &= \mathrm{ww}_{\mathscr{U}_2}(A\vee B,\alpha).\end{aligned}$$

Fall $\exists x A(x)$: Falls ein $\xi \in U$ mit

$$\mathrm{ww}_{\mathscr{U}_1}(A(x),\alpha^x_\xi) = W$$

existiert, folgt einerseits $\mathrm{ww}_{\mathscr{U}_1}(\exists x A(x),\alpha) = W$ und wegen der Induktionsvoraussetzung gilt

$$\begin{aligned}W &= \mathrm{ww}_{\mathscr{U}_1}(A(x),\alpha^x_\xi) = \mathrm{ww}_{\mathscr{U}_2}(A(x),\alpha^x_\xi)\\ &= \mathrm{ww}_{\mathscr{U}_2}(\exists x A(x),\alpha),\end{aligned}$$

also zusammen $\mathrm{ww}_{\mathscr{U}_1}(\exists x A(x), \alpha) = W = \mathrm{ww}_{\mathscr{U}_2}(\exists x A(x), \alpha)$. Ganz analog behandelt man den anderen Fall. ♣

Damit ist insbesondere gezeigt, dass sowohl der Wert eines S-Terms als auch der Wahrheitswert eines S-Ausdrucks nur von der Interpretation für die im Ausdruck wirklich auftretenden Konstanten-, Relations- und Operationssymbole sowie von den Werten der Belegung für die im Ausdruck rel-frei vorkommenden Variablen abhängt. Enthält der Ausdruck keine rel-freien Variablen, so ist er eine Aussage (ein Satz) und sein Wahrheitswert hängt nicht von einer Belegung α ab.

Der folgende Satz begründet, warum die Termeinsetzung in einem Ausdruck nur eingeschränkt möglich ist.

2.5. Wahrheitswerte bei Termeinsetzung: *Es sei $A(x)$ ein S-Ausdruck. Dann gilt für jede S-Algebra $\mathscr{U} = (U, \omega)$, jeden zulässigen Term t und jede Belegung α in U:*

$$\mathrm{ww}_{\mathscr{U}}(A(x|t), \alpha) = \mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_{\omega(t,\alpha)}).$$

Beweis: Der Satz wird induktiv über die Ausdrucksstufe von $A(x)$ bewiesen. Für den Induktionsanfang haben wir relationale Ausdrücke zu untersuchen. Ist $A(x)$ ein relationaler Ausdruck der Form $Rt_1(x) \ldots t_m(x)$, so erhalten wir mit dem Satz über die Wertübertragung bei Termeinsetzung in Termen

$$\begin{aligned}
\mathrm{ww}_{\mathscr{U}}(Rt_1(x|t) \ldots t_m(x|t), \alpha) &= R^\omega \omega(t_1(x|t), \alpha) \ldots \omega(t_m(x|t), \alpha) \\
&= R^\omega \omega(t_1(x), \alpha^x_{\omega(t,\alpha)}) \ldots \omega(t_m(x), \alpha^x_{\omega(t,\alpha)}) \\
&= \mathrm{ww}_{\mathscr{U}}(Rt_1(x) \ldots t_m(x), \alpha^x_{\omega(t,\alpha)}).
\end{aligned}$$

Damit ist der Induktionsanfang abgeschlossen.

Den Induktionsschluss zeigen wir nur für die Funktoren $\neg, \vee$ und den Quantor $\exists$. Es möge etwa der Ausdruck $\neg A$ vorliegen und t sei ein zulässiger Term für eine Termeinsetzung von x. Nach Induktionsvoraussetzung gilt

$$\mathrm{ww}_{\mathscr{U}}(A(x|t), \alpha) = \mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_{\omega(t,\alpha)})$$

und daher

$$\begin{aligned}
\mathrm{ww}_{\mathscr{U}}(\neg A(x|t), \alpha) &= \mathrm{not}(\mathrm{ww}_{\mathscr{U}}(A(x|t), \alpha)) \\
&= \mathrm{not}(\mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_{\omega(t,\alpha)})) \\
&= \mathrm{ww}_{\mathscr{U}}(\neg A(x), \alpha^x_{\omega(t,\alpha)}).
\end{aligned}$$

Liegt ein Ausdruck der Form $A(x) \vee B(x)$ vor, haben wir als Induktionsvoraussetzung die beiden Gleichungen

$$\begin{aligned}
\mathrm{ww}_{\mathscr{U}}(A(x|t), \alpha) &= \mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_{\omega(t,\alpha)}) \\
\mathrm{ww}_{\mathscr{U}}(B(x|t), \alpha) &= \mathrm{ww}_{\mathscr{U}}(B(x), \alpha^x_{\omega(t,\alpha)}),
\end{aligned}$$

womit wir schließen

$$\begin{aligned}
\mathrm{ww}_{\mathscr{U}}(A(x|t) \vee B(x|t), \alpha) &= \mathrm{or}(\mathrm{ww}_{\mathscr{U}}(A(x|t), \alpha), \mathrm{ww}_{\mathscr{U}}(B(x|t), \alpha)) \\
&= \mathrm{or}(\mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_{\omega(t,\alpha)}), \mathrm{ww}_{\mathscr{U}}(B(x), \alpha^x_{\omega(t,\alpha)})) \\
&= \mathrm{ww}_{\mathscr{U}}(A(x) \vee B(x), \alpha^x_{\omega(t,\alpha)})).
\end{aligned}$$

Es bleibt noch der Fall, dass der vorgelegte Ausdruck ex-quantifiziert ist. Es sei also der Ausdruck $\exists y A(x,y)$ gegeben. Nach Induktionsvoraussetzung gilt

$$\mathrm{ww}_{\mathscr{U}}(A(x|t,y), \alpha) = \mathrm{ww}_{\mathscr{U}}(A(x,y), \alpha^x_{\omega(t,\alpha)}).$$

Da t ein zulässiger Term ist, kommt die Variable y nicht in t vor. Daher gilt für jedes $\eta \in U$:

$$\omega(t, \alpha^y_\eta) = \omega(t, \alpha)$$

und daher mit der Induktionsvoraussetzung

$$\mathrm{ww}_{\mathscr{U}}(A(x|t,y), \alpha^y_\eta) = \mathrm{ww}_{\mathscr{U}}(A(x,y), \alpha^{yx}_{\eta\omega(t,\alpha)}),$$

also

$$\begin{aligned}
\mathrm{ww}_{\mathscr{U}}(\exists y A(x|t,y), \alpha) &= \begin{cases} W, & \text{falls ein } \eta \in U \text{ existiert mit} \\ & \mathrm{ww}_{\mathscr{U}}(A(x|t,y), \alpha^y_\eta) = W, \\ F, & \text{sonst.} \end{cases} \\
&= \begin{cases} W, & \text{falls ein } \eta \in U \text{ existiert mit} \\ & \mathrm{ww}_{\mathscr{U}}(A(x,y), \alpha^{yx}_{\eta\omega(t,\alpha)}) = W, \\ F, & \text{sonst.} \end{cases} \\
&= \mathrm{ww}_{\mathscr{U}}(\exists y A(x,y), \alpha^x_{\omega(t,\alpha)}).
\end{aligned}$$

Damit ist der Satz bewiesen. ♣

Wir beweisen nun, dass die gebundene Umbenennung zu keiner Änderung des Wahrheitswertes für einen Ausdruck führt.

2.6. Invarianz des Wahrheitswertes bei gebundener Umbennung: *Wenn ein Ausdruck A durch eine zulässige gebundene Umbenennung in den Ausdruck A' übergeht, so ist bei jeder Interpretation ω und jeder Belegung α in einer Trägermenge U*

$$\mathrm{ww}_{\mathscr{U}}(A, \alpha) = \mathrm{ww}_{\mathscr{U}}(A', \alpha).$$

Beweis: Der Beweis hierfür erfolgt wieder durch vollständige Induktion über die Ausdrucksstufe von A. Ist A ein relationaler Ausdruck, dann muss nichts bewiesen werden, da in diesen Fällen keine gebundene Umbenennung möglich ist. Für die aussagenlogischen Funktoren ist der Beweis sehr einfach und soll dem Leser überlassen bleiben. Es sei der Ausdruck $\exists x A(x)$ vorgelegt und eine gebundene Variable y werde in z umbenannt, so dass der Ausdruck $\exists x A'(x)$ entsteht. Da die zulässige gebundene Umbenennung im Wirkungsbereich der Quantifizierung von x erfolgt, kommt die Variable x im Ausdruck $A'(x)$ abs-frei vor. Nach Induktionsvoraussetzung ist für jede Belegung α in U:

$$\mathrm{ww}_{\mathscr{U}}(A(x),\alpha) = \mathrm{ww}_{\mathscr{U}}(A'(x),\alpha),$$

also auch für jedes $\xi \in U$

$$\mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_\xi) = \mathrm{ww}_{\mathscr{U}}(A'(x),\alpha^x_\xi),$$

woraus

$$\mathrm{ww}_{\mathscr{U}}(\exists x A(x),\alpha^x_\xi) = \mathrm{ww}_{\mathscr{U}}(\exists x A'(x),\alpha^x_\xi)$$

folgt. Wird dagegen die quantifizierte Variable x in y umbenannt, so erhält man den neuen Ausdruck $\exists y A(y)$. Da die neue Variable y nicht im Wirkungsbereich der Quantifizierung von x vorkommen darf, kann sie nicht in $A(x)$ vorkommen, so dass der Übergang von $A(x)$ zu $A(x|y)$ eine zulässige Termeinsetzung darstellt. Nach der Wahrheitswertübertragung bei Termeinsetzung in einem Ausdruck gilt aber für jede Belegung α:

$$\mathrm{ww}_{\mathscr{U}}(A(x|y),\alpha) = \mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_{y^\alpha}).$$

Daraus folgt für jedes $\xi \in U$

$$\begin{aligned}\mathrm{ww}_{\mathscr{U}}(A(x|y),\alpha^y_\xi) &= \mathrm{ww}_{\mathscr{U}}(A(x|y),\alpha^{xy}_{\xi\xi}) \\ &= \mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_\xi),\end{aligned}$$

da y nicht in $A(x)$ vorkommt, also

$$\mathrm{ww}_{\mathscr{U}}(\exists y A(x|y),\alpha) = \mathrm{ww}_{\mathscr{U}}(\exists x A(x),\alpha),$$

womit der Satz bewiesen ist. ♣

Jeder Ausdruck A ist ein Ausdruck über einer Signatur $S(A)$, die dadurch entsteht, dass man in $S(A)$ alle im Ausdruck A auftretenden Symbole aus S zusammenfasst. Entsprechend erhält man dazu eine Unteralgebra $\mathscr{U}(A) = (U,\omega_A)$ der S-Algebra $\mathscr{U} = (U,\omega)$, indem man die Interpretation ω auf $S(A)$ einschränkt. Dabei wird der Wert $\mathrm{ww}_{\mathscr{U}}(A,\alpha)$ offenbar nicht geändert.

Für die Interpretation eines Ausdrucks in homomorphen S-Algebren gilt

2.7. Invarianz des Wahrheitswertes bei einem Homomorphismus: *Ist φ ein Homomorphismus der S-Algebra $\mathscr{U}_1$ auf die S-Algebra $\mathscr{U}_2$, so gilt für jeden Ausdruck A und jede Belegung α aus U_1:* $\mathrm{ww}_{\mathscr{U}_1}(A,\alpha) = \mathrm{ww}_{\mathscr{U}_2}(A,\alpha^\varphi)$.

Den induktiven Beweis über die Ausdrucksstufe führt man analog zu oben. Insbesondere besagt dieser Satz: Der Wahrheitswert eines interpretierten S-Ausdrucks ändert sich beim Übergang zu einer homomorphen Struktur nicht.
In Analogie zur Aussagenlogik führen wir nun die grundlegenden Begriffe Erfüllbarkeit und Allgemeingültigkeit ein, die auf dem Wahrheitswert eines S-Ausdrucks beruhen; dieser wiederum konnte nur auf der Grundlage einer S-Algebra vergeben werden. Daher wird sich die Erfüllbarkeit bzw. Allgemeingültigkeit eines Ausdrucks zunächst auf eine S-Algebra beziehen müssen. Ein S-Ausdruck A heißt in einer S-Algebra $\mathscr{U} = (U,\omega)$ **erfüllbar**, wenn es eine Belegung α aus U derart gibt, dass $\mathrm{ww}_{\mathscr{U}}(A,\alpha) = W$ gilt. Wir nennen einen Ausdruck **allgemeingültig** in $\mathscr{U}$, wenn er durch jede Belegung erfüllt wird. Mit $\mathsf{erf}^S(\mathscr{U})$ und $\mathsf{ag}^S(\mathscr{U})$ bezeichnen wir die Menge aller in $\mathscr{U}$ erfüllbaren bzw. allgemeingültigen Ausdrücke. Über die Erfüllbarkeitsmenge gelten u. a. die folgenden, unmittelbar einsichtigen Aussagen:

$$\begin{aligned}
Rt_1\dots t_m \in \mathsf{erf}^S(\mathscr{U}) &\iff \text{es gibt eine Belegung } \alpha \text{ und}\\
&\qquad (\omega(t_1,\alpha),\dots,\omega(t_m,\alpha)) \in R^\omega,\\
\neg A \in \mathsf{erf}^S(\mathscr{U}) &\iff \text{es gibt eine Belegung } \alpha \text{ und } \mathrm{ww}_{\mathscr{U}}(A,\alpha) = F,\\
A \wedge B \in \mathsf{erf}^S(\mathscr{U}) &\iff \text{es gibt eine Belegung } \alpha \text{ und}\\
&\qquad \mathrm{ww}_{\mathscr{U}}(A,\alpha) = \mathrm{ww}_{\mathscr{U}}(B,\alpha) = W,\\
A \vee B \in \mathsf{erf}^S(\mathscr{U}) &\iff A \in \mathsf{erf}^S(\mathscr{U}) \text{ oder } B \in \mathsf{erf}^S(\mathscr{U}),\\
(A \to B) \in \mathsf{erf}^S(\mathscr{U}) &\iff \text{es gibt eine Belegung } \alpha \text{ und}\\
&\qquad \text{aus } \mathrm{ww}_{\mathscr{U}}(A,\alpha) = W \text{ folgt } \mathrm{ww}_{\mathscr{U}}(B,\alpha) = W,\\
\forall x A(x) \in \mathsf{erf}^S(\mathscr{U}) &\iff \text{es gibt eine Belegung } \alpha \text{ und für alle } \xi \in U \text{ gilt}\\
&\qquad \mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_\xi) = W,\\
\exists x A(x) \in \mathsf{erf}^S(\mathscr{U}) &\iff \text{es gibt eine Belegung } \alpha \text{ und für ein } \xi \in U \text{ gilt}\\
&\qquad \mathrm{ww}_{\mathscr{U}}(A(x),\alpha^x_\xi) = W.
\end{aligned}$$

Jeder in einer S-Algebra $\mathscr{U}$ allgemeingültige Ausdruck ist auch in $\mathscr{U}$ erfüllbar:

$$\mathsf{ag}^S(\mathscr{U}) \subseteqq \mathsf{erf}^S(\mathscr{U}).$$

2.8. Beziehungstheorem: *Hinsichtlich Allgemeingültigkeit und Erfüllbarkeit gelten die folgenden Beziehungen:*

1. $A \in \mathsf{ag}^S(\mathscr{U}) \iff \neg A \notin \mathsf{erf}^S(\mathscr{U})$.

2. $A \in \mathsf{erf}^S(\mathscr{U}) \iff \neg A \notin \mathsf{ag}^S(\mathscr{U})$.
3. $(A \wedge B) \in \mathsf{ag}^S(\mathscr{U}) \iff A \in \mathsf{ag}^S(\mathscr{U})$ *und* $B \in \mathsf{ag}^S(\mathscr{U})$.
4. *Wenn* $A \in \mathsf{ag}^S(\mathscr{U})$ *oder* $B \in \mathsf{ag}^S(\mathscr{U})$, *so* $(A \vee B) \in \mathsf{ag}^S(\mathscr{U})$.
5. *Wenn* $(A \to B) \in \mathsf{ag}^S(\mathscr{U})$ *und* $A \in \mathsf{ag}^S(\mathscr{U})$, *so* $B \in \mathsf{ag}^S(\mathscr{U})$.
6. *Wenn* $(A \leftrightarrow B) \in \mathsf{ag}^S(\mathscr{U})$, *so gilt* $A \in \mathsf{ag}^S(\mathscr{U}) \iff B \in \mathsf{ag}^S(\mathscr{U})$.
7. *Wenn* $(A \wedge B) \in \mathsf{erf}^S(\mathscr{U})$, *so* $A \in \mathsf{erf}^S(\mathscr{U})$ *und* $B \in \mathsf{erf}^S(\mathscr{U})$.
8. $\forall x A(x) \in \mathsf{ag}^S(\mathscr{U}) \iff A(x) \in \mathsf{ag}^S(\mathscr{U})$.
9. $\exists x A(x) \in \mathsf{erf}^S(\mathscr{U}) \iff A(x) \in \mathsf{erf}^S(\mathscr{U})$.
10. *Wenn* $A(x) \in \mathsf{ag}^S(\mathscr{U})$, *so* $\exists x A(x) \in \mathsf{ag}^S(\mathscr{U})$.
11. *Wenn* $\forall x A(x) \in \mathsf{erf}^S(\mathscr{U})$, *so* $A(x) \in \mathsf{erf}^S(\mathscr{U})$.

sind unmittelbar einsichtig. Exemplarisch beweisen wir die Beziehung 9. Dazu sei $\exists x A(x) \in \mathsf{erf}^S(\mathscr{U})$, d. h. es gibt eine Belegung α in U mit $\mathrm{ww}_{\mathscr{U}}(\exists x A(x), \alpha) = W$. Folglich gibt es ein $\xi \in U$ mit $\mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_\xi) = W$, womit bereits eine verifizierende Belegung für den Ausdruck $A(x)$ gefunden ist. Ist umgekehrt $A(x)$ erfüllbar, so gilt für eine gewisse Belegung α:

$$\mathrm{ww}_{\mathscr{U}}(A(x), \alpha) = W.$$

Bei dieser Belegung wird die Variable x mit $\xi = x^\alpha$ belegt; außerdem gilt $\alpha = \alpha^x_\xi$, woraus zusammen mit der Wahrheitswertdefinition

$$W = \mathrm{ww}_{\mathscr{U}}(A(x), \alpha) = \mathrm{ww}_{\mathscr{U}}(A(x), \alpha^x_\xi) = \mathrm{ww}_{\mathscr{U}}(\exists x A(x), \alpha)$$

folgt. ♣

Ein Ziel der mathematischen Logik ist es, das logische Schließen innerhalb der Mathematik zu modellieren, d. h. die in mathematischen Beweisen üblichen Schlussweisen zu begründen. Innerhalb der Sprache $\mathscr{L}^S$ widerspiegeln sich die mathematischen Schlussweisen in formalen Schlussregeln, die die Eigenschaft haben, dass man aus allgemeingültigen Ausdrücken mittels dieser Schlussregeln stets wieder allgemeingültige Ausdrücke erhält. Der folgende Satz fasst die in der Sprache $\mathscr{L}^S$ geltenden formalen Schlussregeln zusammen.

2.9. Satz: *Für allgemeingültige Ausdrücke gelten die folgenden 7 Schlussregeln.*

- **Abtrennungsregel:**
  Aus $A \in \mathsf{ag}^S(\mathscr{U})$ *und* $(A \to B) \in \mathsf{ag}^S(\mathscr{U})$ *folgt* $B \in \mathsf{ag}^S(\mathscr{U})$.
- **Vordere All-Quantifizierung:**
  Aus $(A(x) \to B) \in \mathsf{ag}^S(\mathscr{U})$ *folgt* $(\forall x A(x) \to B) \in \mathsf{ag}^S(\mathscr{U})$.

- **Hintere Ex-Quantifizierung:**
  $(A \to B(x)) \in \mathsf{ag}^S(\mathscr{U})$ *folgt* $(A \to \exists x B(x)) \in \mathsf{ag}^S(\mathscr{U})$.
- **Hintere All-Quantifizierung:**
  Es sei A *ein Ausdruck, in dem die Variable* x *nicht vorkommt. Dann folgt aus* $(A \to B(x)) \in \mathsf{ag}^S(\mathscr{U})$ *stets, dass* $(A \to \forall x B(x)) \in \mathsf{ag}^S(\mathscr{U})$.
- **Vordere Ex-Quantifizierung:**
  Es sei B *ein* S*-Ausdruck, in dem die Variable* x *nicht vorkommt. Dann folgt aus* $(A(x) \to B) \in \mathsf{ag}^S(\mathscr{U})$*, dass auch* $(\exists x A(x) \to B) \in \mathsf{ag}^S(\mathscr{U})$ *gilt.*
- **Termeinsetzung für abs-freie Variable:** *Für jeden für* A *zulässigen Term* t *folgt aus* $A(x) \in \mathsf{ag}^S(\mathscr{U})$*, dass* $A(x|t) \in \mathsf{ag}^S(\mathscr{U})$ *gilt.*
- **Gebundene Umbenennung:** *Wenn* $A \in \mathsf{ag}^S(\mathscr{U})$ *und* A *durch eine zulässige gebundene Umbenennung in einen* S*-Ausdruck* A' *übergeht, so gilt auch* $A' \in \mathsf{ag}^S(\mathscr{U})$.

Beweis: Die Abtrennungsregel ist die 5. Beziehung aus dem Beziehungstheorem. Wir zeigen die Regel der vorderen All-Quantifizierung. Angenommen, sie ist falsch. Dann gibt es eine Belegung α mit

$$\mathrm{ww}_{\mathscr{U}}(A(x) \to B, \alpha) = W, \quad \mathrm{ww}_{\mathscr{U}}(\forall x A(x) \to B, \alpha) = F.$$

Daraus folgt

$$\mathrm{ww}_{\mathscr{U}}(\forall x A(x), \alpha) = W, \quad \mathrm{ww}_{\mathscr{U}}(B, \alpha) = F.$$

Mit der Voraussetzung $\mathrm{ww}_{\mathscr{U}}(A(x) \to B, \alpha) = W$ folgt daraus, dass

$$\mathrm{ww}_{\mathscr{U}}(A(x), \alpha) = F$$

gilt, was aber offensichtlich unmöglich sein kann. Dieser Widerspruch beweist die vordere All-Quantifizierung.
Zum Beweis der hinteren Ex-Quantifizierung nehmen wir an, die Behauptung wäre falsch. Dann gibt es eine Belegung α mit

$$\mathrm{ww}_{\mathscr{U}}(A, \alpha) = W, \quad \mathrm{ww}_{\mathscr{U}}(\exists x B(x), \alpha) = F.$$

Die letzte Gleichung besagt, dass es kein $\xi \in U$ gibt mit $\mathrm{ww}_{\mathscr{U}}(B(x), \alpha^x_\xi) = W$, d. h. für alle $\xi \in U$ ist $\mathrm{ww}_{\mathscr{U}}(B(x), \alpha^x_\xi) = F$, also $\mathrm{ww}_{\mathscr{U}}(B(x), \alpha) = F$, woraus wegen $(A \to B(x)) \in \mathsf{ag}^S(\mathscr{U})$ sofort folgt, dass $\mathrm{ww}_{\mathscr{U}}(A, \alpha) = F$ gilt. Dieser Widerspruch beweist die hintere Ex-Quantifizierung.
Für den Beweis der hinteren All-Quantifizierung sei α eine beliebige Belegung; nach Voraussetzung gilt

$$\mathrm{ww}_{\mathscr{U}}(A \to B(x)), \alpha) = W.$$

Nehmen wir nun an, dass die Behauptung nicht gilt:

$$\mathrm{ww}_{\mathscr{U}}(A \to \forall x B(x)), \alpha) = F.$$

Dann ist $\mathrm{ww}_{\mathscr{U}}(A,\alpha) = W$ und es existiert ein $\xi \in U$ mit

$$\mathrm{ww}_{\mathscr{U}}(B(x), \alpha_\xi^x) = F.$$

Da die Variable x im Ausdruck A nicht vorkommt, stimmen die Belegungen α und α_ξ^x auf dem Ausdruck A überein, so dass

$$\mathrm{ww}_{\mathscr{U}}(A, \alpha_\xi^x) = \mathrm{ww}_{\mathscr{U}}(A, \alpha) = W.$$

Mit der Voraussetzung erhalten wir daraus:

$$W = \mathrm{ww}_{\mathscr{U}}(A \to B(x), \alpha_\xi^x) = \mathsf{seq}(\mathrm{ww}_{\mathscr{U}}(A,\alpha), \mathrm{ww}_{\mathscr{U}}(B(x), \alpha_\xi^x)) = \mathsf{seq}(W,F) = F,$$

was sicherlich unmöglich ist.
Die vordere Ex-Quantifizierung wird nach dem gleichen Schema bewiesen.
Die Schlussregel der Termeinsetzung für abs-freie Variable folgt direkt aus dem Satz über die Wahrheitswertübertragung bei Termeinsetzung.
Die Regel der gebundenen Umbenennung folgt aus dem Satz über die Wahrheitswertinvarianz bei gebundener Umbenennung. ♣
Die Untersuchung allgemeingültiger Ausdrücke in einer konkreten S-Algebra ist natürlich nicht Gegenstand der mathematischen Logik, sondern einer mathematischen Theorie dieser Algebra vorbehalten. Hier interessieren wir uns für jene Ausdrücke und Sätze, die in allen Algebren gelten.
Ein S-Ausdruck A heißt **allgemeingültig** in einer Trägermenge U, wenn er in einer beliebigen S-Algebra $\mathscr{U} = (U, \omega)$ allgemeingültig ist. Dabei sei $\mathsf{ag}^S(U)$ die Menge aller in U allgemeingültigen S-Ausdrücke. Ein S-Ausdruck A heißt **erfüllbar** in U, wenn es eine S-Algebra $\mathscr{U} = (U, \omega)$ gibt, in der A erfüllbar ist. Mit $\mathsf{erf}^S(U)$ wird die Menge aller in U erfüllbaren Ausdrücke bezeichnet. Schließlich sei ag^S die Menge aller S-Ausdrücke, die in jeder Trägermenge allgemeingültig sind; entsprechend sei erf^S die Menge aller S-Ausdrücke, die in mindestens einer Trägermenge erfüllbar sind. Demnach gelten die folgenden Inklusionen:

$$\mathsf{ag}^S \subseteqq \mathsf{ag}^S(U) \subseteqq \mathsf{ag}^S(\mathscr{U}) \subseteqq \mathsf{erf}^S(\mathscr{U}) \subseteqq \mathsf{erf}^S(U) \subseteqq \mathsf{erf}^S.$$

Für alle Arten der Allgemeingültigkeit und Erfüllbarkeit gelten insbesondere die 7 Schlussregeln in analoger Form.
Wenn wir mit Axa^S die Menge aller jener S-Ausdrücke bezeichnen, die man aus dem aussagenlogischen Axiomensystem Axa dadurch erhält, dass man für die dort auftretenden Aussagenvariablen gleichzeitig beliebige S-Ausdrücke einsetzt, so sind alle diese in jeder Trägermenge allgemeingültig: $\mathsf{Axa}^S \subseteqq \mathsf{ag}^S$. Im übernächsten Abschnitt verschaffen wir uns einen gewissen Überblick über allgemeingültige Ausdrücke in jeder Trägermenge.

2.4. Folgern, Ableiten, Beweisen

Das logische Folgern gehört zu den grundlegenden Begriffen der mathematischen Logik. Hierbei geht es darum zu modellieren, was ein Mathematiker tut, wenn er mathematische Sätze „folgert“. Dazu benötigen wir den Modellbegriff. Es sei $\mathscr{X} \subseteqq \mathscr{L}^S$ eine Menge von S-Ausdrücken der Sprache $\mathscr{L}^S$. Eine S-Algebra $\mathscr{U} = (U, \omega)$ heißt **Modell** für die Ausdrucksmenge $\mathscr{X}$, wenn jeder Ausdruck aus $\mathscr{X}$ allgemeingültig in $\mathscr{U}$ ist: $\mathscr{X} \subseteqq \mathsf{ag}^S(\mathscr{U})$. Der Modellbegriff stellt somit eine Relation zwischen einer Ausdrucksmenge und solchen algebraischen Strukturen her, in denen alle Ausdrücke der Menge so interpretiert werden können, dass aus ihnen wahre Sätze der Struktur werden. Damit können wir insbesondere sagen: Ein Ausdruck A ist genau dann allgemeingültig in $\mathscr{U}$, wenn $\mathscr{U}$ Modell der Einermenge $\{A\}$ ist, d. h. wenn $\mathscr{U}$ Modell für $\{\mathsf{All}(A)\}$ ist. Analog ist ein Ausdruck A genau dann erfüllbar in $\mathscr{U}$, wenn die Algebra $\mathscr{U}$ Modell für $\{\mathsf{Ex}(A)\}$ ist. Betrachten wir dazu einige Beispiele.
Es sei $S = \{e, \cdot\}$ mit einem zweistelligen Operationssymbol $\cdot$. Eine solche Signatur ist z. B. Grundlage der Gruppentheorie. Eine konkrete Halbgruppe ist dann Modell für die Ausdrucksmenge

$$\mathscr{H}(\cdot) = \{\forall x \forall y \forall z[(x \cdot y) \cdot z = x \cdot (y \cdot z)]\},$$

eine kommutative Halbgruppe ist Modell von

$$\mathscr{H}_k(\cdot) = \mathscr{H}(\cdot) \cup \{\forall x \forall y(x \cdot y = y \cdot x)\},$$

eine Gruppe ist Modell von

$$\mathscr{G}(e, \cdot) = \mathscr{H}(\cdot) \cup \{\forall x[e \cdot x = x], \forall x \exists y[y \cdot x = e]\}.$$

(Zur besseren Übersichtlichkeit haben wir in den Ausdrücken eigentlich unzulässige Klammern eingefügt.) Die kommutativen Gruppen sind Modelle von

$$\mathscr{G}_k(e, \cdot) = \mathscr{G}(e, \cdot) \cup \{\forall x \forall y(x \cdot y = y \cdot x)\}.$$

Wählt man als Signatur $S = \{o, +, \cdot\}$ mit zwei zweistelligen Operationssymbolen $\cdot$ und $+$, so ist ein kommutativer Ring Modell von

$$\mathscr{R}_k(o, +, \cdot) = \mathscr{G}_k(o, +) \cup \mathscr{H}_k(\cdot) \cup \{\forall (x, y, z)[x \cdot (y + z) = x \cdot y + x \cdot z]\}.$$

Wählt man schließlich als Signatur $S = \{o, e, +, \cdot\}$, dann ist ein Körper Modell der Ausdrucksmenge

$$\mathscr{K}(o, e, +, \cdot) = \mathscr{R}_k(o, +, \cdot) \cup \{\forall x(x \cdot e = x), \forall x[x \neq o \rightarrow \exists y(x \cdot y = e)], o \neq e\}.$$

Wir sagen, dass ein S-Ausdruck A aus $\mathscr{X}$ folgt, wenn jedes Modell für $\mathscr{X}$ auch Modell für $\{A\}$ ist, d. h. wenn A in jeder Algebra allgemeingültig ist, in der die Ausdrücke aus $\mathscr{X}$ allgemeingültig sind. Mit $\mathsf{Fl}^S(\mathscr{X})$ bezeichnen wir die Menge aller Ausdrücke, die aus $\mathscr{X}$ folgen. Dabei gilt offensichtlich

$$\mathscr{X} \subseteqq \mathsf{Fl}^S(\mathscr{X}).$$

Da im Falle $\mathscr{X}_1 \subseteqq \mathscr{X}_2$ jedes Modell für $\mathscr{X}_2$ auch Modell für $\mathscr{X}_1$ ist, gilt die Monotonie

$$\mathscr{X}_1 \subseteqq \mathscr{X}_2 \quad \Longrightarrow \quad \mathsf{Fl}^S(\mathscr{X}_1) \subseteqq \mathsf{Fl}^S(\mathscr{X}_2).$$

Jede Algebra ist Modell der leeren Menge; also folgt ein Ausdruck genau dann aus der leeren Menge, wenn er in jeder Algebra allgemeingültig ist:

$$\mathsf{Fl}^S(\emptyset) = \mathsf{ag}^S.$$

Daher ist die Folgerungsmenge der leeren Menge bezüglich der 7 Schlussregeln abgeschlossen, falls man diese als rein syntaktische Regeln auffasst. Man sieht leicht, dass dies für jede Folgerungsmenge gilt. Da ein Ausdruck A genau dann allgemeingültig in einer S-Algebra ist, wenn dies für seine All-Quantifizierte $\mathsf{All}(A)$ gilt, haben wir

$$A \in \mathsf{Fl}^S(\mathscr{X}) \Longleftrightarrow \mathsf{All}(A) \in \mathsf{Fl}^S(\mathscr{X}),$$

und damit

$$\mathsf{Fl}^S(\mathscr{X}) = \mathsf{Fl}^S(\mathsf{All}(\mathscr{X})),$$

wobei $\mathsf{All}(\mathscr{X})$ die Menge aller all-quantifizierten Ausdrücke aus $\mathscr{X}$ ist. Mithin kann man sich darauf beschränken, nur aus Aussagenmengen zu folgern und daraus auch nur Aussagen.

2.10. Abgeschlossenheit der Folgerungsmenge: *Die Folgerungsmenge jeder Menge von S-Ausdrücken ist abgeschlossen bezüglich des logischen Folgerns:*
Wenn $\mathscr{X} \subseteqq \mathscr{L}^S$, so $\mathsf{Fl}^S(\mathsf{Fl}^S(\mathscr{X})) \subseteqq \mathsf{Fl}^S(\mathscr{X})$.

Beweis: Wir zeigen zunächst, dass jedes Modell für $\mathscr{X}$ auch ein Modell für die Folgerungsmenge $\mathsf{Fl}^S(\mathscr{X})$ sein muss. Dazu sei $\mathscr{U}$ ein Modell für $\mathscr{X}$ und $A \in \mathsf{Fl}^S(\mathscr{X})$. Dann ist A allgemeingültig in $\mathscr{U}$, woraus wir schließen, dass $\mathscr{U}$ ein Modell für $\mathsf{Fl}^S(\mathscr{X})$ ist. Es sei nun $A \in \mathsf{Fl}^S(\mathsf{Fl}^S(\mathscr{X}))$; dann ist A sicher allgemeingültig in jedem Modell für $\mathsf{Fl}^S(\mathscr{X})$. Da aber jedes Modell für $\mathscr{X}$ auch Modell für deren Folgerungsmenge ist, muss A erst recht in jedem Modell für $\mathscr{X}$ allgemeingültig sein, d. h.

$A \in \mathsf{Fl}^S(\mathscr{X})$. ♣

Wir wollen versuchen, die allgemeingültigen Ausdrücke bzw. die Folgerungsmenge einer gegebenen Menge von Ausdrücken axiomatisch zu charakterisieren. In der Aussagenlogik war dies eine einfache Aufgabe, konnte man doch mittels Wahrheitstafel, Normalform oder Standardform entscheiden, ob ein Ausdruck allgemeingültig ist. Hier hat diese Frage grundsätzliche Bedeutung, da man in den meisten Fällen kein allgemeines Verfahren hat, um diese Frage in endlich vielen Schritten zu entscheiden. Es gibt nämlich Ausdrücke, die nur in einer unendlichen Algebra allgemeingültig sind.

Beispiel: Betrachten wir den Ausdruck

$$\forall x xRf(x) \wedge \forall x \neg xRx \wedge \forall x \forall y \forall z[(xRy \wedge yRz) \rightarrow xRz],$$

worin R ein zweistelliges Relationssymbol und f ein einstelliges Operationssymbol bedeuten sollen. Dieser Ausdruck wird im Bereich der natürlichen Zahlen $\mathbb{N}_0$ eine wahre Aussage, wenn man R als $<$-Beziehung und $f(x)$ als Nachfolger von x interpretiert: $f(x) = x+1$. Er lautet dann nämlich in ausgesprochener Form: „Für jedes $x \in \mathbb{N}_0$ ist $x < x+1$ und für kein $x \in \mathbb{N}_0$ gilt $x < x$ und für alle natürlichen Zahlen x, y, z gilt: Aus $x < y$ und $y < z$ folgt $x < z$“.

Nehmen wir an, dass der Ausdruck in einer endlichen Algebra $\mathscr{U} = (U, \omega)$ allgemeingültig ist. Für $m \in U$ betrachten wir die Folge

$$m_0 = m, \quad m_{i+1} = f^\omega(m_i), \quad i = 0, 1, 2, \ldots$$

Da U endlich ist, muss diese Folge enden; es existieren zwei natürliche Zahlen k, l mit $k < l$ und $m_k = m_l$. Wegen des ersten Teils im Ausdruck gilt $(m_i, m_{i+1}) \in R^\omega$; nach dem dritten Teil ist R^ω eine transitive Relation, also muss $(m_k, m_l) \in R^\omega$ sein, was aber wegen $m_k = m_l$ dem zweiten Teil des Ausdrucks widerspricht.

Dieses Beispiel zeigt uns, dass man die Allgemeingültigkeit mittels Belegungen im allgemeinen nicht in endlich vielen Schritten entscheiden kann.

Als Schlussregeln verwenden wir die oben erklärten 7 in rein syntaktischer Form. Ein Ausdruck $A \in \mathscr{L}^S$ heißt aus einer Menge $\mathscr{X} \subseteqq \mathscr{L}^S$ **ableitbar**, kurz in der Form $\mathscr{X} \models\!\Rightarrow A$ geschrieben, wenn man A durch endlich oftmaliges Anwenden der folgenden Regeln erhält.

1. Wenn $A \in \mathscr{X}$, so $\mathscr{X} \models\!\Rightarrow A$.
   - Wenn $\mathscr{X} \models\!\Rightarrow A$ und $\mathscr{X} \models\!\Rightarrow (A \rightarrow B)$, so $\mathscr{X} \models\!\Rightarrow B$.
   - Wenn $\mathscr{X} \models\!\Rightarrow (A(x) \rightarrow B)$, so $\mathscr{X} \models\!\Rightarrow (\forall x A(x) \rightarrow B)$.
   - Wenn $\mathscr{X} \models\!\Rightarrow (A \rightarrow B(x))$, so $\mathscr{X} \models\!\Rightarrow (A \rightarrow \exists x B(x))$.
   - Wenn $\mathscr{X} \models\!\Rightarrow (A \rightarrow B(x))$ und $x \notin \mathsf{var}(A)$, so $\mathscr{X} \models\!\Rightarrow (A \rightarrow \forall x B(x))$.

- Wenn $\mathscr{X} \models\!\!\Rightarrow (A(x) \to B)$ und $x \notin \mathsf{var}(B)$, so $\mathscr{X} \models\!\!\Rightarrow (\exists x A(x) \to B)$.
- Wenn $\mathscr{X} \models\!\!\Rightarrow A(x)$, so $\mathscr{X} \models\!\!\Rightarrow A(x|t)$ für jeden zulässigen Term t.
- Wenn $\mathscr{X} \models\!\!\Rightarrow A$ und A' entsteht durch eine zulässige gebundene Umbenennung aus A, so $\mathscr{X} \models\!\!\Rightarrow A'$.

2. Zu jedem aus $\mathscr{X}$ ableitbaren Ausdruck A gibt es eine natürliche Zahl n, so dass A durch n-malige Anwendung der Regeln in 2. aus den Ausdrücken aus $\mathscr{X}$ gewonnen werden kann.

Die Ableitungsmenge von $\mathscr{X}$ bezeichnen wir mit $\mathsf{Ab}^S(\mathscr{X})$; sie ist die kleinste Menge von Ausdrücken, die die Menge $\mathscr{X}$ umfasst und abgeschlossen hinsichtlich der obigen 7 Schlussregeln ist. Durch vollständige Induktion über die Ableitungsstufe zeigt man

2.11. Endlichkeitssatz für die Ableitbarkeit: *Jeder aus einer Menge $\mathscr{X}$ ableitbare Ausdruck ist aus einer endlichen Teilmenge von $\mathscr{X}$ ableitbar.*

Ein Ausdruck A heißt aus einer Menge $\mathscr{X} \subseteqq \mathscr{L}^S$ **beweisbar**, kurz in der Form $\mathscr{X} \vdash\!\!\!\rightarrow A$ geschrieben, wenn er aus der Menge $\mathscr{X} \cup \mathsf{Axa}^S$ ableitbar ist:

$$\mathscr{X} \vdash\!\!\!\rightarrow A \iff \mathscr{X} \cup \mathsf{Axa}^S \models\!\!\Rightarrow A.$$

Es sei $\mathsf{Bw}^S(\mathscr{X})$ die Menge aller aus $\mathscr{X}$ beweisbaren Ausdrücke, d. h.

$$\mathsf{Bw}^S(\mathscr{X}) = \mathsf{Ab}^S(\mathsf{Axa}^S \cup \mathscr{X}).$$

2.12. Satz: *Die Beweisbarkeit hat folgende Eigenschaften:*

1. **Einbettung:** *Für jede Menge $\mathscr{X} \subseteqq \mathscr{L}^S$ gilt: $\mathscr{X} \subseteqq \mathsf{Bw}^S(\mathscr{X})$.*
2. **Monotonie:** *Für beliebige Mengen $\mathscr{X}_1, \mathscr{X}_2 \subseteqq \mathscr{L}^S$ gilt:*
   Aus der Relation $\mathscr{X}_1 \subseteqq \mathscr{X}_2$ folgt $\mathsf{Bw}^S(\mathscr{X}_1) \subseteqq \mathsf{Bw}^S(\mathscr{X}_2)$.
3. **Abgeschlossenheit:** *Für jede Menge $\mathscr{X} \subseteqq \mathscr{L}^S$ gilt:*

   $$\mathsf{Bw}^S(\mathsf{Bw}^S(\mathscr{X})) = \mathsf{Bw}^S(\mathscr{X}).$$

4. **Endlichkeit:** *Jeder aus $\mathscr{X} \subseteqq \mathscr{L}^S$ beweisbare Ausdruck ist aus einer endlichen Teilmenge von $\mathscr{X}$ beweisbar.*
5. **Ableitbarkeit:**
   Wenn $(A \to B)$ aus $\mathscr{X} \subseteqq \mathscr{L}^S$ beweisbar ist, so ist B aus $\mathscr{X} \cup \{A\}$ beweisbar.
6. **Deduktion:** *Ist A eine S-Aussage und B aus $\mathscr{X} \cup \{A\}$ beweisbar, so ist auch $(A \to B)$ aus $\mathscr{X}$ beweisbar.*

Die Beweise der einzelnen Aussagen sind sehr leicht bzw. lassen sich leicht über die Ausdrucksstufe führen.
Den Zusammenhang zwischen der syntaktischen Beweisbarkeit und dem semantischen logischen Folgern stellt der folgende Satz her.

2.13. Hauptsatz der Prädikatenlogik erster Stufe: *Ein S-Ausdruck ist genau dann aus einer Ausdrucksmenge $\mathscr{X} \subseteqq \mathscr{L}^S$ beweisbar, wenn er aus $\mathscr{X}$ folgt:*

$$\mathsf{Bw}^S(\mathscr{X}) = \mathsf{Fl}^S(\mathscr{X}).$$

Eine kleine Folgerung soll aus dem Hauptsatz gezogen werden. Es sei $\mathscr{X}$ eine Ausdrucksmenge über S, $S(\mathscr{X})$ die Signatur aus allen jenen Symbolen aus S, die in den Ausdrücken von $\mathscr{X}$ effektiv vorkommen. Nach dem Hauptsatz gilt dann

$$\mathsf{Bw}^{S(\mathscr{X})}(\mathscr{X}) = \mathsf{Fl}^{S(\mathscr{X})}(\mathscr{X}).$$

Mit $\mathsf{Fl}^{S(\mathscr{X})}(\mathscr{X}) = \mathsf{Fl}^S(\mathscr{X}) \cap \mathscr{L}^{S(\mathscr{X})}$ schließen wir

$$\mathsf{Bw}^{S(\mathscr{X})}(\mathscr{X}) = \mathsf{Bw}^S(\mathscr{X}) \cap \mathscr{L}^{S(\mathscr{X})},$$

d. h. alles, was man in einer Sprache erster Stufe formulieren und innerhalb einer elementaren Erweiterung dieser Sprache beweisen kann, ist bereits in der engeren Sprache beweisbar.

2.5. Prädikatenlogische Sätze

Wir untersuchen hier solche Ausdrücke einer Sprache erster Stufe über einer Signatur S, die in jeder S-Algebra allgemeingültig sind.

2.14. Gödel'scher Vollständigkeitssatz: *Jeder allgemeingültige Ausdruck über der Signatur S ist aus Axa^S ableitbar:* $\mathsf{ag}^S \subseteqq \mathsf{Ab}^S(\mathsf{Axa}^S)$.

Nach dem Vollständigkeitssatz sind alle allgemeingültigen Ausdrücke aus Axa^S ableitbar, d. h. aus der leeren Menge beweisbar. Auf Grund der Monotonieeigenschaft sind die allgemeingültigen Ausdrücke daher aus jeder Menge beweisbar. Es sollen hier einige Ableitungen effektiv ausgeführt werden. Anstelle von $\emptyset \longmapsto A$ schreiben wir kurz $\longmapsto A$.
Zunächst ist klar, dass aus Axa^S alle aussagenlogisch allgemeingültigen Ausdrücke ableitbar sind. Insbesondere ist der Ausdruck $A(x) \rightarrow A(x)$ aussagenlogisch allgemeingültig, also gilt

$$(1) \quad \longmapsto \quad A(x) \rightarrow A(x).$$

Wenden wir die vordere All-Quantifizierung bzw. die hintere Ex-Quantifizierung an, so folgt

(2) $\vdash\!\!\longrightarrow \quad \forall x A(x) \to A(x)$,

(3) $\vdash\!\!\longrightarrow \quad A(x) \to \exists x A(x)$.

Indem auf (2) die hintere Ex-Quantifizierung angewendet wird, folgt

(4) $\vdash\!\!\longrightarrow \quad \forall x A(x) \to \exists x A(x)$.

Diese Schlussweise mehrfach (mit eventueller gebundener Umbenennung) angewendet, liefert

(5) $\vdash\!\!\longrightarrow \quad \mathsf{All}(A) \to A$,

(6) $\vdash\!\!\longrightarrow \quad A \to \mathsf{Ex}(A)$,

(7) $\vdash\!\!\longrightarrow \quad \mathsf{All}(A) \to \mathsf{Ex}(A)$,

(8) $\mathscr{X} \vdash\!\!\longrightarrow \quad A(x) \Longleftrightarrow \mathscr{X} \vdash\!\!\longrightarrow \quad \forall x A(x)$.

Beweis: Ist $\mathscr{X} \vdash\!\!\longrightarrow \quad \forall x A(x)$, so folgt aus (2) mit der Abtrennungsregel, dass

$$\mathscr{X} \vdash\!\!\longrightarrow \quad A(x).$$

Es sei umgekehrt $\mathscr{X} \vdash\!\!\longrightarrow \quad A(x)$ und A^* ein Ausdruck, der die Variable x nicht enthält, aber aus Axa^S ableitbar ist. Wegen $p \to (q \to p) \in \mathsf{ag}$ folgt

$$\mathscr{X} \vdash\!\!\longrightarrow \quad A(x) \to (A^* \to A(x))$$

und daraus mit der Abtrennungsregel

$$\mathscr{X} \vdash\!\!\longrightarrow \quad A^* \to A(x).$$

Der Ausdruck A^* enthält nicht die Variable x; also können wir die hintere All-Quantifizierung anwenden:

$$\mathscr{X} \vdash\!\!\longrightarrow \quad A^* \to \forall x A(x).$$

Mit der Abtrennungsregel folgt die Behauptung. ♣

Durch mehrmalige Anwendung von (8) und gebundener Umbenennung folgt

(9) $\mathscr{X} \vdash\!\!\longrightarrow \quad A(x) \Longleftrightarrow \mathscr{X} \vdash\!\!\longrightarrow \quad \mathsf{All}(A(x))$.

Es gelten die folgenden Regeln der Quantorenvertauschung

(10) $\vdash\!\!\longrightarrow \quad \forall x \forall y A(x,y) \leftrightarrow \forall y \forall x A(x,y)$,

(11) $\quad \longmapsto \quad \exists x \exists y A(x,y) \leftrightarrow \exists y \exists x A(x,y)$,

(12) $\quad \longmapsto \quad \exists x \forall y A(x,y) \rightarrow \forall y \exists x A(x,y)$.

Beweis: Bei der Regel (10) gehen wir von (1) mit $A(x,y)$ aus und wenden der Reihe nach zweimal die vordere All-Quantifizierung, zweimal die gebundene Umbenennung, zweimal die hintere All-Quantifizierung und schließlich zweimal die gebundene Umbenennung an, wodurch wir die folgende Beweisfolge erhalten:

$$\begin{aligned}
&\longmapsto \quad A(x,y) \rightarrow A(x,y), \longmapsto \quad \forall x \forall y A(x,y) \rightarrow A(x,y), \\
&\longmapsto \quad \forall u \forall v A(u,v) \rightarrow A(x,y), \longmapsto \quad \forall u \forall v A(u,v) \rightarrow \forall y \forall x A(x,y), \\
&\longmapsto \quad \forall x \forall y A(x,y) \rightarrow \forall y \forall x A(x,y).
\end{aligned}$$

Indem wir x und y vertauschen, erhalten wir

$$\longmapsto \quad \forall y \forall x A(x,y) \rightarrow \forall x \forall y A(x,y).$$

Aus beiden folgt über das Schließen auf eine Äquivalenz

$$(p \rightarrow q) \rightarrow [(q \rightarrow p) \rightarrow (p \leftrightarrow q)]$$

mittels Abtrennung sofort (10). Ganz analog zeigt man (11).
Zum Beweis von (12) gehen wir wieder von (1) mit $A(x,y)$ aus und wenden vordere All-Quantifizierung, hintere Ex-Quantifizierung, gebundene Umbennung, vordere Ex-Quantifizierung, gebundene Umbenennung, hintere All-Quantifizierung und gebundene Umbenennung an:

$$\begin{aligned}
&\longmapsto \quad A(x,y) \rightarrow A(x,y), \longmapsto \quad \forall y A(x,y) \rightarrow \exists u A(u,y), \\
&\longmapsto \quad \forall v A(x,v) \rightarrow \exists u A(u,y), \longmapsto \quad \exists x \forall v A(x,v) \rightarrow \forall y \exists u A(u,y), \\
&\longmapsto \quad \exists x \forall y A(x,y) \rightarrow \forall y \exists x A(x,y),
\end{aligned}$$

womit schon alles bewiesen ist. ♣
Aus diesen kleinen Beweisen wird das allgemeine Beweisprinzip klar: Man suche sich geeignete allgemeingültige, aussagenlogische Ausdrücke (z. B. Axiome aus Axa) und wende darauf eine geeignete Folge von Schlussregeln an. Welche Folge von Schlussregeln schließlich zum Ziel führt, bleibt der Intuition des Akteurs überlassen. So gibt es die folgenden Regeln der Quantorenverteilung.

(13) $\quad \longmapsto \quad \forall x[A(x) \wedge B(x)] \leftrightarrow \forall x A(x) \wedge \forall x B(x)$,

(14) $\quad \longmapsto \quad \forall x A(x) \vee \forall x B(x) \rightarrow \forall x[A(x) \vee B(x)]$,

(15) $\quad \longmapsto \quad \forall x[A(x) \rightarrow B(x)] \rightarrow [\forall x A(x) \rightarrow \forall x B(x)]$,

(16) $\quad \longmapsto \quad \forall x[A(x) \leftrightarrow B(x)] \rightarrow [\forall x A(x) \leftrightarrow \forall x B(x)]$,

(17) $\quad \longmapsto \quad \exists x[A(x) \wedge B(x)] \to \exists x A(x) \wedge \exists x B(x),$

(18) $\quad \longmapsto \quad \exists x[A(x) \vee B(x)] \leftrightarrow \exists x A(x) \vee \exists x B(x).$

Beweis: Wir beweisen beispielhaft (15) und gehen dabei von

$$\longmapsto \quad (A(x) \to B(x)) \to (A(x) \to B(x))$$

aus. Die vordere All-Quantifzierung liefert

$$\longmapsto \quad \forall x(A(x) \to B(x)) \to (A(x) \to B(x)).$$

Mit der Prämissenvertauschung folgt daraus

$$\longmapsto \quad A(x) \to [\forall x(A(x) \to B(x)) \to B(x)],$$

worin wir die vordere All-Quantifizierung ausführen dürfen:

$$\longmapsto \quad \forall x A(x) \to [\forall x(A(x) \to B(x)) \to B(x)].$$

Die Prämissenverbindung gilt in der Form

$$[p \to (q \to r)] \leftrightarrow (p \wedge q \to r),$$

was zwei aussagenlogisch allgemeingültige Ausdrücke liefert:

$$[p \to (q \to r)] \to (p \wedge q \to r),$$

$$(p \wedge q \to r) \to [p \to (q \to r)].$$

Wenn man $p = \forall x A(x), q = \forall x(A(x) \to B(x))$ und $r = B(x)$ in der ersten setzt, ergibt sich mit der Abtrennungsregel

$$\longmapsto \quad [\forall x A(x) \wedge \forall x(A(x) \to B(x))] \to B(x).$$

Nach gebundenen Umbenennungen, hinterer All-Quantifizierung und gebundenen Umbenennungen erhalten wir

$$\longmapsto \quad [\forall x A(x) \wedge \forall x(A(x) \to B(x))] \to \forall x B(x).$$

Dieser Ausdruck hat die aussagenlogische Form der Prämisse aus der Prämissenverbindung (zweite Form), woraus wir

$$\longmapsto \quad \forall x A(x) \to [\forall x(A(x) \to B(x)) \to \forall x B(x)]$$

schließen und mit der Prämissenvertauschung die Behauptung erhalten. Eine mögliche Kurzform dieses Beweises ist die folgende Kette:

$$(A \to B) \to (A \to B);$$

$$\begin{pmatrix} \forall x(A \to B) \to (A \to B) \\ p \quad\to\quad (q \to r) \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} A \to [\forall x(A \to B) \to B] \\ q \to \quad (p \quad \to r) \end{pmatrix};$$

$$\begin{pmatrix} \forall x A \to [\forall x(A \to B) \to B] \\ q \quad\to\quad (p \quad\to r) \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} \forall x A \wedge \forall x(A \to B) \to B \\ q \quad\wedge\quad p \quad\to r \end{pmatrix};$$

$$\begin{pmatrix} \forall x A \wedge \forall x(A \to B) \to \forall x B \\ q \quad\wedge\quad p \quad\to\quad r \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} \forall x A \to [\forall x(A \to B) \to \forall x B] \\ q \quad\to\quad (p \quad\to\quad r) \end{pmatrix}$$

$$\begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} \forall x(A \to B) \to (\forall x A \to \forall x B) \\ p \quad\to\quad (q \to r) \end{pmatrix}.$$

In dieser Kurzform sind die möglicherweise notwendigen gebundenen Umbenennungen nicht angezeigt; sie sind jedoch leicht zu erkennen. Wenn man den obigen Beweis verstanden hat, sollte auch die Kurzform lesbar sein. Die Kurzform eines Beweises von (17) ist folgende:

$$\begin{pmatrix} A \wedge B \to A \\ A \wedge B \to B \end{pmatrix}; \begin{pmatrix} A \wedge B \to \exists x A \\ A \wedge B \to \exists x B \end{pmatrix}; \begin{pmatrix} A \wedge B \to \exists x A \wedge \exists x B \\ p \quad\to\quad q \wedge r \end{pmatrix};$$

$$\exists x(A \wedge B) \to \exists x A \wedge \exists x B.$$

Nach diesem Muster möge der Leser Ableitungen für die anderen Behauptungen finden. $\clubsuit$

Die Negationsregeln lauten:

(19) $\quad \vdash\!\!\to \quad \exists x \neg A(x) \leftrightarrow \neg \forall x A(x),$

(20) $\quad \vdash\!\!\to \quad \forall x \neg A(x) \leftrightarrow \neg \exists x A(x).$

Beweis: Wir beweisen nur (20). Dazu sind zwei Beweise nötig:

$$\vdash\!\!\to \quad \forall x \neg A(x) \to \neg \exists x A(x) \quad \text{und} \quad \vdash\!\!\to \quad \neg \exists x A(x) \to \forall x \neg A(x).$$

Die folgende Beweiskette zeigt die Beweisbarkeit der ersten Behauptung; sie beginnt mit (2) und der Kontraposition:

$$\begin{pmatrix} \forall x \neg A \to \neg A \\ p \to q \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} A \to \neg \forall x \neg A \\ \neg q \to \neg p \end{pmatrix};$$

$$\begin{pmatrix} \exists x A \to \neg \forall x \neg A \\ p \to q \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} \forall x \neg A \to \neg \exists x A \\ \neg q \to \neg p \end{pmatrix}.$$

Die Beweiskette für die zweite Behauptung beginnt mit (3) und der Kontraposition:

$$\begin{pmatrix} A \to \exists x A \\ p \to q \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} \neg\exists x A \to \neg A \\ \neg q \to \neg p \end{pmatrix} ; \neg\exists x A \to \forall x \neg A.$$

Die Aussage (19) wird analog bewiesen. ♣

Für die Regeln der Quantorenverschiebung sei A^* ein Ausdruck, in dem die Variable x nicht vorkommt.

(21) $\quad \longmapsto \quad \forall x(A(x) \wedge A^*) \leftrightarrow \forall x A(x) \wedge A^*,$

(22) $\quad \longmapsto \quad \forall x(A(x) \vee A^*) \leftrightarrow \forall x A(x) \vee A^*,$

(23) $\quad \longmapsto \quad \forall x(A(x) \to A^*) \leftrightarrow \exists x A(x) \to A^*,$

(24) $\quad \longmapsto \quad \forall x(A^* \to A(x)) \leftrightarrow A^* \to \forall x A(x),$

(25) $\quad \longmapsto \quad \exists x(A(x) \wedge A^*) \leftrightarrow \exists x A(x) \wedge A^*,$

(26) $\quad \longmapsto \quad \exists x(A(x) \vee A^*) \leftrightarrow \exists x A(x) \vee A^*,$

(27) $\quad \longmapsto \quad \exists x(A(x) \to A^*) \leftrightarrow \forall x A(x) \to A^*,$

(28) $\quad \longmapsto \quad \exists x(A^* \to A(x)) \leftrightarrow A^* \to \exists x A(x).$

Beweis: Wir geben die Beweisketten für (21) und (23) an; zu jeder Regel gehören jeweils zwei. Die beiden Beweisketten für (21) lauten:

$$\begin{pmatrix} A \wedge A^* \to A \\ A \wedge A^* \to A^* \end{pmatrix} ; \begin{pmatrix} \forall x(A \wedge A^*) \to A \\ \forall x(A \wedge A^*) \to A^* \end{pmatrix} ; \begin{pmatrix} \forall x(A \wedge A^*) \to \forall x A \\ \forall x(A \wedge A^*) \to A^* \end{pmatrix} ;$$

$$\forall x(A \wedge A^*) \to \forall x A \wedge A^*; \begin{pmatrix} \forall x A \to A \\ p \to q \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix}$$

$$\begin{pmatrix} \forall x A \wedge A^* \to A \wedge A^* \\ p \wedge r \to q \wedge r \end{pmatrix} ; \forall x A \wedge A^* \to \forall x(A \wedge A^*).$$

Die beiden Beweisketten für (23) lauten:

$$\begin{pmatrix} \forall x(A \to A^*) \to (A \to A^*) \\ p \to (q \to r) \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} A \to [\forall x(A \to A^*) \to A^*] \\ q \to (p \to r) \end{pmatrix} ;$$

$$\begin{pmatrix} \exists x A \to [\forall x(A \to A^*) \to A^*] \\ p \to (q \to r) \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} \forall x(A \to A^*) \to (\exists x A \to A^*) \\ q \to (p \to r) \end{pmatrix} ,$$

$$\begin{pmatrix} A \to \exists x A \\ p \to q \end{pmatrix} \begin{matrix} ; \\ \to \end{matrix} \begin{pmatrix} (\exists x A \to A^*) \to (A \to A^*) \\ (q \to r) \to (p \to r) \end{pmatrix} ; (\exists x A \to A^*) \to \forall x(A \to A^*).$$

Damit ist die grundlegende Beweismethode hinreichend erläutert. ♣

2.6. Prädikatenlogische Normalformen

Für die automatische Verarbeitung von Ausdrücken auf Rechnern ist es wesentlich, alle Ausdrücke einer Ausdrucksmenge auf eine standardisierte Form zu transformieren, wobei sich ihr Wahrheitswert nicht ändern darf. Ein S-Ausdruck A befindet sich in einer **pränexen Normalform**, wenn er die Form

$$q_1 x_1 q_2 x_2 \cdots q_n x_n A'$$

hat, wobei $q_i \in \{\forall, \exists\}, i = 1, \ldots, n$ und in A' kein Quantor vorkommt.

2.15. Satz: *Jeder S-Ausdruck aus $\mathscr{L}^S$ kann semantisch bzw. syntaktisch äquivalent in eine pränexe Normalform überführt werden.*

Beweis: Es soll nur angedeutet werden, wie man bei einer Überführung eines gegebenen Ausdrucks A in eine pränexe Normalform vorzugehen hat. Zunächst werden aus A die Funktoren $\rightarrow$ und $\leftrightarrow$ äquivalent eliminiert. Danach werden die Negationssymbole durch Anwenden der bekannten Regeln soweit nach innen getrieben, dass sie höchstens noch unmittelbar vor einem relationalen Teilausdruck auftreten; doppelte Verneinungen werden gestrichen. Nun benennt man die Variablen so um, dass jede nur noch an höchstens einer Stelle vorkommt und alle rel-freien Variablen sogar abs-frei vorkommen. Schließlich treibt man mittels Äquivalenzen aus dem letzten Abschnitt die auftretenden Quantifizierungen nach vorn. ♣

So lautet z. B. für den Ausdruck

$$\forall x \exists y [xPf(y, g(x))] \vee \neg Qz \vee \neg \forall x(xRy),$$

worin P, R, f je zweistellig, Q, g einstellig sein mögen, eine pränexe Normalform

$$\exists u \forall x \exists y [xPf(y, g(x))] \vee \neg Qz \vee \neg(uRv).$$

Für Erfüllbarkeitsuntersuchungen ordnen wir einer pränexen Normalform A eine **Skolemform** zu, indem wir auf A den folgenden Algorithmus anwenden:

Eingabe:

A : pränexe Normalform,

$gibf$: Programm, das zu einem gegebenen Ausdruck und einer natürlichen Zahl n ein n-stelliges Oprationssysmbol liefert, das nicht im Ausdruck vorkommt,

$giba$: Programm, das zu einem gegebenen Ausdruck ein Konstantensysmbol liefert, das nicht im Ausdruck vorkommt.

Ausgabe:

A : Skolemform

Programm:

```
while A enthält das Zeichen ∃ do
  if A hat die Form ∀x_1 ··· ∀x_n ∃yB then
    f := gibf(B,n); A := ∀x_1 ··· ∀x_n B(y|f(x_1, ··· , x_n))
  end if
  if A hat die Form ∃yB then
    a := giba(B); A := B(y|a)
  end if
end while
```

Nach diesem Algorithmus wird suksessive von links nach rechts jeder Ex-Quantor gestrichen und für die betreffende danach abs-freie Variable ein einfacher Term der Form $f(x_1,\ldots,x_n)$ eingesetzt, wobei das Operationssymbol f noch nicht im Ausdruck vorkommen darf. Dieser Term verknüpft alle links vom aktuell gestrichenen Ex-Quantor all-quantifizierten Variablen. Sollten solche Variablen nicht existieren, wird anstelle der betreffenden Variablen ein noch nicht im Ausdruck vorkommendes Konstantensymbol eingesetzt. Natürlich setzt der Algorithmus voraus, dass in der Signatur S die geforderten Operations- und Konstantensymbole auch vorhanden sind. Sollte dies nicht der Fall sein, werden entsprechend neue Symbole „erfunden“ und zur Signatur hinzugefügt. Es ist klar, dass eine Skolemform nicht eindeutig bestimmt ist.

2.16. Erblichkeit der Erfüllbarkeit: *Eine pränexe Normalform A ist genau dann erfüllbar, wenn jede Skolemform von A erfüllbar ist.*

Beweis: Es sei A von der Form $\forall x_1 \cdots \forall x_n \exists y B$. Nach einem Durchlauf des Algorithmus zur Konstruktion einer Skolemform entsteht ein Ausdruck A' der Form

$$\forall x_1 \cdots \forall x_n B(y|f(x_1,\ldots,x_n))$$

und wir haben zu zeigen: A ist genau dann erfüllbar, wenn A' erfüllbar ist.
Es sei A' erfüllbar; dann gibt es eine Algebra $\mathscr{U} = (U,\omega)$ und eine Belegung α aus U mit

$$\mathrm{ww}_{\mathscr{U}}(A',\alpha) = W$$

und für alle $\xi_1,\ldots,\xi_n \in U$ gilt

$$\begin{aligned} W &= \mathrm{ww}_{\mathscr{U}}(B(y|f(x_1,\ldots,x_n)),\alpha^{x_1,\ldots,x_n}_{\xi_1,\ldots,\xi_n}) \\ &= \mathrm{ww}_{\mathscr{U}}(B,\alpha^{x_1,\ldots,x_n,y}_{\xi_1,\ldots,\xi_n,f^\omega(\xi_1,\ldots,\xi_n)}), \end{aligned}$$

also gibt es eine Belegung α^* mit

$$\mathrm{ww}_{\mathscr{U}}(\forall x_1 \cdots \forall x_n \exists y B,\alpha^*) = W,$$

d. h. A ist erfüllbar.
Es sei nun umgekehrt $A = \forall x_1 \cdots \forall x_n \exists y B$ erfüllbar in einer Algebra $\mathscr{U} = (U,\omega)$, wobei in der Sprache nur die in B effektiv auftretenden Relations-, Operations- und Konstantensymbole sowie freien Variablen vorkommen mögen. Für eine gewisse Belegung α gilt also in $\mathscr{U}$

$$\mathrm{ww}_{\mathscr{U}}(A,\alpha) = \mathrm{ww}_{\mathscr{U}}(\forall x_1 \cdots \forall x_n \exists y B, \alpha) = W,$$

d. h. zu beliebigen n Konstanten $\xi_1,\ldots,\xi_n \in U$ gibt es ein $\xi \in U$ mit

$$\mathrm{ww}_{\mathscr{U}}(B, \alpha^{x_1,\ldots,x_n,y}_{\xi_1,\ldots,\xi_n,\xi}) = W.$$

Wir definieren nun ein n-stelliges Operationssymbol f, das entsprechend dieser Gleichung interpretiert wird, d. h. für $\xi_1,\ldots,\xi_n \in U$ soll $f^\omega(\xi_1,\ldots,\xi_n)$ gerade eine solche Konstante $\xi \in U$ sein. Es wird aber i. a. mehrere solcher Konstanten zu einem n-Tupel geben. Daher bilden wir zu jedem n-Tupel $(\xi_1,\ldots,\xi_n)$ die Menge

$$X_{(\xi_1,\ldots,\xi_n)} = \left\{ (\xi_1,\ldots,\xi_n,\xi) \mid \mathrm{ww}_{\mathscr{U}}(B, \alpha^{x_1,\ldots,x_n,y}_{\xi_1,\ldots,\xi_n,\xi}) = W \right\}$$

und erhalten ein Mengensystem, in dem je zwei Mengen elementfremd sind. Nach dem Auswahlprinzip gibt es eine Auswahlmenge $\mathscr{X}$, die aus jeder Menge dieses Mengensystems genau ein Element enthält. Damit liegt die Operation f^ω wie folgt fest:

$$\xi = f^\omega(\xi_1,\ldots,\xi_n) \quad \Longleftrightarrow \quad (\xi_1,\ldots,\xi_n,\xi) \in \mathscr{X}.$$

Die so definierte Operation fügen wir zur Algebra $\mathscr{U}$ hinzu und erhalten eine erweiterte Algebra $\mathscr{U}'$. Nach Definition der Operation f^ω gilt damit für alle $\xi_1,\ldots,\xi_n \in U$:

$$\begin{aligned} W &= \mathrm{ww}_{\mathscr{U}}(B, \alpha^{x_1,\ldots,x_n,y}_{\xi_1,\ldots,\xi_n,f^\omega(\xi_1,\ldots,\xi_n)}) \\ &= \mathrm{ww}_{\mathscr{U}}(B(y|f^\omega(\xi_1,\ldots,\xi_n)), \alpha^{x_1,\ldots,x_n}_{\xi_1,\ldots,\xi_n}), \end{aligned}$$

also

$$\mathrm{ww}_{\mathscr{U}}(\forall x_1 \cdots \forall x_n B(y|f(x_1,\ldots,x_n)), \alpha) = W,$$

d. h. der mit dem ersten Durchlauf entstehende Ausdruck ist in der erweiterten Algebra erfüllbar. ♣
Wir sind nun in der Lage, alle Transformationen aufzuschreiben, mittels derer man einen Ausdruck A in eine erfüllbarkeits-äquivalente Klauselmenge überführen kann. Vorgegeben sei also ein Ausdruck A.

- Durch gebundene Umbenennung überführe man A in einen Ausdruck A_1, in dem jede auftretende Variable entweder abs-frei oder gebunden vorkommt.
- Es seien $x_1, \ldots, x_n$ alle in A_1 abs-frei auftretenden Variablen; diese werden ex-quantifiziert, so dass aus A_1 ein abgeschlossener Ausdruck A_2 der Form $\exists x_1 \cdots \exists x_n A_1$ entsteht, der erfüllbarkeits-äquivalent zu A_1 und damit zu A ist.
- Man überführe A_2 in eine pränexe Normalform A_3.
- Man überführe A_3 in eine Skolemform A_4; sind $x_1, \ldots, x_n$ alle in A_4 auftretenden Variablen, so hat A_4 die Form

  $$\forall x_1 \cdots \forall x_n B(x_1, \ldots, x_n),$$

  wobei $B(x_1, \ldots, x_n)$ ein aussagenlogischer Ausdruck ist, den man **Matrix** von A_4 nennt.
- Man überführe die Matrix $B(x_1, \ldots, x_n)$ von A_4 in eine konjunktive Standardform und bilde dazu die Klauselmenge A_5.

Beispiel: Gegeben sei der Ausdruck

$$\neg \exists y [yPz \vee \forall xyQf(x)] \vee \forall x [g(x,y)Pz].$$

Durch gebundene Umbenennung erhalten wir den Ausdruck

$$\neg \exists v [vPz \vee \forall xvQf(x)] \vee \forall u [g(u,y)Pz].$$

Da die Variablen y und z abs-frei vorkommen, werden sie ex-quantifiziert:

$$\exists y \exists z \{ \neg \exists v [vPz \vee \forall xvQf(x)] \vee \forall u [g(u,y)Pz] \}.$$

Hierzu gehört z. B. die pränexe Normalform

$$\exists y \exists z \forall v \exists x \forall u \{ [\neg vPz \wedge \neg vQf(x)] \vee g(u,y)Pz \}.$$

Um zu einer Skolemform zu kommen, haben wir für y und z je ein Konstantensymbol a bzw. b und für x einen Term $h(v)$ einzusetzen, womit wir den Ausdruck

$$\forall v \forall u \{ [\neg vPb \wedge \neg vQf(h(v))] \vee g(u,a)Pb \}$$

erhalten. Die Matrix dieses Ausdruck formen wir in eine konjunktive Standardform um:

$$\forall v \forall u \{ [\neg vPb \vee g(u,a)Pb] \wedge [\neg vQf(h(v)) \wedge g(u,a)Pb] \}.$$

Diesen letzten Ausdruck, der erfüllbarkeits-äquivalent zum ersten ist, schreiben wir nun in Klauselform:

$$\{\,\{\,\neg vPb, g(u,a)Pb\,\}\,, \{\,\neg vQf(h(v)), g(u,a)Pb\,\}\,\}\,.$$

In dieser Klauselform muss man sich jede vorkommende Variable all-quantifiziert denken.

2.7. Herbrand-Strukturen

Wie wir bereits festgestellt haben, gibt es Ausdrücke, die nur in einer unendlichen Algebra erfüllbar sein können. Dieser Umstand hat zur Folge, dass man Methoden der Aussagenlogik, wie z. B. die Wahrheitstafelmethode, nicht zu einem Entscheidungsverfahren für die Erfüllbarkeit von Ausdrücken aus Sprachen erster Stufe heranziehen kann. Ohne einen exakten Begriff von „entscheidbar“ zu geben, was in der Theorie der formalen Sprachen geschieht, wollen wir ein Problem **entscheidbar** oder **rekursiv** nennen, wenn es ein Rechenverfahren – etwa als C++-Programm geschrieben – gibt, das auf den Daten des Problems arbeitet (diese als Input hat) und nach endlicher Zeit eine korrekte Antwort „ja“ oder „nein“ in Bezug auf die gegebene Fragestellung gibt.

2.17. Satz von A. CHURCH**:** *Die Allgemeingültigkeit von Ausdrücken einer Sprache erster Stufe ist unentscheidbar, d. h. folgendes Problem ist unentscheidbar:*

> *Gegeben sei ein beliebiger S-Ausdruck A;*
> *gesucht ist eine korrekte Antwort auf die Frage: Ist A allgemeingültig?*

Aus der Unentscheidbarkeit der Allgemeingültigkeit folgt sofort, dass auch die Erfüllbarkeit unentscheidbar ist. Wir können uns also keinen vollständigen Überblick über alle wahren Sätze einer Sprache erster Stufe verschaffen. Es gibt jedoch die Möglichkeit, die Unerfüllbarkeit eines Ausdrucks zu entscheiden. Dazu werden wir zu einem gegebenen Ausdruck A in Skolemform eine spezielle Algebra konstruieren, deren abzählbare Trägermenge aus variablenfreien Termen besteht, die sich selbst interpretieren. Diese Terme können uneingeschränkt für Termeinsetzungen in der Matrix von A verwendet werden. Durch vollständige Termeinsetzungen mit allen Termen der Termalgebra wird dem gegebenen Ausdruck A eine abzählbare Menge von aussagenlogischen Ausdrücken zugeordnet mit der Eigenschaft, dass A genau dann erfüllbar ist, wenn alle diese Ausdrücke erfüllbar sind. Dieses Programm soll nun ausgeführt werden. Nach den obigen Überlegungen können wir uns dabei auf abgeschlossene Ausdrücke, also Aussagen beschränken. Es sei daher A eine Aussage in Skolemform. Unter dem **Herbrand-Bereich** $\mathscr{H}(A)$ (nach J. HERBRAND) verstehen wir die folgende, induktiv definierte Menge von Termen:

1. Atomare Terme: Alle in A vorkommenden Konstantensymbole gehören zu $\mathscr{H}(A)$. Sollte A kein Konstantensymbol enthalten, nehmen wir ein beliebiges Konstantensymbol a der Sprache in $\mathscr{H}(A)$ auf.

2. Abgeleitete Terme: Ist f ein m-stelliges Operationssymbol aus A und sind $t_1, \ldots, t_m$ Terme aus $\mathscr{H}(A)$, so ist $f(t_1, \ldots, t_m) \in \mathscr{H}(A)$.

3. Zu jedem Term aus $\mathscr{H}(A)$ gibt es eine natürliche Zahl n, so dass man den Term durch n-malige Anwendung von 2. aus den atomaren Termen von $\mathscr{H}(A)$ gewinnen kann.

Wir bemerken, dass $\mathscr{H}(A)$ nur variablenfreie Terme enthält und daher alle Terme aus $\mathscr{H}(A)$ uneingeschränkt für Termeinsetzungen verwendet werden dürfen. Für den Ausdruck

$$\forall x \forall y Raf(x)g(y,b)$$

lautet der Herbrand-Bereich

$$\mathscr{H}(A) = \left\{ \begin{array}{l} a, b, f(a), f(b), g(a,a), g(a,b), g(b,a), g(b,b), \\ f(f(a)), f(f(b)), f(g(a,a)), f(g(a,b)), \ldots \end{array} \right\}.$$

Eine solche Wortmenge wählen wir als Trägermenge für eine Algebra. Eine Algebra $(\mathscr{H}(A), \omega)$ heißt **H-Algebra**, falls für jedes in A vorkommende n-stellige Operationssymbol f und beliebige n Terme $t_1, \ldots, t_n \in \mathscr{H}(A)$ gilt

$$f^\omega(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$$

gilt. Damit sind bei einer H-Algebra die Trägermenge und die Interpretation der Operationssymbole festgelegt, während über die Interpretation der Relationssymbole noch frei verfügt werden kann. Die Interpretation der Operationssymbole erfolgt so, dass der Wert eines Terms der Term selbst ist, d. h. für jeden Term $t \in \mathscr{H}(A)$ gilt bei jeder Belegung α:

$$t^\omega_\alpha = t.$$

Daraus folgt für jeden Ausdruck A der Form $\forall x A'(x)$:

$$\mathrm{ww}_{\mathscr{H}(A)}(A'(x|t), \alpha) = \mathrm{ww}_{\mathscr{H}(A)}(A', \alpha^x_t)$$

für jede Belegung α aus $\mathscr{H}(A)$ und jeden Term $t \in \mathscr{H}(A)$.
Im Falle des Ausdrucks

$$\forall x \forall y \forall z Rxf(y)g(z,x)$$

gilt also

$$\mathscr{H}(A) = \{ a, f(a), g(a,a), \dots \}$$

und

$$\begin{aligned} f^\omega(a) &= f(a), \\ f^\omega(f^\omega(a)) &= f(f(a)), \\ f^\omega(g(a,a)) &= f(g(a,a)), \text{ usw.} \end{aligned}$$

Über die Interpretation des Relationssymbols R können wir noch frei verfügen, indem wir z. B. setzen:

$$(t_1,t_2,t_3) \in R^\omega \quad \Longleftrightarrow \quad g^\omega(t_2,t_3) = g^\omega(f^\omega(t_1), f^\omega(t_2)).$$

In dieser H-Algebra $\mathscr{U}$ ist A sicherlich falsch, da für $x = y = z = a$ das Tripel $(a, f(a), g(a,a))$ in R^ω liegen müsste, was aber offensichtlich nicht gilt.

2.18. Satz von Herbrand: *Wenn eine Aussage A in Skolemform erfüllbar ist, gibt es eine H-Algebra $\mathscr{U}_* = (\mathscr{H}(A), \omega_*)$, in der A erfüllbar ist.*

Beweis: Es sei $\mathscr{U} = (U, \omega)$ eine Algebra, in der A erfüllt ist. Es soll nun eine im Satz behauptete Algebra $\mathscr{U}_* = (\mathscr{H}(A), \omega_*)$ konstruiert werden. Falls in A kein Konstantensymbol vorkommt, wählen wir aus U ein beliebiges Element p aus und setzen $a^\omega = p$, wenn a das einzige Konstantensymbol aus dem Herbrand-Bereich $\mathscr{H}(A)$ ist. Da die Terme aus dem Herbrand-Bereich keine Variablen enthalten, ist ihr Wert in U unabhängig von einer Belegung, d. h. für jede Belegung α gilt $t^\omega_\alpha = t^\omega$ (für alle $t \in \mathscr{H}(A)$). In der H-Algebra $\mathscr{U}_*$ haben wir die Interpretation der in A auftretenden Relationssymbole noch festzulegen. Es sei also R ein m-stelliges Relationssymbol aus A. Für $t_1, \dots, t_m \in \mathscr{H}(A)$ definieren wir

$$(t_1, \dots, t_m) \in R^{\omega_*} \quad \Longleftrightarrow \quad (t_1^\omega, \dots, t_m^\omega) \in R^\omega.$$

Durch vollständige Induktion über die Anzahl n der All-Quantoren in A zeigen wir nun, dass die Aussage A in der H-Algebra $\mathscr{U}_*$ wahr ist. Im Falle $n = 0$ enthält A keine All-Quantoren, ist also ein variablenfreier, aussagenlogischer Ausdruck und daher wegen der Interpretation der Relationssymbole: $\mathrm{ww}_{\mathscr{U}}(A, \alpha) = \mathrm{ww}_{\mathscr{H}(A)}(A, \alpha)$ (für alle α). Es sei nun A eine Aussage mit genau n All-Quantoren und von der Form $\forall x A'$, wobei A' nur $n-1$ All-Quantoren enthält. Nach Voraussetzung ist A erfüllbar in $\mathscr{U}$; also gilt bei einer gewissen Belegung α für alle $\xi \in U$:

$$\mathrm{ww}_{\mathscr{U}}(A', \alpha^x_\xi) = W$$

und daher speziell auch für $\xi = t^\omega$ für alle $t \in \mathscr{H}(A)$, d. h. für alle $t \in \mathscr{H}(A)$ gilt

$$W = \mathrm{ww}_{\mathscr{U}}(A', \alpha^x_{t^\omega}) = \mathrm{ww}_{\mathscr{U}}(A'(x|t), \alpha).$$

Damit schließen wir mit der Induktionsvoraussetzung für alle $t \in \mathscr{H}(A)$

$$\begin{aligned} W &= \mathrm{ww}_{\mathscr{U}}(A'(x|t), \alpha) = \mathrm{ww}_{\mathscr{H}(A)}(A'(x|t), \alpha) \\ &= \mathrm{ww}_{\mathscr{H}(A)}(A', \alpha^x_{t^{\omega *}}) \\ &= \mathrm{ww}_{\mathscr{H}(A)}(A', \alpha^x_t) \end{aligned}$$

und erhalten $\mathrm{ww}_{\mathscr{H}(A)}(\forall x A', \alpha) = W$. ♣
Jeder Ausdruck ist erfüllbarkeits-äquivalent in eine Skolemform transformierbar und die einer Skolemform zugeordneten H-Algebren sind abzählbar; daher ergibt sich als Folgerung der nächste Satz.

2.19. Satz von Löwenheim-Skolem: *Jeder erfüllbare Ausdruck ist in einer abzählbaren Algebra erfüllbar.*

Es sei A eine Aussage in Skolemform mit genau n all-quantifizierten Variablen:

$$A = \forall x_1 \cdots \forall x_n A'(x_1, \ldots, x_n).$$

Der Ausdruck $A'(x_1, \ldots, x_n)$ ist die Matrix von A. Wenn wir in ihr für alle Variablen Terme aus $\mathscr{H}(A)$ einsetzen und dabei alle Terme des Herbrand-Bereiches von A durchlaufen, erhalten wir eine Aussagenmenge $\mathscr{E}(A)$, die **Herbrand-Expansion** von A:

$$\mathscr{E}(A) = \left\{ A'(x_1|t_1, \ldots, x_n|t_n) \;\middle|\; t_1, \ldots, t_n \in \mathscr{H}(A) \right\}.$$

Da die Aussagen der Herbrand-Expansion von A keine Quantifizierungen enthalten, können alle Elemente aus $\mathscr{E}(A)$ wie aussagenlogische Ausdrücke behandelt werden.

2.20. Satz von Gödel-Herbrand-Skolem: *Eine Aussage in Skolemform ist dann und nur dann erfüllbar, wenn jeder Ausdruck aus der Herbrand-Expansion erfüllbar ist.*

Beweis: Wir haben nur zu zeigen: A ist in einer H-Algebra genau erfüllbar, wenn die Ausdrücke aus $\mathscr{E}(A)$ aussagenlogisch erfüllbar sind.
Die Aussage A habe die Form $\forall x_1 \cdots \forall x_n A'$. Dann gilt die folgenden Kette von Äquivalenzen:

A ist in einer H-Algebra $\mathscr{U} = (\mathscr{H}(A), \omega)$ erfüllbar
$\Longleftrightarrow$ für eine gewisse Belegung α und alle $t_1, \ldots, t_n \in \mathscr{H}(A)$:

$$\mathrm{ww}_{\mathscr{H}(A)}(A', \alpha^{x_1, \ldots, x_n}_{t_1, \ldots, t_n}) = W,$$

d. h. $\mathrm{ww}_{\mathscr{H}(A)}(A'(x_1|t_1,\ldots,x_n|t_n),\alpha) = W$
$\Longleftrightarrow$ für alle $B \in \mathscr{E}(A)$ bei einer gewissen Belegung α gilt:

$$\mathrm{ww}_{\mathscr{H}(A)}(B,\alpha) = W,$$

d. h. alle Ausdrücke aus $\mathscr{E}(A)$ sind erfüllbar. ♣
Kombinieren wir diesen Satz mit dem Endlichkeitssatz der Aussagenlogik, so folgt

2.21. Satz von Herbrand: *Eine Aussage in Skolemform ist genau dann unerfüllbar, wenn es in ihrer Herbrand-Expansion einen aussagenlogisch unerfüllbaren Ausdruck gibt.*

Dieser Satz macht es möglich, wenigstens die Unerfüllbarkeit einer Aussage A in endlich vielen Schritten zu entscheiden, was durch den Gilmore-Algorithmus geschieht:

Eingabe:
A : Ausdruck in Skolemform,
$gibH$: Programm, das bei jedem Aufruf ein neues Element der Herbrand-Expansion eines vorgebenen Ausdrucks liefert; beim ersten Aufruf wird das Programm mit dem gegebenen Ausdruck initialisiert.
Programm:

```
A := gibH(A)
while A ist erfüllbar do
   A := A ∧ gibH
end while
```

Die Unerfüllbarkeit des Ausdrucks $A_1 \wedge A_2 \wedge \ldots \wedge A_n$ kann mit Methoden der Aussagenlogik geprüft werden. Der Gilmore-Algorithmus stoppt bei Eingabe eines unerfüllbaren Ausdrucks nach endlicher Zeit, während er bei Eingabe eines erfüllbaren Ausdrucks niemals stoppt („er schleift unendlich“). Ein solcher Algorithmus heißt **Semi-Entscheidungsverfahren**. Insbesondere haben wir damit gezeigt, dass die Unerfüllbarkeit in Sprachen erster Stufe semi-entscheidbar ist.
Durch Eingabe von $\neg A$ anstelle von A wird aus dem Unerfüllbarkeitstest ein Test auf Allgemeingültigkeit. Daher ist auch die Allgemeingültigkeit semi-entscheidbar.
Der Unerfüllbarkeitstest im Gilmore-Algorithmus kann mit der aussagenlogischen Resolventenmethode durchgeführt werden. Dazu muss die Matrix A' des eingegebenen Ausdrucks A in konjunktiver Standardform vorliegen. Wegen der speziellen Konstruktion der Herbrand-Expansion $\mathscr{E}(A)$ sind dann auch alle Ausdrücke der Herbrand-Expansion in konjunktiver Standardform. Der Gilmore-Algorithmus geht damit in die folgende Resolventen-Methode über. Es sei A eine Aussage in Skolemform mit einer Matrix in konjunktiver Standardform.

Eingabe:
A : Ausdruck in Skolemform,
Res : aussagenlogische Resolventenmethode.
Programm:
$A := gibH(A);\ A := Res(A)$
while $\emptyset \notin A$ do
$A := A \cup gibH;\ A := Res(A)$
end while

Dieser Algorithmus kann erheblich kultiviert werden, indem man für jede Klausel aus A' geeignete Termeinsetzungen sucht, die dann nur auf diese Klausel und nicht auf alle angewendet werden. Es sei die Aussage

$$\forall x \forall y[(\neg Px \vee \neg Pf(a) \vee Qy) \wedge Py \wedge (\neg Pg(b,x) \vee \neg Qb)]$$

gegeben. Daraus folgt die Klauseldarstellung der Matrix

$$\{\{\neg Px, \neg Pf(a), Qy\}, \{Py\}, \{\neg Pg(b,x), \neg Qb\}\}.$$

Wir machen in der 1. Klausel die Termeinsetzung $x|f(a), y|b$, in der 2. Klausel $y|f(a)$ und $y|g(b,a)$ sowie in der 3. Klausel $x|a$. Damit erhalten wir die Klauselmenge

$$\{\{\neg Pf(a), Qb\}, \{Pf(a)\}, \{Pg(b,a)\}, \{\neg Pg(b,a), \neg Qb\}\}.$$

Aus der 1. und 2. Klausel folgt die Resolvente $\{Qb\}$, aus der 3. und 4. Klausel erhalten wir die Resolvente $\{\neg Qb\}$. Folglich ist der Ausgangsausdruck unerfüllbar.

2.8. Axiomatisierbarkeit und Algorithmierbarkeit

Unter einer Theorie erster Stufe versteht man ein Tupel $(S, M, e, R, \mathscr{A}, \mathscr{S}, \mathsf{F})$ mit folgender Bedeutung: Die Menge S enthält alle verwendeten Grundzeichen, M ist die Menge der daraus gebildeten Wörter der Theorie, e repräsentiert das leere Wort, R ist die Verkettungsrelation für Wörter, $\mathscr{A}$ die Ausdrucksmenge, $\mathscr{S}$ die Satzmenge der Theorie und F der zu verwendende Ableitungsoperator. Die Satzmenge kann man sematisch oder syntaktisch definieren. Bei einer semantisch definierten Satzmenge ist $\mathscr{S}$ die Menge aller allgemeingültigen Ausdrücke einer S-Algebra. Bei einer Theorie mit syntaktisch definierter Satzmenge ist ein Axiomensystem $\mathscr{X}$ vorgegeben und $\mathscr{S}$ ist die Ableitungsmenge $\mathsf{F}(\mathscr{X})$. Als Ableitungsoperator wird bei semantisch definierter Satzmenge das logische Folgern und bei syntaktisch definierter Satzmenge das Beweisen genommen. Beide sind umfangsgleich. Eine Theorie erster Stufe ist hinsichtlich des Ableitungsoperators abgeschlossen: $\mathsf{F}(\mathscr{X}) \subseteqq \mathscr{S}$. Die Problemstellungen sind aber unterschiedlich. Bei einer Theorie mit semantisch definierter Satzmenge ist das Problem der Axiomatisierbarkeit wesentlich: Gibt es eine Menge $\mathscr{X}$ – ein Axiomensystem – derart, dass man von jedem Satz der Theorie in endlich vielen Schritten mit dem Ableitungsoperator entscheiden kann, ob er wahr ist oder falsch? Meist fordert man sogar ein endliches Axiomensystem. Bei einer Theorie mit syntaktisch definierter Satzmenge sucht man nach einem Überblick über alle Modelle, d. h. man möchte alle Algebren kennen, in denen die Sätze aus $\mathscr{X}$ gelten. Dabei ist zunächst zu klären, ob die Satzmenge überhaupt ein Modell hat.

Beispiel: Es sei $S = \{\,\mathsf{0}, =, \mathsf{succ}, +, \cdot\,\}$. Als Theorie $\mathscr{T}_1$ betrachten wir die elementare Zahlentheorie, $\mathscr{U} = (\mathbb{N}_0, \omega)$, wobei succ die Nachfolgerbeziehung bedeuten soll, + und · sind die Addition und Multiplikation zwischen natürlichen Zahlen. Dann ist die Satzmenge $\mathscr{S}_1$ die Menge aller wahren Sätze über natürliche Zahlen: $\mathscr{S}_1 = \mathsf{ag}^S(\mathscr{U})$. Die Theorie $\mathscr{T}_2$ sei die Peano-Arithmetik mit der Satzmenge $\mathscr{S}_2$, die aus den Sätzen (Axiomen)

$$
\begin{aligned}
&\forall x(\neg\mathsf{succ}(x) = \mathsf{0}),\\
&\forall x(x + \mathsf{0} = x),\\
&\forall x\forall y[x + \mathsf{succ}(y) = \mathsf{succ}(x+y)],\\
&\forall x(x \cdot \mathsf{0} = \mathsf{0}),\\
&\forall x\forall y(x \cdot \mathsf{succ}(y) = x \cdot y + x),\\
&\text{für jeden Ausdruck } A(x) \text{ gilt:}\\
&A(x|\mathsf{0}) \wedge \forall x[A(x) \rightarrow A(\mathsf{succ}(x))] \rightarrow \forall x A(x)
\end{aligned}
$$

abgeleitet werden kann. Hierin beinhaltet der letzte Ausdruck das Prinzip der vollständigen Induktion. Offenbar ist jeder Satz der Peano-Arithmetik auch ein Satz der elementaren Zahlentheorie: $\mathscr{S}_2 \subseteqq \mathscr{S}_1$. Das angegebene Axiomensystem ist auch grundlegend für mathematische Beweise. Im Jahre 1931 hat K. GÖDEL bewiesen, dass die Inklusion echt ist: $\mathscr{S}_2 \subset \mathscr{S}_1$, d. h. es gibt Sätze der elementaren Zahlentheorie, die nicht aus dem angegebenen Axiomensystem ableitbar sind. Doch Gödels Aussage geht noch weiter: Er bewies ferner, dass es unmöglich ist, ein entscheidbares Axiomensystem für die elementare Zahlentheorie anzugeben. Seine Beweismethode für diese grundlegenden Aussagen lässt keine Illusionen für die Zukunft offen: In seinem Beweis wird ein offensichtlich richtiger Satz der Zahlentheorie angegeben, der nicht aus der Theorie abgeleitet werden kann, wenn man nur Hilfsmittel der Theorie verwendet. Die Schwierigkeiten sollen nun an Algorithmen über natürlichen Zahlen etwas beleuchtet werden. Wir verwenden einen intuitiven Algorithmenbegriff. Ein in einer Programmiersprache geschriebener Algorithmus ist eine Mischung von Operations-, Relations- und Kontrollanweisungen. Wir betrachten eine Programmiersprache – sie soll AL1 heißen –, die als einzige Kontrollanweisung die begrenzte Schleife hat. Als weitere Anweisungen lassen wir zu:

- Addition und Multiplikation natürlicher Zahlen,
- Feststellen, ob zwei natürliche Zahlen gleich sind bzw. welche von ihnen größer oder kleiner ist.

Eine Gruppe von Anweisungen darf nur endlich oft wiederholt werden. Die maximale Anzahl solcher Wiederholungen muss vor Eintritt in die Schleife bekannt sein, notfalls vorher algorithmisch berechnet werden.
Beispiel:

```
Procedure zwei-hoch-zwei-hoch(N)
  a := 1
  for i = 1 to N do
    a := 2 · a
  end for
  b := 1
  for i = 1 to a do
    b := 2 · b
  end for
  out := b
```

Unsere Programmiersprache AL1 gestattet eine modulare Programmierung: Man kann z. B. eine Operation mit natürlichen Zahlen mittels einer Prozedur definieren und diese dann in einer anderen, später definierten Prozedur aufrufen. Gewisse Prozeduren in AL1 repräsentieren Relationen; diese enden im Namen mit „?“ und haben als Ausgabewert „ja“ oder „nein“:

```
Procedure primzahl?(N)
  if n < 2 then
    exit
  end if
  a := 2
  for i = 1 to minus(N,2) do
    if rest(N,a) = 0 then
      break
    else
      a := a + 1
    end if
  end for
  out :=„ja“
```

Hierin ist angenommen, dass neben der Prozedur *minus*(N, m) auch die Prozedur *rest*(N, M) definiert ist, die den Divisionsrest von N/M liefert.
Ein vollständiges AL1-Programm ist eine endliche Folge von Prozedurdefinitionen, von denen jede höchstens vorausgegangene aufrufen darf. Am Ende folgt schließlich eine endliche Folge von Prozeduraufrufen. Ein aufrufloses Programm ist dann ein AL1-Programm ohne Prozeduraufrufe am Ende. Wir nennen eine Funktion **einfach-rekursiv**, wenn sie mittels eines AL1-Programms berechnet werden kann. Relationen, die mit AL1-Programmen untersucht werden können, heißen einfach-rekursive Relationen. So ist z. B. 2^{2^n} eine einfach-rekursive Funktion und „n ist eine Primzahl“ ist eine einfach-rekursive Relation. Nun gilt die folgende Tatsache: Jede Aussage der elementaren Zahlentheorie, die von einem Rechner in vorhersagbar endlicher Zeit entschieden werden kann, ist auch in der Theorie $\mathscr{T}_2$ entscheidbar. Anders: Wenn ein AL1-Programm für eine Relation zwischen natürlichen Zahlen niedergeschrieben werden kann, ist diese Eigenschaft auch in $\mathscr{S}_2$ repräsentiert. Wir stellen die Frage: Kann jede Eigenschaft von natürlichen Zahlen durch ein AL1-Programm aufgefunden werden? Präziser: Kann man stets Obergrenzen für die Anzahl der benötigten Rechenoperationen zum Feststellen einer Eigenschaft der natürlichen Zahlen angeben? Zur Beantwortung dieser Frage setzen wir auf die Menge aller AL1-Programme drei Filter an: Zunächst filtern wir alle aufruflosen Programme heraus. Aus diesen nehmen wir nur die Funktionen. Mit dem dritten Filter erhalten wir schließlich nur jene aufruflosen Programme, die einstellige Funktionen berechnen. Es sei AL1^o die Menge aller aufruflosen AL1-Programme, die Funktionen von genau einer natürlichen Zahl repräsentieren. Jedes dieser Programme besteht aus einer endlichen Anzahl von Zeichen, die wir Länge des Programms nennen. Die Programme aus AL1^o legen wir in Büchern ab. Im Buch N bringen wir alle Programme der Länge N unter. Da jedes Buch nur endlich viele Programme enthält, kann man innerhalb eines Buches alle Programme alphabetisch ordnen. Damit lassen sich alle AL1^o-Programme indizieren; wir bezeichnen die vom i-ten Programm berechnete Funktion mit AL1$^o_i(N)$; dabei ist i die Nummer des Programms und N der einzige Aufrufparameter. Es sei

$$\text{AL1}^n(N) = 1 + \text{AL1}^o_N(N)$$

Nehmen wir nun an, das AL1^n durch ein AL1^o-Programm beschrieben werden kann. Dann muss es nach der obigen Konstruktion einen Index l haben:

$$\text{AL1}^n(N) = \text{AL1}^o_l(N).$$

Berechnen wir nun AL1$^n(l)$; nach Definition erhalten wir einerseits

$$\text{AL1}^n(l) = 1 + \text{AL1}^o_l(l)$$

und nach unserer Annahme

$$\text{AL1}^n(l) = \text{AL1}^o_l(l),$$

was offenbar unmöglich ist. Folglich kann AL1^n keine einfach-rekursive Funktion sein. Unser Ergebnis lautet: Mit AL1-Programmen können nicht alle Funktionen über natürlichen Zahlen aufgeschrieben werden. Als wesentliche Einschränkung hatten wir in AL1 die Begrenztheit seiner Schleifendurchläufe. Diese lassen wir fallen und erhalten so die Programmiersprache AL2. In AL2 können Schleifen so aussehen:

```
loop
    ...
end loop
```

Eine in AL2 programmierbare Funktion heißt **rekursiv**. Auf die AL2-Programme können wir wie oben die drei Filter anwenden und erhalten die Menge aller aufruflosen AL2-Programme, die Funktionen von genau einem Eingabewert berechnen. Wegen der endlosen Schleifen gibt es aber zwei Sorten von AL2-Programmen: endende und nicht-endende. Die endenden Programme kommen bei jeder Eingabe nach endlicher Zeit zum Halten; ein nicht-endendes Programm schleift für mindestens eine Eingabe endlos. Nehmen wir nun an, dass es durch eine Prüfung möglich ist, die endenden von den nicht-endenden Programmen zu unterscheiden. Diese Prüfung übertragen wir einem AL2-Programm. Da wir als Eingabewerte nur natürliche Zahlen akzeptieren, nehmen wir eine Gödelnummerierung der AL2-Programme vor. Es sei also endet?(N) ein AL2-Programm, das „ja“ ausgibt, wenn sein Eingabewert die Gödel-Nummer eines endenden AL2-Programms ist und sonst „nein“. Natürlich muss endet?(N) ein endendes Programm sein. Dieses Programm verwenden wir nun als vierten Filter und erhalten so die Menge AL2^e aller aufruflosen, endenden AL2-Programme, die einstellige Funktionen berechnen. Analog zu oben lassen sich die Programme aus AL2^e indizieren; wir können

$$\text{AL2}^n(N) = 1 + \text{AL2}^e_N(N)$$

bilden und erhalten, dass AL2^n kein AL2-Programm ist. Daher müssen wir AL2 erweitern. Aber welche Einschränkung hat AL2? Die Funktion AL2$^n(N)$ kann von jedem Menschen prinzipiell berechnet werden; sie lässt sich aber nicht in AL2 programmieren. Üblicherweise werden Programmiersprachen konstruiert, die im Leistungsumfang mit AL2 übereinstimmen. Es gibt keine leistungsfähigere Programmiersprache als AL2. Damit haben wir auch keine Möglichkeit, AL2 zu erweitern. Wir können sagen: AL2$^n(N)$ ist für jede natürliche Zahl N von Menschen berechenbar; es gibt aber keine Methode zur Programmierung. Unsere Konstruktion beruht auf der Annahme, dass es eine stets endende Methode gibt, die endende Programme von nicht-endenden unterscheiden kann. Also müssen wir schließen: Das Programm endet?(N) gibt es nicht. Daraus resultiert die **Church’sche These** in etwa folgenden Versionen:

- Was Menschen berechnen können, können auch Maschinen berechnen.
- Was Maschinen berechnen können, kann man in AL2 programmieren.
- Was Menschen berechnen können, lässt sich in AL2 programmieren.
- Jede berechenbare Funktion ist rekursiv.

Es sei noch ein anderer Gesichtspunkt erwähnt: Die einstelligen Funktionen AL1^n und AL2^n sind mittels unendlich vieler Anweisungen repräsentiert. So muss das Programm AL1^n alle Programme aus AL1^o enthalten, damit es bei jeder Eingabe N ausgeführt werden kann, obwohl für jede Eingabe immer nur endlich viele Anweisungen, nämlich die Anweisungen eines AL1^o-Programms, ausgeführt werden. Damit sind die obigen Realisierungen der Funktionen AL1^n und AL2^n keine Programme.

2.9. Übungen

1. Man gebe in geordneter Reihenfolge alle ein- und zweistelligen Wahrheitsfunktionen in Form einer Wahrheitstafel an. Weiterhin drücke man alle zweistelligen Wahrheitsfunktionen nur mit Hilfe von $\neg$ und $\vee$ aus.

2. Ist es möglich, alle zweistelligen Wahrheitsfunktionen nur mit Hilfe der Operatoren

   (a) $\neg$ und $\rightarrow$,

   (b) $\neg$ und $\leftrightarrow$

   auszudrücken?

3. Auf der Suche nach einem Schatz kam Märchenman an eine Weggabelung, von der aus ein Weg nach links und einer nach rechts führte. Dort traf er einen Jungen, über den geweissagt wurde, dass er nur mit „ja“ oder „nein“ antwortet und dass er einem Fremden gegenüber entweder immer die Wahrheit sagt oder immer lügt. Außerdem beantwortet er nur eine einzige Frage. Welche Frage muss unser tapferer Held stellen, um mit Sicherheit den richtigen Weg zu wählen?

4. Man zeige mittels

   (a) indirekten Beweises,

   (b) Resolventenmethode,

dass die beiden Ausdrücke

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

$$(p \to q) \leftrightarrow (\neg q \to \neg p)$$

allgemeingültig sind.

5. Man beweise mit Hilfe von

   - $\neg\neg p \cong p$,
   - $p \vee q \cong q \vee p$,
   - $\neg(p \vee q) \cong (\neg p \wedge \neg q)$,
   - $\neg(p \wedge q) \cong (\neg p \vee \neg q)$,
   - $p \wedge (q \vee r) \cong (p \wedge q) \vee (p \wedge r)$,
   - $p \to q \cong \neg p \vee q$

   folgende semantische Äquivalenzen:

   (a) $p \vee (q \wedge r) \cong (p \vee q) \wedge (p \vee r)$,

   (b) $(p \vee q) \to r \cong (p \to r) \wedge (q \to r)$.

6. Man überführe den folgenden Ausdruck in eine konjunktive und danach in eine alternative Standardform (oder umgekehrt):

$$\neg(q \vee ((p \leftrightarrow \neg q) \wedge \neg p) \vee (r \wedge \neg q)) \wedge (p \to r) \wedge p.$$

7. Man überführe folgende Ausdrücke in alternative und konjunktive Standardformen:

   (a) $p \wedge q$,

   (b) $p \vee q$,

   (c) $p \to q$,

   (d) $p \leftrightarrow q$,

   (e) $(p \vee q) \to (p \vee r)$,

   (f) $(p \wedge q) \leftrightarrow (p \wedge r)$.

   Man gebe für die ersten vier Ausdrücke die alternative Normalform an.

8. Gegeben sei eine Menge $\mathscr{X}$ von logischen Ausdrücken:

$$\mathscr{X} = \left\{ \begin{array}{l} p \wedge q \to p, p \wedge q \to q, (p \to q) \to ((p \to r) \to (p \to q \wedge r)), \\ (p \to q) \to ((q \to p) \to (p \leftrightarrow q)) \end{array} \right\}.$$

   Man zeige die syntaktische Äquivalenz von $p \wedge q$ und $q \wedge p$ bezüglich der Menge $\mathscr{X}$.

9. Es sei A ein Ausdruck, der die Variablen $p_1, p_2, \ldots, p_n$ enthält.
   $k_1 \vee k_2 \vee \cdots \vee k_m$ sei die alternative Normalform von A.

   (a) Wie oft tritt der Funktor $\vee$ in der alternativen Normalform des Ausdrucks $\neg A$ auf?

   (b) Wie oft kommt der Funktor $\wedge$ in der konjunktiven Normalform des Ausdrucks $\neg A$ vor?

10. Man gebe für die Ausdrücke A_1 und A_2 mit folgenden Belegungen möglichst kurze alternative Standardformen an.

$\alpha(p)$	$\alpha(q)$	$\alpha(r)$	$ww(A_1, \alpha)$	$ww(A_2, \alpha)$
W	W	W	F	W
W	W	F	W	W
W	F	W	F	F
W	F	F	W	W
F	W	W	W	W
F	W	F	W	W
F	F	W	F	F
F	F	F	F	F

11. Man prüfe, ob die Ausdrücke $\neg(p \wedge q)$ und $\neg p \wedge \neg q$ semantisch bzw. syntaktisch äquivalent bezüglich der Ausdrucksmenge X sind, wobei

$$X = \left\{ \begin{array}{l} (p \to q) \to ((q \to p) \to (p \leftrightarrow q)), \\ (p \to q) \to ((p \to r) \to (p \to q \wedge r)), p \to p \wedge q, \\ q \to p \wedge q, (p \to q) \to (\neg q \to \neg p), \neg p \wedge \neg q \to \neg r \end{array} \right\}.$$

12. Man überprüfe folgende Ausdrücke mit Hilfe der Resolventenmethode auf Erfüllbarkeit bzw. Allgemeingültigkeit.

   (a) $(p \vee q \vee r) \wedge (\neg p \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r)$,

   (b) $(p \vee q) \wedge (p \vee \neg q \vee r) \wedge (q \vee \neg r) \wedge (r \vee \neg r)$,

(c) $(p \vee q \vee \neg p) \wedge (q \vee \neg q \vee r) \wedge (r \vee p \vee \neg r)$,

(d) $\neg(q \vee ((p \leftrightarrow \neg q) \wedge \neg p) \vee (r \wedge \neg q)) \wedge (p \rightarrow r) \wedge p$.

13. Man überprüfe folgende Ausdrücke mit dem Horn-Algorithmus auf Erfüllbarkeit.

    (a) $(\neg p \vee q) \wedge (\neg p \vee \neg r \vee \neg s) \wedge (\neg p \vee \neg q) \wedge r \wedge \neg s$,

    (b) $(\neg q \vee \neg r) \wedge (\neg p \vee q) \wedge p \wedge r \wedge (\neg q \vee \neg r \vee s)$,

    (c) $(\neg q \vee \neg p \vee \neg r) \wedge (\neg q \vee p) \wedge q \wedge r$,

    (d) $(\neg p \vee q) \wedge (\neg q \vee r) \wedge s \wedge (s \vee \neg r) \wedge (\neg q \vee \neg p \vee r) \wedge r$.

14. Man beweise:

    (a) $p \rightarrow p \in \mathsf{Ab}(\mathsf{Axa})$,

    (b) $p \leftrightarrow p \wedge p \in \mathsf{Ab}(\mathsf{Axa})$,

    (c) $p \vee q \leftrightarrow q \vee p \in \mathsf{Ab}(\mathsf{Axa})$.

15. Nach angestrengter Arbeit legten sich drei Philosophen in den Schatten eines Baumes und hielten ein Mittagsschläfchen. Während sie schliefen, kam ein Schelm vorbei und schwärzte ihnen die Gesichter. Als die Philosophen erwachten, lachten sie lauthals los. Aber bald hörte der klügste von ihnen auf zu lachen, denn er wusste, dass auch sein Gesicht schwarz war. Wie konnte er dies mit Sicherheit folgern?

16. Man leite folgendes aus Axa ab:

    (a) $\neg(p \vee q) \rightarrow \neg p \wedge \neg q$,

    (b) $\neg p \vee q \rightarrow (p \rightarrow q)$.

17. Man realisiere einen Dual-Adder ausschließlich mit Hilfe von NAND- und NOR-Schaltungen:

    (a) $\mathrm{NAND}_1(p) = \neg p$,

    (b) $\mathrm{NAND}_2(p, q) = \neg(p \wedge q)$,

    (c) $\mathrm{NAND}_3(p, q, r) = \neg(p \wedge q \wedge r)$,

    (d) $\mathrm{NOR}_2(p, q) = \neg(p \vee q)$,

    (e) $\mathrm{NOR}_3(p, q, r) = \neg(p \vee q \vee r)$.

18. Man wähle S, U, ω und gebe Ausdrücke aus folgenden Mengen an:

(a) ag^S,

(b) $\mathsf{ag}^S(U)\backslash\mathsf{ag}^S$,

(c) $\mathsf{ag}^S(\mathscr{U})\backslash\mathsf{ag}^S(U)$.

19. Gegeben sei die Signatur $S = (\{a_0\},\{R\},\{f,g\})$, wobei R ein zweistelliges Relationssymbol, f ein einstelliges und g ein zweistelliges Operationssymbol bezeichnen.
Sind folgende Wörter auch Ausdrücke? Wenn ja, in welchen kommen Variable abs-frei, in welchen rel-frei vor?

    (a) $\exists p \forall x f(x) x R p$,

    (b) $\forall\varepsilon\exists\delta\forall x(R(x,x_0)\delta Rg(f(x),f(x_0))\varepsilon)$,

    (c) $Rg(g(\alpha\beta),\gamma)a_0$,

    (d) $\exists x(((xR\alpha \vee xR\beta)\vee xR\gamma)\wedge f(a_0)Rx)$.

20. In $S = (\{a_0\},\{R\},\{f_1,f_2,g\})$ mit R zweistellig, f_1,f_2 einstellig, g zweistellig seien folgende Ausdrücke gegeben:

$$g(f_1(x),f_2(x))Ra_0,$$

$$\exists x f_1(x)Rg(f_2(y),a_0).$$

Weiter seien auf der Trägermenge $\mathbb{R}$ folgende Interpretationen ω_1,ω_2 von S gegeben:

$$\begin{array}{llll}
a_0^{\omega_1} = 1, & & a_0^{\omega_2} = 0 & \\
xR^{\omega_1}y \iff & x = y, & xR^{\omega_2}y \iff & x < y, \\
f_1^{\omega_1}(x) = \sin^2 x, & & f_1^{\omega_2}(x) = \mid x \mid, & \\
f_2^{\omega_1}(x) = \cos^2 x, & & f_2^{\omega_2}(x) = \mid x \mid, & \\
g^{\omega_1}(x,y) = x+y, & & g^{\omega_2}(x,y) = x+y. &
\end{array}$$

Zu welchen der folgenden Mengen gehören die genannten Ausdrücke?

$\mathsf{ag}^S(\mathscr{U}_1)$, $\mathsf{erf}^S(\mathscr{U}_1)$, $\mathsf{ag}^S(\mathscr{U}_2)$, $\mathsf{erf}^S(\mathscr{U}_2)$, $\mathsf{ag}^S(\mathbb{R})$, $\mathsf{erf}^S(\mathbb{R})$,

wobei $\mathscr{U}_1 = (\mathbb{R},\omega_1)$, $\mathscr{U}_2 = (\mathbb{R},\omega_2)$.

21. Gegeben sei $S = (\{a_1,a_2\},\{R\},\{f,g,h\})$ (R zweistellig, f einstellig, g,h zweistellig) sowie die beiden S-Algebren $\mathscr{U}_1,\mathscr{U}_2$, wobei

$$\mathscr{U}_1 = (U_1,\omega_1), \quad U_1 = \{W,F\},$$

$$a_1^{\omega_1} = W, \quad a_2^{\omega_1} = F$$

$$xR^{\omega_1}y \quad \Longleftrightarrow \quad x = y$$

$$f^{\omega_1}(x) = \neg x, \quad g^{\omega_1}(x,y) = x \wedge y, \quad h^{\omega_1}(x,y) = x \vee y$$

$$\mathscr{U}_2 = (U_2, \omega_2), \quad U_2 = \{0,1,2,\ldots,15\},$$

$$a_1^{\omega_2} = 15, \quad a_2^{\omega_2} = 0,$$

$$xR^{\omega_2}y \quad \Longleftrightarrow \quad (x \leqq 7 \text{ und } y \leqq 7) \text{ oder } (x > 7 \text{ und } y > 7)$$

$$(f^{\omega_2}(x) = 15 - x, \quad g^{\omega_2}(x,y) = \min(x,y), \quad h^{\omega_2}(x,y) = \max(x,y).$$

(a) Man überlege sich einen Homomorphismus von $\mathscr{U}_2$ auf $\mathscr{U}_1$ und prüfe alle Homomorphieeigenschaften.

(b) Man interpretiere folgende Ausdrücke in $\mathscr{U}_2$ und entscheide über den Wahrheitswert:
$\forall x h(a_2, x) R x$,
$\forall x g(x, f(x)) R a_2$.

(c) Mit Hilfe des Homomorphismus bilde man die Interpretation dieser Ausdrücke in $\mathscr{U}_1$ und kontrolliere sie, indem die Werte direkt in $\mathscr{U}_1$ berechnet werden.

22. Man zeige die Beweisbarkeit folgender prädikatenlogischer Sätze

(a) $\exists x(A(x) \vee B(x)) \leftrightarrow \exists x A(x) \vee \exists x B(x)$,

(b) $\forall x \neg A(x) \leftrightarrow \neg \exists x A(x)$.

23. Gegeben seien $\mathscr{X}_1 = \{\, xRy \to \neg xRy \,\}$ und $\mathscr{X}_2 = \{\, \neg xRy \to xRy \,\}$.

(a) Man finde ein Modell für $\mathscr{X}_1$.

(b) Gibt es ein Modell für $\mathscr{X}_1 \cup \mathscr{X}_2$?

(c) Man zeige:
$xRy \leftrightarrow \neg xRy \in \mathsf{Fl}^S(\mathscr{X}_1 \cup \mathscr{X}_2)$.

24. Man untersuche, ob die folgenden beiden Ausdrücke allgemeingültig in jeder Algebra sind:

(a) $\exists x(A(x) \wedge B(x)) \to \exists x A(x) \wedge \exists x B(x)$,

(b) $\exists x A(x) \wedge \exists x B(x) \to \exists x(A(x) \wedge B(x))$.

25. Mit Hilfe der Prämissenverbindung zeige man die Beweisbarkeit des Ausdruckes

$$\forall x(A^* \to A(x)) \to (A^* \to \forall x A(x)),$$

wobei A^* ein Ausdruck sei, in dem x nicht vorkommt.

26. Man überführe die folgenden Ausdrücke in eine pränexe Normalform und eine Skolemform:

(a) $\forall x(\forall y x R y \to P x) \to \forall x x R y,$

(b) $\exists x(\forall y x R_1 y \leftrightarrow \forall z z R_2 x) \to \forall x x R_3 t.$

27. Man teste die folgenden Ausdrücke auf Unerfüllbarkeit:

(a) $\neg\exists x x R_1 y \land \neg(\exists x x R_1 y \to \exists z y R_2 z),$

(b) $\forall y((\forall x \neg x R_1 y \to \exists z b R_2 z) \land \forall u \neg u R_1 y \land \forall z \neg b R_2 z) \land \exists y y R_3 a.$

Bemerkung: a, b seien Konstantensymbole.

28. Man gebe eine Signatur und eine Ausdrucksmenge an, so dass euklidische Vektorräume Modell dieser Ausdrucksmenge sind.

Index