Logik

Prof. Dr. Madlener

TU Kaiserslautern

SS 2011

Logik

Studiengang „Informatik“, „Ang. Informatik“und „ WiWi/Inf“
SS’11
Prof. Dr. Madlener TU - Kaiserslautern

Vorlesung:
Mi 11.45-13.15 52/207

- Informationen
  http://www-madlener.informatik.uni-kl.de/teaching/ss2011/logik/logik.html
- Grundlage der Vorlesung: Skript
  Einführung in die Logik und Korrektheit von Programmen.

- Bewertungsverfahren:
  Zulassungsvoraussetzungen zu Abschlussklausur:
  Übungen: mind. 50 %
  Aufsichtsarbeit: mind. 50 %
- Aufsichtsarbeit: Vor. Freitag 1/06/11
- Abschlussklausur: 2011 /17.08/ ?.10
- Übungen: Gruppen
  Einschreiben, Sprechzeiten siehe Homepage

Einleitung

Methoden zur Lösung von Problemen mit Hilfe von Rechnern Formalisierung ($\equiv$ Festlegung)

- **Logik::** „Lehre vom folgenrichtigen Schließen“ bzw. „Lehre von formalen Beziehungen zwischen Denkinhalten“

Zentrale Fragen: Wahrheit und Beweisbarkeit von Aussagen $\rightsquigarrow$ **Mathematische Logik**.

- **Logik in der Informatik**:
  - **Aussagenlogik**: Boolsche Algebra. Logische Schaltkreise (Kontrollsystemen), Schaltungen, Optimierung.
  - **Prädikatenlogik**: Spezifikation und Verifikation von Softwaresystemen.
  - **Modal- und Temporallogik**: Spezifikation und Verifikation reaktiver Systeme.

Logik in der Informatik

1. Semantik von Programmiersprachen (Hoarscher Kalkül).
2. Spezifikation von funktionalen Eigenschaften.
3. Verifikationsprozess bei der SW-Entwicklung.
   Beweise von Programmeigenschaften.
4. Spezielle Programmiersprachen (z.B. PROLOG)

- **Automatisierung des logischen Schließens**
  1. Automatisches Beweisen (Verfahren,...)
  2. Grundlagen von Informationsystemen (Verarbeitung von Wissen, Reasoning,. . .)

Voraussetzungen

1. **Mathematische Grundlagen**. Mengen, Relationen, Funktionen. Übliche Formalisierungen: „Mathematische Beweise“, Mathematische Sprache, d.h. Gebrauch und Bedeutung der üblichen Operatoren der naiven Logik. Also Bedeutung von **nicht, und, oder, impliziert, äquivalent, es gibt, für alle**.
2. **Grundlagen zur Beschreibung formaler Sprachen**. Grammatiken oder allgemeiner **Kalküle** (Objektmenge und Regeln zur Erzeugung neuer Objekte aus bereits konstruierter Objekte), Erzeugung von Mengen, Relationen und Funktionen, Hüllenoperatoren (Abschluss von Mengen bzgl. Relationen).
3. **Vorstellung von Berechenbarkeit**, d.h. entscheidbare und rek.aufzählbare Mengen, Existenz nicht entscheidbarer Mengen und nicht berechenbarer Funktionen.

Berechnungsmodelle/Programmiersprachen

Algorithmische Unlösbarkeit?

prinzipielle Lösbarkeit

$\downarrow$

effiziente Lösbarkeit

$\downarrow$

algorithmischer Entwurf

$\downarrow$

P: Programm in einer HPS

Problem
Spezifikation

(Formalisiert)

Syntaktische und semantische Verifikation von P.

- **Syntaxanalyse**
  Sprachen Chomski-Hierarchie
  Kontext freie Sprachen
  Grammatiken/Erzeugungsprozess

- **Programmverifikation**
  Tut P auch was erwartet wird.
  Gilt $P \rightsquigarrow$ Problem Spezifikation

Typische Ausdrücke

- $(x+1)(y-2)/5$ Terme als Bezeichner von Objekten.
- $3+2=5$ Gleichungen als spezielle Formeln.
- „29 ist (k)eine Primzahl " Aussagen.
- „$3+2=5$ und 29 ist keine Primzahl " Aussage.
- „wenn 29 keine Primzahl ist, dann ist $0=1$ " Aussage.
- „jede gerade Zahl, die größer als 2 ist, ist die Summe zweier Primzahlen " Aussage.
- $2 \leq x$ und $(\forall y \in \mathbb{N})$
  $((2 \leq y$ und $y+1 \leq x) \rightarrow$ nicht$(\exists z \in \mathbb{N}) y * z = x)$
  Aussage.

Typische Ausdrücke (Fort.)

- $(\forall X \subseteq \mathbb{N})(0 \in X \wedge (\forall x \in \mathbb{N})(x \in X \rightarrow x+1 \in X) \rightarrow X = \mathbb{N})$
  Induktionsprinzip.
- $(\forall X \subseteq \mathbb{N})(X \neq \emptyset \rightarrow X$ hat ein kleinstes Element$)$
  Jede nichtleere Menge natürlicher Zahlen enthält ein minimales Element.

Zweiwertige Logik Jede Aussage ist entweder **wahr** oder **falsch**.

- Es gibt auch andere Möglichkeiten (Mehrwertige Logik).
- Prädikatenlogik erster Stufe (PL1): Nur Eigenschaften von Elementen und Quantifizierung von Elementvariablen erlaubt.

Kapitel I

Grundlagen der Aussagenlogik

Aussagenlogik

- Aussagen $\rightsquigarrow$ Bedeutung **wahr**(1), **falsch** (0)
- Aufbau von Aussagen $\rightsquigarrow$ **Syntax**.
- Bedeutung von Aussagen $\rightsquigarrow$ **Semantik**.

Syntax

Definition 1.1 (Syntax)

Die Sprache der Aussagenlogik
Sei $\Sigma = V \cup O \cup K$ Alphabet mit $V = \{p_1, p_2, \ldots\}$ abzählbare Menge von **Aussagevariablen**, $O = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \ldots\}$ Menge von **Verknüpfungen** mit Stelligkeiten (Junktoren, Operatoren) und $K = \{(,)\}$ **Klammern** Hilfssymbole.
Die Menge der **Aussageformen** (Formeln der Aussagenlogik) $F \subset \Sigma^*$ wird induktiv definiert durch:

1. $V \subset F$ Menge der **atomaren Aussagen**
2. $A, B \in F$ so $(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B) \in F$
3. F ist die kleinste Menge die V enthält und 2. erfüllt (Hüllenoperator)

Bemerkung 1.2

- *Eigenschaften von Elementen in F werden durch* **strukturelle Induktion***, d.h. durch Induktion über den Aufbau der Formeln, nachgewiesen.*
- *Beispiele für Eigenschaften sind:*
  1. *Für $A \in F$ gilt: A ist atomar (ein p_i) oder beginnt mit „(“ und endet mit „)“.*
  2. *Sei $f(A, i) = \sharp$ „(“$- \sharp$ „)“ in den ersten i Buchstaben von A, dann gilt $f(A, i) > 0 \quad$ für $1 \leq i < |A|$ und $f(A, i) = 0$ für $i = |A|$.*
- *F kann als Erzeugnis einer Relation $R \subset U^* \times U$ mit $U = \Sigma^*$ oder eines Kalküls dargestellt werden. Dabei wird F frei von dieser Relation erzeugt, da für alle $u, v \in U^*$ und $A \in F$ gilt: uRA und vRA so $u = v$.*
- *$F = L(G)$ für eine eindeutige kontextfreie Grammatik G.*

Satz 1.3 (Eindeutigkeitssatz)

Jede A-Form $A \in F$ ist entweder atomar oder sie lässt sich eindeutig darstellen als
$A \equiv (\neg A_1)$ *oder* $A \equiv (A_1 * A_2)$ *mit* $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ *wobei* $A_1, A_2 \in F$.

Beweis: Induktion über Aufbau von F.

Vereinbarungen

Schreibweisen, Abkürzungen, Prioritäten.

- Äußere Klammern weglassen.
- A-Formen sind z.B.: p_1, p_{101},
  $p_1 \vee p_{12}$ als Abkürzung für $(p_1 \vee p_{12})$,
  $(((p_1 \rightarrow p_2) \wedge (\neg p_2)) \rightarrow (\neg p_1))$, $p_1 \vee (\neg p_1)$
- Zur besseren Lesbarkeit: Prioritäten: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ d.h.
  $A \wedge B \rightarrow C$ steht für $((A \wedge B) \rightarrow C)$
  $A \vee B \wedge C$ steht für $(A \vee (B \wedge C))$
  $\neg A \vee B \wedge C$ steht für $((\neg A) \vee (B \wedge C))$
  $A \vee B \vee C$ steht für $((A \vee B) \vee C)$ (Linksklammerung).
- Andere Möglichkeiten. „Präfix“- oder „Suffix“- Notation
  Für $(A * B)$ schreibe $*AB$ und für $(\neg A)$ schreibe $\neg A$

Semantik

Definition 1.4 (Bewertung, Belegung)

Eine **Bewertung** der A-Formen ist eine Funktion
$\varphi : F \to \{0, 1\} = \mathbb{B}$ mit

1. $\varphi(\neg A) = 1 - \varphi(A)$
2. $\varphi(A \vee B) = max(\varphi(A), \varphi(B))$
3. $\varphi(A \wedge B) = min(\varphi(A), \varphi(B))$
4. $\varphi(A \to B) = \begin{cases} 0 & \text{falls } \varphi(A) = 1 \text{ und } \varphi(B) = 0 \\ 1 & \text{sonst} \end{cases}$
5. $\varphi(A \leftrightarrow B) = \begin{cases} 0 & \text{falls } \varphi(A) \neq \varphi(B) \\ 1 & \text{falls } \varphi(A) = \varphi(B) \end{cases}$

Belegungen und Bewertungen (Fort.)

- Sprechweise: A ist „falsch“ unter φ, falls $\varphi(A) = 0$
  A ist „wahr“ unter φ oder φ „erfüllt“ A, falls $\varphi(A) = 1$.
- Darstellung von Bewertungen durch **Wahrheitstafeln**:

A	$\neg A$
1	0
0	1

A	B	$A \vee B$	$A \wedge B$	$A \rightarrow B$	$A \leftrightarrow B$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

Belegungen und Bewertungen (Fort.)

- Eine **Belegung** der *A*-Variablen V ist eine Funktion $\psi : V \to \mathbb{B}$.
- Offenbar induziert jede Bewertung eine Eindeutige Belegung durch $\psi(p_i) := \varphi(p_i)$.

Lemma 1.5

Jede Belegung $\psi : V \to \mathbb{B}$ *lasst sich auf genau eine Weise zu einer Bewertung* $\varphi : F \to \mathbb{B}$ *fortsetzen. Insbesondere wird jede Bewertung durch die Werte auf* V *eindeutig festgelegt.*

Bewertungen

Folgerung 1.6

Die Bewertung einer Aussageform $A \in F$ hängt nur von den Werten der in ihr vorkommenden Aussagevariablen aus V ab. Das heißt, will man $\varphi(A)$ berechnen, genügt es, die Werte $\varphi(p)$ zu kennen für alle Aussagevariablen p, die in A vorkommen.

- Beispiel: Sei $\varphi(p) = 1, \varphi(q) = 1, \varphi(r) = 0$. Dann kann $\varphi(A)$ iterativ berechnet werden:

$$A \equiv \underbrace{(\underbrace{(\underbrace{p}_{1} \to \underbrace{(\underbrace{q}_{1} \to \underbrace{r}_{0})}_{0})}_{0} \to \underbrace{(\underbrace{(\underbrace{p}_{1} \wedge \underbrace{q}_{1})}_{1} \to \underbrace{r}_{0})}_{0})}_{1}$$

Also gilt $\varphi(A) = 1$.

- **Frage** Welche Werte kann $\varphi(A)$ annehmen, wenn φ alle Belegungen durchläuft. Ist etwa $\varphi(A) = 1$ für alle Belegungen φ? Um das nachzuprüfen, „genügt“ es, die endlich vielen unterschiedlichen Belegungen der Variablen, die in A vorkommen, zu überprüfen. Kommen n Variablen in A vor, so gibt es 2^n verschiedene Belegungen.

A definiert eine Boolesche Funktion $f_A : \mathbb{B}^n \to \mathbb{B}$.

- Beispiel: Für die drei Variablen p, q und r aus A im obigen Beispiel gibt es 8 Belegungen, die betrachtet werden müssen.

Bewertungen

p	q	r	$q \rightarrow r$	$p \wedge q$	$p \rightarrow (q \rightarrow r)$	$(p \wedge q) \rightarrow r$	A
0	0	0	1	0	1	1	1
0	0	1	1	0	1	1	1
0	1	0	0	0	1	1	1
0	1	1	1	0	1	1	1
1	0	0	1	0	1	1	1
1	0	1	1	0	1	1	1
1	1	0	0	1	0	0	1
1	1	1	1	1	1	1	1

A ist „wahr“ unabhängig von den Werten von p, q, r, d.h. für jede Bewertung φ. Weitere solche Formeln sind etwa: $(A \rightarrow (B \rightarrow A))$, $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$ oder $((\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A))$.

Wichtige Begriffe

Definition 1.7

Sei $A \in F$, $\Sigma \subseteq F$.

1. (a) A heißt **Tautologie** (**allgemeingültig**), falls $\varphi(A) = 1$ für jede Bewertung φ gilt. (Schreibweise "$\models A$")
   (b) A ist **erfüllbar**, falls es eine Bewertung φ gibt, mit $\varphi(A) = 1$.
   (c) A ist **widerspruchsvoll**, falls $\varphi(A) = 0$ für jede Bewertung φ.
   (d) Schreibe
   - Taut $= \{A \mid A \in F \text{ ist Tautologie}\}$, die Menge der Tautologien oder „Theoreme“ der Aussagenlogik, bzw.
   - Sat $:= \{A \mid A \in F \text{ und } A \text{ ist erfüllbar}\}$ die Menge der erfüllbaren Formeln.

Definition (Fort.)

2.(a) Σ ist **erfüllbar**, falls es eine Bewertung φ gibt mit $\varphi(A) = 1$ für alle $A \in \Sigma$. (“φ **erfüllt** Σ”)

(b) **Semantischer Folgerungsbegriff:** A ist **logische Folgerung** von Σ, falls $\varphi(A) = 1$ für jede Bewertung φ, die Σ erfüllt.

Man schreibt “$\Sigma \models A$”.
Ist $\Sigma = \{A_1, \dots, A_n\}$, ist die Kurzschreibweise “$A_1, \dots, A_n \models A$” üblich.

(c) Die Menge Folg(Σ) der Folgerungen aus Σ ist definiert durch:

$$\mathrm{Folg}(\Sigma) := \{A \mid A \in F \text{ und } \Sigma \models A\}.$$

Einfache Folgerungen

Bemerkung 1.8

Beispiele

1. $(p \vee (\neg p))$, $((p \to q) \vee (q \to r))$, $p \to (q \to p)$, $(p \to p)$, $(p \to \neg\neg p)$ *und* A *aus Folgerung 1.6 sind Tautologien.*

   $(p \wedge (\neg p))$ *ist widerspruchsvoll.*
   $A \in \mathrm{Taut}$ *gdw* $\neg A$ *widerspruchsvoll*

   $(p \wedge q)$ *ist erfüllbar jedoch keine Tautologie und nicht widerspruchsvoll.*

   Die Mengen $\mathrm{Taut}, \mathrm{Sat}$ *sind entscheidbar.*

   Beachte $\mathrm{Taut} \subset \mathrm{Sat}$.

Bemerkung (Fort.)

2.(a) *Sei* $\Sigma = \{p\}$ *und* $A = p \vee q$. *Dann gilt* $\Sigma \models A$, *denn falls* $\varphi(p) = 1$, *dann auch* $\varphi(p \vee q) = 1$. *Jede Bewertung, die* Σ *erfüllt, erfüllt also auch* A.

(b) *Ist* $\Sigma = \emptyset$, *dann gilt* $\Sigma \models A$ *genau dann, wenn* A *Tautologie ist, d.h.* $\mathrm{Folg}(\emptyset) = \mathrm{Taut}$.

(c) *Ist* Σ *nicht erfüllbar, dann gilt* $\Sigma \models A$ *für alle* $A \in F$, *d.h.* $\mathrm{Folg}(\Sigma) = F$. *Insbesondere* $\Sigma \models A, \neg A$ *für ein* A.

(d) *Sei* $\Sigma \subseteq \Sigma'$. *Ist* Σ' *erfüllbar, dann ist auch* Σ *erfüllbar.*

(e) *Es gilt* $\Sigma \subseteq \mathrm{Folg}(\Sigma)$ *und* $\mathrm{Folg}(\mathrm{Folg}(\Sigma)) = \mathrm{Folg}(\Sigma)$.

(f) *Falls* $\Sigma \subseteq \Sigma'$, *dann gilt* $\mathrm{Folg}(\Sigma) \subseteq \mathrm{Folg}(\Sigma')$.

3. $\Sigma \models A$ *gilt genau dann, wenn* $\Sigma \cup \{\neg A\}$ *nicht erfüllbar.*
Ist Σ *endlich, dann ist es entscheidbar, ob* Σ *erfüllbar ist, und die Menge* $\mathrm{Folg}(\Sigma)$ *ist entscheidbar.*

Deduktionstheorem und Modus-Ponens Regel

Lemma 1.9

a) **Deduktionstheorem**:

$$\Sigma, A \models B \qquad \text{gdw} \qquad \Sigma \models (A \to B).$$

(Σ, A ist Kurzschreibweise für $\Sigma \cup \{A\}$)

b) **Modus-Ponens-Regel**:
Es gilt $\quad \{A, A \to B\} \models B.$

Insbesondere ist B eine Tautologie, falls A und $(A \to B)$ Tautologien sind.

Übliche Notationen für Regeln der Form "$A_1, \ldots, A_n \models B$" sind:

$$\begin{array}{c} A_1 \\ \vdots \\ A_n \\ \hline B \end{array} \quad \text{und} \quad \frac{A_1, \ldots, A_n}{B}$$

Für die Modus Ponens Regel also:

$$\frac{A, (A \rightarrow B)}{B} \; (\textbf{MP})$$

Kompaktheitssatz der Aussagenlogik

Satz 1.10 (Kompaktheitssatz)

$\Sigma \subseteq F$ ist erfüllbar genau dann, wenn jede endliche Teilmenge von Σ erfüllbar ist.

$\Sigma \subseteq F$ ist unerfüllbar genau dann, wenn es eine unerfüllbare endliche Teilmenge von Σ gibt.

Insbesondere gilt $\Sigma \models A$ genau dann, wenn es eine endliche Teilmenge $\Sigma_0 \subseteq \Sigma$ gibt mit $\Sigma_0 \models A$.

Anwendungen Kompaktheitssatz

Beispiel 1.11

Sei $\Sigma \subseteq F$. Gibt es zu jeder Bewertung φ ein $A \in \Sigma$ mit $\varphi(A) = 1$, so gibt es $A_1, \dots, A_n \in \Sigma$ $(n > 0)$ mit $\models A_1 \vee \dots \vee A_n$.

- Betrachte die Menge $\Sigma' = \{\neg A \mid A \in \Sigma\}$, nach Voraussetzung ist sie unerfüllbar. Also gibt es eine endliche nichtleere Teilmenge $\{\neg A_1, \dots, \neg A_n\}$ von Σ' die unerfüllbar ist. Also gilt für jede Bewertung φ gibt es ein i mit $\varphi(\neg A_i) = 0$ oder $\varphi(A_i) = 1$ und somit $\varphi(A_1 \vee \dots \vee A_n) = 1$.

- Der zweite Teil des Satzes ist die Grundlage für Beweisverfahren für $\Sigma \models A$. Dies ist der Fall wenn $\Sigma \cup \{\neg A\}$ unerfüllbar ist.
  Widerspruchbeweise versuchen systematisch eine endliche Menge $\Sigma_0 \subset \Sigma$ zu finden, so dass $\Sigma_0 \cup \{\neg A\}$ unerfüllbar ist.

Logische Äquivalenz

Definition 1.12 (Logische Äquivalenz)

Seien $A, B \in F$ heißen **logisch äquivalent** mit der Schreibweise $A \models\!\!\dashv B$, falls für jede Bewertung φ gilt: $\varphi(A) = \varphi(B)$.

Insbesondere ist dann $A \models B$ und $B \models A$.

- Einige Beispiele für logisch äquivalente Formeln:
  1. $A \models\!\!\dashv \neg(\neg A)$, $\quad A \models\!\!\dashv A \vee A$, $\quad A \models\!\!\dashv A \wedge A$
  2. $A \wedge B \models\!\!\dashv B \wedge A$ und $A \vee B \models\!\!\dashv B \vee A$,
  3. $A \wedge (B \wedge C) \models\!\!\dashv (A \wedge B) \wedge C$ und $A \vee (B \vee C) \models\!\!\dashv (A \vee B) \vee C$,
  4. $A \wedge (B \vee C) \models\!\!\dashv (A \wedge B) \vee (A \wedge C)$ und
     $A \vee (B \wedge C) \models\!\!\dashv (A \vee B) \wedge (A \vee C)$ (**Distributiv**)

Logische Äquivalenz (Fort.)

5. $\neg(A \wedge B) \models\!\!\!\!\models (\neg A) \vee (\neg B)$ und $\neg(A \vee B) \models\!\!\!\!\models (\neg A) \wedge (\neg B)$ (**De Morgan**)
6. $A \rightarrow B \models\!\!\!\!\models (\neg A) \vee B$,
   $A \wedge B \models\!\!\!\!\models \neg(A \rightarrow (\neg B))$ und
   $A \vee B \models\!\!\!\!\models (\neg A) \rightarrow B$.
7. $A \leftrightarrow B \models\!\!\!\!\models (A \rightarrow B) \wedge (B \rightarrow A)$

- Man beachte, dass $\models\!\!\!\!\models$ reflexiv, transitiv und symmetrisch, d.h. eine Äquivalenzrelation ist.
- Ersetzt man in einer Formel eine Teilformel durch eine logisch äquivalente Formel, so erhält man eine logisch äquivalente Formel.

Logische Äquivalenz (Fort.)

- Folgende Aussagen sind äquivalent:
  - $\models (A \leftrightarrow B)$
  - $A \models B$ und $B \models A$
  - $A \models\!\!\!\!= \!\!\!\!\!\!\dashv B$
  - $\mathrm{Folg}(A) = \mathrm{Folg}(B)$

Folgerung 1.13

Zu jedem $A \in F$ gibt es $B, C, D \in F$ mit

1. *$A \models\!\dashv B$, B enthält nur $\rightarrow$ und $\neg$ als log. Verknüpfungen*
2. *$A \models\!\dashv C$, C enthält nur $\wedge$ und $\neg$ als log. Verknüpfungen*
3. *$A \models\!\dashv D$, D enthält nur $\vee$ und $\neg$ als log. Verknüpfungen*

Logische Äquivalenz (Fort.)

Definition 1.14 (Vollständige Operatorenmengen)

Eine Menge $OP \subseteq \{\neg, \vee, \wedge, \rightarrow, \leftrightarrow, ..\}$ heißt **vollständig**, falls es zu jedem $A \in F$ eine logisch äquivalente A-Form $B \in F(OP)$ gibt.

- Vollständige Operatorenmengen für die Aussagenlogik sind z.B.: $\{\neg, \rightarrow\}, \{\neg, \vee\}, \{\neg, \wedge\}, \{\neg, \vee, \wedge\}, \{\text{false}, \rightarrow\}$
- Dabei ist false eine Konstante, mit $\varphi(\text{false}) = 0$ für jede Bewertung φ. Offenbar gilt $\neg A \models\mathrel{\mkern-3mu}\Dashv (A \rightarrow \text{false})$.
- **Normalformen**:: DNF (Disjunktive Normalform), KNF (Konjunktive Normalform), KDNF, KKNF (Kanonische Formen).

Boolsche Funktionen

Jede Aussageform $A(p_1, ..., p_n)$ stellt in natürlicher Form eine Boolsche Funktion $f_A : \mathbb{B}^n \to \mathbb{B}$ dar. Nämlich durch die Festlegung $f_A(b_1, ..., b_n) = \varphi_{\vec{b}}(A)$ mit der Bewertung $\varphi_{\vec{b}}(p_i) = b_i$

- Man kann leicht durch Induktion nach n zeigen, dass jede Boolsche Funktion $f : \mathbb{B}^n \to \mathbb{B}$ $(n > 0)$ sich in obiger Form durch eine Aussageform in $p_1, ..., p_n$ und einer vollständigen Operatorenmenge darstellen lässt.
- Die Boolsche Algebra über $\mathbb{B}$ hat als übliche Operatormenge **true, false, not, or, and** mit der standard Interpretation.
- Für andere Operatormengen die etwa **nand, nor** enthalten, siehe Digitale Logik
  (Gatter: Ein- Ausgabesignale, Verzögerung. **nand, nor** Gattern werden bevorzugt, da nur zwei Transistoren nötig).

Beispiel Patientenüberwachungssystem

Beispiel Patientenüberwachungssystem erhält gewisse Daten über den Zustand eines Patienten. Z.B. Temperatur, Blutdruck, Pulsrate. Die Schwellenwerte für die Daten seien etwa wie folgt festgelegt:

Zustände Ein/ Ausgaben	Bedeutung
A	Temperatur außerhalb 36-39°C.
B	Blutdruck außerhalb 80-160 mm.
C	Pulsrate außerhalb 60-120 Schläge pro min.
O	Alarmaktivierung ist notwendig.

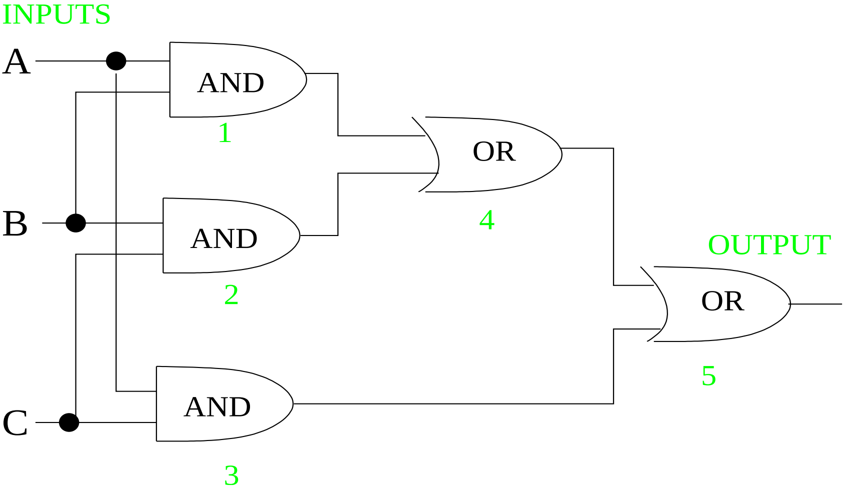
Die Anforderungen, d.h. bei welchen Kombinationen der Werte der Zustände eine Alarmaktivierung notwendig ist, werden durch den Medizin-Experten festgelegt. Sie seien in folgender Tabelle fixiert.

I/O - **Tabelle**

A	B	C	O
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Logischer Entwurf: Betrachte die Zeilen in denen O den Wert 1 hat und stelle eine KDNF auf (Disjunktion von Konjunktionen von Literalen, wobei ein Literal eine atomare Form oder die Negation einer solchen ist).
$(\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$

Als eine Realisierung könnte man das folgende Schaltnetz nehmen:



Deduktiver Aufbau der Aussagenlogik

Dieser Abschnitt beschäftigt sich mit einem axiomatischen Aufbau der Aussagenlogik mittels eines **“Deduktiven Systems”** oder eines **„Kalküls“**.
Eine syntaktisch korrekte Formel in einem Deduktiven System wird “Theorem” genannt, wenn sie durch rein mechanische Anwendungen der Regeln des Systems aus den Axiomen des Systems “abgeleitet” werden kann.
Man kann mehrere deduktive Systeme angeben, in denen aussagenlogische Formeln genau dann Theoreme sind, wenn sie auch Tautologien sind.

Deduktive Systeme-Kalküle

Definition 1.15 (Deduktives System)

Ein **Deduktives System** $\mathcal{F} = \mathcal{F}(\mathrm{Ax}, R)$ besteht aus

- einem Alphabet Δ (hier $\Delta = V \cup K \cup \{\rightarrow, \neg\}$),
- $F \subseteq \Delta^\star$, einer Menge von (wohldefinierten) Formeln (hier die Aussageformen),
- $\mathrm{Ax} \subseteq F$, einer Menge von Axiomen und
- R, einer Menge von Regeln der Form $\dfrac{A_1, \ldots, A_n}{A}$ $(n \in \mathbb{N}^+)$. $(A_1, ..., A_n, A \in F)$

Die Mengen F, Ax und R sind im allgemeinen rekursiv entscheidbar.

Deduktive Systeme-Kalküle

- Die Menge $T = T(\mathcal{F})$ der **Theoreme** ist definiert durch:
  1. $\mathrm{Ax} \subseteq T$ (d.h. alle Axiome sind Theoreme)
  2. Sind $A_1, \dots, A_n \in T$ und ist die Regel $\frac{A_1, \dots, A_n}{A}$ in R, dann ist $A \in T$.
  3. T ist die kleinste Menge von Formeln, die (1) und (2) erfüllt.
- Man schreibt für $A \in T(\mathcal{F})$ auch $\vdash_{\mathcal{F}} A$ oder einfach $\vdash A$ und sagt "A ist in $\mathcal{F}$ herleitbar".
- **Deduktiver Folgerungsbegriff:** Sei $\Sigma \subseteq F$, $A \in F$, dann bedeutet $\Sigma \vdash_{\mathcal{F}(Ax,R)} A$ nichts anderes als $\vdash_{\mathcal{F}(Ax \cup \Sigma, R)} A$. Sprechweise: "$A$ ist in $\mathcal{F}$ aus Σ herleitbar".
- Sind $\mathcal{F}_1$ und $\mathcal{F}_2$ deduktive Systeme über der Formelmenge F und gilt $T(\mathcal{F}_1) = T(\mathcal{F}_2)$ so nennt man sie **äquivalent.**

Bemerkung

Bemerkung 1.16

1. *Eigenschaften der Elemente von T werden durch strukturelle Induktion bewiesen.*
   T wird von einer Relation $R' \subseteq F^{\star} \times F$ erzeugt.
   Eine Formel A ist ein Theorem oder ist in $\mathcal{F}$ herleitbar, falls es eine endliche Folge von Formeln $B_0, \ldots, B_n$ gibt mit $A \equiv B_n$ und für $0 \leq i \leq n$ gilt:
   $B_i \in Ax$ oder es gibt l und $i_1, \ldots, i_l < i$ und eine Regel $\frac{B_{i_1} \ldots B_{i_l}}{B_i} \in R$.
   - *Die Folge $B_0, \ldots, B_n$ heißt auch **Beweis (Herleitung)** für A in $\mathcal{F}$.*
   - *Das bedeutet $\vdash A$ gilt genau dann, wenn es einen Beweis $B_0, \ldots, B_n$ mit $A \equiv B_n$ gibt.*

Bemerkung (Fort.)

2. *Die Menge T der Theoreme ist rekursiv aufzählbar (denn Ax und R sind rekursiv). Die Menge der Beweise*

$$\text{Bew} := \{B_1 \star B_2 \star \ldots \star B_n \mid B_1, \ldots, B_n \textit{ ist Beweis}\}$$

ist rekursiv. (Siehe Argumentation von $L(G)$ ist rekursiv aufzählbar für Grammatiken G).

- *Ist Σ rekursiv entscheidbar, so gelten obige Aussagen entsprechend. Insbesondere ist $Folg_{\mathcal{F}}(\Sigma) = \{A \mid \Sigma \vdash_{\mathcal{F}(Ax,R)} A\}$ rekursiv aufzählbar.*
- **Beachte**: *Beweise sind im allgemeinen nicht eindeutig. Es wird im allgemeinen nicht verlangt, dass T von R frei erzeugt wird.*

Bemerkung (Fort.)

3. *Gibt es ein deduktives System $\mathcal{F}_0$, so dass $\vdash_{\mathcal{F}_0} A$ genau dann gilt, wenn $\models A$ gilt?*

- *Hierzu werden Ax und R häufig endlich beschrieben durch Schemata.*
Beispielsweise beschreibt das Schemata $(A \to (B \to A))$ die Menge $\{A_0 |\ \text{es gibt}\ A, B \in F\ \text{mit}\ A_0 \equiv (A \to (B \to A))\}$

und das Schemata $\dfrac{A, A \to B}{B}$ *beschreibt die Menge von Regeln*

$$\left\{ \frac{A_0, A_1}{B_0} \mid \text{Es gibt}\ A, B \in F\ \text{mit} \right.$$
$$\left. A_0 \equiv A, B_0 \equiv B\ \text{und}\ A_1 \equiv A \to B \right\}.$$

Das deduktive System $\mathcal{F}_0$

Definition 1.17 (Das deduktive System $\mathcal{F}_0$)

Das deduktive System $\mathcal{F}_0$ für die Aussagenlogik besteht aus der Formelmenge F_0 der Formeln in $V, \neg, \rightarrow, ($ und $)$. Die Axiomenmenge Ax wird durch folgende Axiomenschemata beschrieben:

Ax1: $A \rightarrow (B \rightarrow A)$

Ax2: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

Ax3: $((\neg A) \rightarrow (\neg B)) \rightarrow (B \rightarrow A)$

Dabei beschreiben Ax1, Ax2 und Ax3 disjunkte Formelmengen.

Das deduktive System $\mathcal{F}_0$

Die Regelmenge R wird beschrieben durch das Regelschema

$$\text{MP:} \quad \frac{A, (A \to B)}{B} \quad \text{(modus ponens).}$$

- Beachte: Ax und R sind rekursiv entscheidbar.
- Es genügt zunächst nur Axiome für Formeln in $\to$ und $\neg$ zu betrachten, da alle anderen Formeln zu einer Formel in $\to$ und $\neg$ logisch äquivalent sind.
- Die Menge der Theoreme von $\mathcal{F}_0$ wird nicht frei erzeugt. Die Modus-Ponens-Regel ist hochgradig nicht eindeutig. $\frac{A, A \to B}{B}$ und $\frac{A', A' \to B}{B}$ sind beides Regeln mit gleicher Folgerung. Das erschwert sehr das Finden von Beweisen.

Beispiel

Beispiel 1.18

Für jedes $A \in F_0$ gilt $\vdash (A \rightarrow A)$, d.h. $(A \rightarrow A) \in T(\mathcal{F}_0)$

Beweis:

$$
\begin{array}{lll}
B_0 \equiv & (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow & \\
 & \quad ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)) & \text{Ax2} \\
B_1 \equiv & A \rightarrow ((A \rightarrow A) \rightarrow A) & \text{Ax1} \\
B_2 \equiv & (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A) & \text{MP}(B_0, B_1) \\
B_3 \equiv & A \rightarrow (A \rightarrow A) & \text{Ax1} \\
B_4 \equiv & A \rightarrow A & \text{MP}(B_2, B_3)
\end{array}
$$

■

- Wie findet man Beweise im System $\mathcal{F}_0$?
  Einziger Hinweis: Die Zielformel B, sofern sie kein Axiom ist, muss in der Form $(A_1 \rightarrow (...(A_n \rightarrow B)...))$ vorkommen. Wähle geeignete A´s.
- **Beachte:** Alle Axiome sind Tautologien der Aussagenlogik. Da diese abgeschlossen gegenüber Modus Ponens sind, sind alle Theoreme von $\mathcal{F}_0$ Tautologien. D.h. $T(\mathcal{F}_0) \subseteq Taut(F_0)$.
- Will man in ganz F Beweise führen, so muss man weitere Axiome einführen.
  Z.B.
  Ax1$\wedge$: $(A \wedge B) \rightarrow (\neg(A \rightarrow (\neg B)))$
  Ax2$\wedge$: $(\neg(A \rightarrow (\neg B))) \rightarrow (A \wedge B)$

Deduktiver Folgerungsbegriff

Definition 1.19 (Axiomatischer Folgerungsbegriff)

Sei $\Sigma \subseteq F_0, A \in F_0$.

1. A ist aus Σ in $\mathcal{F}_0$ **herleitbar**, wenn A sich aus $\mathrm{Ax} \cup \Sigma$ mit den Regeln aus R herleiten lässt, d.h. A ist Theorem im deduktiven System $\mathcal{F}$ mit Axiomenmenge $\mathrm{Ax} \cup \Sigma$ und gleicher Regelmenge wie $\mathcal{F}_0$. Schreibweise $\Sigma \vdash_{\mathcal{F}_0} A$, einfacher $\Sigma \vdash A$.

   $B_0, \ldots, B_n$ ist ein **Beweis** für $\Sigma \vdash A$, falls $A \equiv B_n$ und für alle $0 \leq i \leq n$ gilt: $B_i \in \mathrm{Ax} \cup \Sigma$ oder es gibt $j, k < i$ mit $B_k \equiv (B_j \rightarrow B_i)$.

2. Σ heißt **konsistent**, falls für keine Formel $A \in F_0$ gilt $\Sigma \vdash A$ und $\Sigma \vdash \neg A$.
   Gibt es eine solche Formel, so heißt Σ **inkonsistent**.

Folgerung 1.20 (Beweishilfsmittel)

1. *Gilt* $\Sigma \vdash A$, *so folgt unmittelbar aus der Definition 1.19, dass es eine endliche Teilmenge* $\Sigma_0 \subseteq \Sigma$ *gibt mit* $\Sigma_0 \vdash A$.
   Dies entspricht dem Kompaktheitssatz für "$\models$*".*
2. *Ist* Σ *inkonsistent, dann gibt es eine endliche Teilmenge* $\Sigma_0 \subseteq \Sigma$, *die inkonsistent ist*
   (denn ist $\Sigma \subseteq \Gamma$ *und* $\Sigma \vdash A$, *dann gilt auch* $\Gamma \vdash A$*).*
3. *Ist* $\Sigma \subseteq \Gamma$ *so* $Folg_{\mathcal{F}_0}(\Sigma) \subseteq Folg_{\mathcal{F}_0}(\Gamma)$.
4. *Aus* $\Sigma \vdash A$ *und* $\Gamma \vdash B$ *für alle* $B \in \Sigma$ *folgt* $\Gamma \vdash A$.
   Ist also $\Sigma \subseteq Folg_{\mathcal{F}_0}(\Gamma)$ *so* $Folg_{\mathcal{F}_0}(\Sigma) \subseteq Folg_{\mathcal{F}_0}(\Gamma)$.
   Beweise lassen sich also zusammensetzen.
5. *Gilt* $\Sigma \vdash A$, *so ist* $\{\Sigma, \neg A\}$ *inkonsistent.*
   Gilt auch die Umkehrung?
6. *Es gilt stets* $T(\mathcal{F}_0) \subseteq Folg_{\mathcal{F}_0}(\Sigma)$ *für jede Menge* Σ.

Satz 1.21 (Deduktionstheorem)

Sei $\Sigma \subseteq F_0$ *und seien* $A, B \in F_0$.
Dann gilt: $\Sigma, A \vdash B \quad \text{gdw} \quad \Sigma \vdash (A \to B)$

Beweis:

„ $\Leftarrow$ “ Klar wegen MP-Regel.
„ $\Rightarrow$ “ Sei $B_0, \ldots, B_m$ ein Beweis für $\Sigma, A \vdash B$, d.h. $B \equiv B_m$.
Beh.: Für $i = 0, \ldots, m$ gilt $\Sigma \vdash (A \to B_i)$

Induktion nach i und Fallunterscheidung, je nachdem ob B_i gleich A ist, in $\mathrm{Ax} \cup \Sigma$ liegt oder mit MP-Regel aus B_j, B_k mit $j, k < i$ entsteht. ■

Anwendungen des Deduktionstheorems

Beispiel 1.22 (Beweistransformationen. Wiederverwendung von Beweisen.)

- Vereinbarungen zur Darstellung von Beweisen:
  $B_1, \ldots, B_n$ heißt **abgekürzter Beweis** für $\Sigma \vdash B_n$, falls für jedes j mit $1 \leq j \leq n$ gilt: $\Sigma \vdash B_j$ oder es gibt $j_1, \ldots, j_r < j$ mit $B_{j_1}, \ldots, B_{j_r} \vdash B_j$.
- Gibt es einen abgekürzten Beweis für $\Sigma \vdash A$, dann gibt es auch einen Beweis für $\Sigma \vdash A$.

1. $\vdash (A \rightarrow A)$ folgt aus dem Deduktionstheorem, da $A \vdash A$ gilt.
2. Um $A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$ zu zeigen, zeige
   $A, A \rightarrow B, B \rightarrow C \vdash C$.

Anwendungen des Deduktionstheorems (Fort.)

3. $\vdash (\neg\neg A \to A)$ dazu genügt es zu zeigen
   $\neg\neg A \vdash A$

Beweis:

$B_1 \equiv \neg\neg A$	
$B_2 \equiv \neg\neg A \to (\neg\neg\neg\neg A \to \neg\neg A)$	Ax1
$B_3 \equiv \neg\neg\neg\neg A \to \neg\neg A$	MP
$B_4 \equiv (\neg\neg\neg\neg A \to \neg\neg A) \to (\neg A \to \neg\neg\neg A)$	Ax3 ■
$B_5 \equiv \neg A \to \neg\neg\neg A$	MP
$B_6 \equiv (\neg A \to \neg\neg\neg A) \to (\neg\neg A \to A)$	Ax3
$B_7 \equiv \neg\neg A \to A$	MP
$B_8 \equiv A$	MP

Anwendungen des Deduktionstheorems (Fort.)

4. $\vdash (A \to B) \to ((B \to C) \to (A \to C))$
   (zeige: $A \to B, B \to C \vdash A \to C$)
5. $\vdash (B \to ((B \to A) \to A))$
6. $\vdash (\neg B \to (B \to A))$ (zu zeigen: $\neg B, B \vdash A$)

Beweis:

$B_1 \equiv \neg B$	Vor
$B_2 \equiv \neg B \to (\neg A \to \neg B)$	Ax1
$B_3 \equiv \neg A \to \neg B$	MP
$B_4 \equiv (\neg A \to \neg B) \to (B \to A)$	Ax3
$B_5 \equiv B \to A$	MP
$B_6 \equiv B$	Vor
$B_7 \equiv A$	MP ∎

7. $\vdash B \rightarrow \neg\neg B$
8. $\vdash ((A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A))$ und
   $\vdash ((\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B))$
9. $\vdash (B \rightarrow (\neg C \rightarrow \neg(B \rightarrow C)))$
10. $\vdash ((B \rightarrow A) \rightarrow ((\neg B \rightarrow A) \rightarrow A))$
11. $\vdash (A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$

Frage: Lassen sich alle Tautologien als Theoreme im System $\mathcal{F}_0$ herleiten ?

Vollständigkeit und Entscheidbarkeit von $\mathcal{F}_0$

Satz 1.23 (Korrektheit und Vollständigkeit von $\mathcal{F}_0$)

Sei $A \in F_0$ eine Formel der Aussagenlogik.

a) Korrektheit: *Aus $\vdash_{\mathcal{F}_0} A$ folgt $\models A$, d.h. nur Tautologien können als Theoreme in $\mathcal{F}_0$ hergeleitet werden.*

b) Vollständigkeit: *Aus $\models A$ folgt $\vdash_{\mathcal{F}_0} A$, d.h. alle Tautologien lassen sich in $\mathcal{F}_0$ herleiten.*

Vollständigkeit und Entscheidbarkeit von $\mathcal{F}_0$ (Fort.)

Als Hilfsmittel dient:

Lemma 1.24

Sei $A \equiv A(p_1, \ldots, p_n) \in F_0, n > 0$, *wobei* $p_1, \ldots, p_n$ *die in* A *vorkommenden Aussagevariablen sind. Sei* φ *eine Bewertung. Ist*

$$P_i := \begin{cases} p_i \quad, \mathit{falls}\ \varphi(p_i) = 1 \\ \neg p_i, \mathit{falls}\ \varphi(p_i) = 0 \end{cases} \qquad A' := \begin{cases} A \quad, \mathit{falls}\ \varphi(A) = 1 \\ \neg A, \mathit{falls}\ \varphi(A) = 0 \end{cases}$$

$(1 \leq i \leq n)$, *dann gilt* $P_1, \ldots, P_n \vdash A'$.

Angenommen das Lemma gilt und sei $\models A$, d.h. $\varphi(A) = 1$ für alle Bewertungen φ. Sei φ eine Bewertung mit $\varphi(p_n) = 1$. Es gilt $P_1, \ldots, P_n \vdash A$ und wegen $P_n \equiv p_n$ gilt $P_1, \ldots, P_{n-1}, p_n \vdash A$. Betrachtet man eine Bewertung φ' mit $\varphi'(p_n) = 0$ und sonst gleich φ , erhält man $P_1, \ldots, P_{n-1}, \neg p_n \vdash A$.

Vollständigkeit und Entscheidbarkeit von $\mathcal{F}_0$ (Fort.)

- Durch Anwenden des Deduktionstheorems entstehen daraus
  $P_1, \ldots, P_{n-1} \vdash p_n \to A$ und
  $P_1, \ldots, P_{n-1} \vdash \neg p_n \to A$.
  Gleichzeitig gilt nach dem 10. Beispiel von 1.22 auch
  $P_1, \ldots, P_{n-1} \vdash ((p_n \to A) \to ((\neg p_n \to A) \to A))$.
- Durch zweimaliges Anwenden des Modus-Ponens entsteht
  $P_1, \ldots, P_{n-1} \vdash A$.
- Dies gilt für jede Wahl der $P_i, i = 1, ..., n-1$ und somit lässt sich das Argument iterieren. D.h. in einer Herleitung von A muss kein p_i verwendet werden, also $\vdash A$.
- Das Lemma wird durch Induktion über den Aufbau von A nachgewiesen. D.h. für $A \equiv p_1, \neg C, B \to C$ unter Verwendung von Deduktionen aus Beispiel 1.22.

Folgerung

Folgerung 1.25

Sei $\Sigma \subseteq F_0, A \in F_0$.

1. $\Sigma \vdash_{\mathcal{F}_0} A$ *gilt genau dann, wenn* $\Sigma \models A$ *gilt.*
2. Σ *ist genau dann konsistent, wenn* Σ *erfüllbar ist.*
3. Σ *ist genau dann inkonsistent, wenn* Σ *unerfüllbar ist.*
4. *Ist* Σ *endlich und* $A \in F_0$, *dann ist* $\Sigma \vdash_{\mathcal{F}_0} A$ *entscheidbar.*

Beweis der Folgerung

Beweis:

1.

$$\begin{aligned}
&\Sigma \vdash_{\mathcal{F}_0} A \\
&\overset{1.20}{\iff} \text{Es gibt } A_1,\ldots,A_n \in \Sigma \text{ mit } A_1,\ldots,A_n \vdash_{\mathcal{F}_0} A \\
&\overset{\text{D.T.}}{\iff} \text{Es gibt } A_1,\ldots,A_n \in \Sigma \text{ mit} \\
&\qquad \vdash_{\mathcal{F}_0} (A_1 \to (A_2 \to \ldots (A_n \to A)\ldots)) \\
&\overset{1.23}{\iff} \text{Es gibt } A_1,\ldots,A_n \in \Sigma \text{ mit} \\
&\qquad \models (A_1 \to (A_2 \to \ldots (A_n \to A)\ldots)) \\
&\overset{\text{D.T.}}{\iff} \text{Es gibt } A_1,\ldots,A_n \in \Sigma \text{ mit } A_1,\ldots,A_n \models A \\
&\overset{\text{K.S.}}{\iff} \Sigma \models A
\end{aligned}$$

Beweis der Folgerung

2. Σ ist konsistent. $\iff$
   Es gibt kein A mit $\Sigma \vdash A$ und $\Sigma \vdash \neg A$. $\iff$
   Es gibt kein A mit $\Sigma \models A$ und $\Sigma \models \neg A$. $\iff$
   Σ ist erfüllbar (Bemerkung 1.8 c)).

Natürliche Kalküle

Es gibt andere deduktive Systeme, für die Satz 1.23 gilt. Das deduktive System $\mathcal{F}_0$ wurde von S.C. Kleene eingeführt. Das folgende deduktive System geht auf G. Gentzen zurück.

Definition 1.26 (Gentzen-Sequenzenkalkül)

Eine Sequenz ist eine Zeichenreihe der Form $\Gamma \vdash \Delta$ mit zwei endlichen Mengen von Formeln Γ und Δ.
Seien $\Gamma, \Delta \subseteq F$ endliche Mengen von Formeln und $A, B \in F$.
Der Kalkül für Objekte der Form $\Gamma \vdash_G \Delta$ wird definiert durch folgende Axiome und Regeln:

Gentzen-Sequenzenkalkül: Axiome und Regeln

Ax1: $\Gamma, A \vdash_G A, \Delta$

Ax2: $\Gamma, A, \neg A \vdash_G \Delta$

Ax3: $\Gamma \vdash_G A, \neg A, \Delta$

$\mathbf{R}_{\wedge,\vee}$: $\dfrac{\Gamma, A, B \vdash_G \Delta}{\Gamma, A \wedge B \vdash_G \Delta}$ $\qquad$ $\dfrac{\Gamma \vdash_G A, B, \Delta}{\Gamma \vdash_G (A \vee B), \Delta}$

$\mathbf{R}_{\rightarrow}$: $\dfrac{\Gamma, A \vdash_G \Delta, B}{\Gamma \vdash_G (A \rightarrow B), \Delta}$ $\qquad$ $\dfrac{\Gamma \vdash_G A, \Delta; \quad \Gamma, B \vdash_G \Delta}{\Gamma, (A \rightarrow B) \vdash_G \Delta}$

$\mathbf{R}_{\neg}$: $\dfrac{\Gamma, A \vdash_G \Delta}{\Gamma \vdash_G \neg A, \Delta}$ $\qquad$ $\dfrac{\Gamma \vdash_G A, \Delta}{\Gamma, \neg A \vdash_G \Delta}$

$\mathbf{R}_{\wedge'}$: $\dfrac{\Gamma \vdash_G A, \Delta; \quad \Gamma \vdash_G B, \Delta}{\Gamma \vdash_G (A \wedge B), \Delta}$

$\mathbf{R}_{\vee'}$: $\dfrac{\Gamma, A \vdash_G \Delta; \quad \Gamma, B \vdash_G \Delta}{\Gamma, (A \vee B) \vdash_G \Delta}$

Gentzen-Sequenzenkalkül

$\Gamma \vdash_G \Delta$ ist ableitbar bedeutet: Es gibt ein $r \in \mathbb{N}$ und eine Folge von Sequenzen $\Gamma_1 \vdash_G \Delta_1, \ldots, \Gamma_r \vdash_G \Delta_r$ mit

1. $\Gamma_r \equiv \Gamma$ und $\Delta_r \equiv \Delta$
2. Jedes $\Gamma_j \vdash_G \Delta_j$ mit $1 \leq j \leq r$ ist Axiom oder geht aus vorangehenden Folgegliedern aufgrund einer Regel hervor.

Bemerkung 1.27 (**Semantische Interpretation**)

Die Aussage $\Gamma \vdash_G \Delta$ kann wie folgt anschaulich interpretiert werden: Für jede Bewertung φ gibt es eine Formel $A \in \Gamma$ mit $\varphi(A) = 0$ oder es gibt eine Formel $B \in \Delta$ mit $\varphi(B) = 1$. Sind $\Gamma = \{A_1, \ldots, A_n\}$ und $\Delta = \{B_1, \ldots, B_m\}$, also endlich, entspricht dies also der Formel $(A_1 \wedge \cdots \wedge A_n) \rightarrow (B_1 \vee \cdots \vee B_m)$.

- Der Semantische Folgerungsbegriff $\Sigma \models A$ für eine Menge von Formeln $\{\Sigma, A\}$ kann wie folgt auf Mengenpaare Γ, Δ erweitert werden:

$$\Gamma \models \Delta \quad \text{gdw} \quad \Gamma \models A$$

wobei A die Disjunktion der Formeln in Δ ist.

- Interpretiert man in einer Sequenz $\Gamma \vdash_G \Delta$ die Menge Γ als Voraussetzungen, und die Menge Δ als Konklusion, so lässt sich die Korrektheit des Kalküls leicht nachweisen.
- Es gilt also:
  Aus $\Gamma \vdash_G \Delta$ folgt $\Gamma \models \Delta$. (**Übung**)
- Es gilt auch die Umkehrung dieser Aussage, d.h. der Sequenzenkalkül von Gentzen ist korrekt und vollständig. (Bew. siehe z.B. Kleine Büning/Lettmann: Aussagenlogik, Deduktion und Algorithmen)

Beispiel

Beispiel 1.28

Es gilt $p \vee q, (\neg p) \vee r \vdash_G q \vee r$

Beweis:

$B_1 \equiv q, r \vdash q, r$	Ax1
$B_2 \equiv q, \neg p \vdash q, r$	Ax1
$B_3 \equiv q, (\neg p) \vee r \vdash q, r$	$R_{\vee'}(1,2)$
$B_4 \equiv p, r \vdash q, r$	Ax1
$B_5 \equiv \neg p, p \vdash q, r$	Ax2
$B_6 \equiv p, (\neg p) \vee r \vdash q, r$	$R_{\vee'}(4,5)$
$B_7 \equiv p \vee q, (\neg p) \vee r \vdash q, r$	$R_{\vee'}(3,6)$
$B_8 \equiv p \vee q, (\neg p) \vee r \vdash q \vee r$	$R_{\vee}(7)$

■

Bemerkung 1.29 (**Weitere Kalküle für die Aussagenlogik**)

Man findet in der Literatur eine Vielzahl von „natürlichen“ Kalkülen (deduktiven Systemen), die ebenfalls korrekt und vollständig sind. Für diese werden auch Beweisstrategien für so genannte „Goals“ und „Subgoals“ vorgestellt.

Als Beispiel Hilberts Kalkül, das z.B. für jeden Operator eine Regel für die Einführung und eine für die Entfernung des Operators enthält.

Hilberts Kalkül

- Konjunktion $\wedge\_I : \dfrac{p, q}{p \wedge q}$ $\wedge\_E : \dfrac{p \wedge q}{p}$
- Disjunktion $\vee\_I : \dfrac{p}{p \vee q}$ $\vee\_E : \dfrac{p \vee q, \neg p}{q}$
- Implikation $\to E : \dfrac{p, p \to q}{q}$ $\to E : \dfrac{\neg q, p \to q}{\neg p}$
  Modus Ponens Modus Tollens
- Negation $\neg\_E : \dfrac{p, \neg p}{q}$ $\neg\_E : \dfrac{\neg\neg p}{p}$
  Widerspruchsregel Doppelnegation
- Äquivalenz $\leftrightarrow E : \dfrac{p \leftrightarrow q}{p \to q}$ $\leftrightarrow E : \dfrac{p \leftrightarrow q}{q \to p}$

- Transitivität $\leftrightarrow I : \dfrac{p \leftrightarrow q, q \leftrightarrow r}{p \leftrightarrow r}$
- Deduktions - Theorem $\rightarrow I : \dfrac{p, \ldots, r, \underline{s} \vdash t}{p, \ldots, r \vdash s \rightarrow t}$
- Reductio ad absurdum $\neg I : \dfrac{p, \ldots, r, \underline{s} \vdash t, p, \ldots, r, \underline{s} \vdash \neg t}{p, \ldots, r \vdash \neg s}$
- Hypothetischer Syllogismus $\dfrac{p \rightarrow q, q \rightarrow r}{p \rightarrow r}$
- Konstruktives Dilemma $\dfrac{p \rightarrow q, r \rightarrow s, p \vee r}{q \vee s}$

Hinzukommen die üblichen Assoziativitäts-, Kommutativitäts-, Distributivitäts-, Negations-, Implikations- und de Morgan Regeln.

Beispiele in Hilberts Kalkül

Beispiel 1.30

Zeige $(p \wedge q) \vee r \vdash \neg p \rightarrow r$

Beweis:

- **Transformationsbeweis**

1.	$(p \wedge q) \vee r$	Prämisse
2.	$r \vee (p \wedge q)$	Kommutativität
3.	$(r \vee p) \wedge (r \vee q)$	Distributivität
4.	$(r \vee p)$	$\wedge\_E$
5.	$(p \vee r)$	Kommutativität
6.	$(\neg\neg p \vee r)$	Negations-Gesetz
7.	$\neg p \rightarrow r$	Implikations-Gesetz

■

Beispiele in Hilberts Kalkül

Zeige $(p \wedge q) \vee r \vdash \neg p \rightarrow r$

Beweis:

- **Bedingter Beweis**

1.	$(p \wedge q) \vee r$	Prämisse
2.	$\neg(\neg p \vee \neg q) \vee r$	Doppelnegation, de Morgan
3.	$(\neg p \vee \neg q) \rightarrow r$	Implikationsgesetz
4.	$\neg p$	Annahme
5.	$\neg p \vee \neg q$	$\vee_{-}I$
6.	r	Modus Ponens $\rightarrow_{-}E$ aus 3. und 5.
7.	$\neg p \rightarrow r$	Aus 4, 5, 6 mit Ded. Theo. $\rightarrow_{-}I$

■

Beispiele in Hilberts Kalkül

Zeige $(p \land q) \lor r \vdash \neg p \rightarrow r$

Beweis:

- **Indirekter Beweis**

1.	$(p \land q) \lor r$	Prämisse
2.	$(p \lor r) \land (q \lor r)$	Distributivgesetz
3.	$(p \lor r)$	$\land\_E$
4.	$\neg(\neg p \rightarrow r)$	Annahme
5.	$\neg(p \lor r)$	Implikations-und Negationsgesetz
6.	$\neg\neg(\neg p \rightarrow r)$	Red. Abs. $\rightarrow I$ aus 3, 4, 5.
7.	$\neg p \rightarrow r$	Doppelnegation

■