Einführung in die Logik

Klaus Madlener

4. Juni 2002

Vorwort

Dieses Skript entstand aus dem “alten” Vorlesungsskript “Einführung in die Logik und Korrektheit von Programmen”, das sich über viele Jahre bewährte. Es umfasst nur den Teil über Logik – die Kapitel über Programmverifikation wurden weggelassen. Hauptziel ist es die Vorteile einer Formalisierung der Logik deutlich zu machen. Der Übergang von der Umgangssprache zu einer formalisierten Sprache, welcher erfahrungsgemäß gewisse Schwierigkeiten bereitet, wird besprochen und eingeübt.

Die Auswahl des Stoffes für eine solche Vorlesung bereitet immer Probleme, denn das Gebiet der Logik ist so umfangreich, dass hier nur die wichtigsten Ergebnisse vorgestellt werden können.

Die Aussagenlogik dient der Einführung der Haupttechniken der Logik. Die Formalisierung von Aussagen und die Einführung des semantisch begründeten Folgerungsbegriffes sind Vorbilder für die Vorgehensweise in anderen Logiken. Eine der wesentlichen Eigenschaften der Logik, dass man nämlich den Folgerungsbegriff durch nachweislich äquivalente formale Ableitungssysteme ersetzen kann, wird ausführlich diskutiert. Der Kompaktheitssatz für die Aussagenlogik dient ebenfalls als Vorbild für den entsprechenden Satz der Prädikatenlogik.

Ein wesentlicher Teil der Vorlesung, nämlich die Übungen, sind in diesem Skript nicht enthalten. Es sei darauf hingewiesen, dass das Skript ausgezeichnete Literatur auf diesem Gebiet nicht ersetzen kann, sondern eher die Stoffauswahl der Vorlesung umreißt und Anregung zu weiterem Studium geben soll.

Inhaltsverzeichnis

1 Aussagenlogik

1.1 Die Sprache der Aussagenlogik

Als Einleitung und zur Einführung in die Methoden der Logik geht es in diesem Kapitel um die Grundlagen der Aussagenlogik. Im Mittelpunkt steht die Frage nach der Bedeutung einer Aussage: Wann ist eine Aussage wahr und wann ist sie falsch? Darüber hinaus beschäftigt sich die Aussagenlogik mit dem Zusammensetzen mehrerer Aussagen zu neuen, komplexeren Aussagen und den Zusammenhängen von Aussagen untereinander. Um die Bedeutung einer Aussage zu bestimmen, müssen zunächst die Begriffe "wahr" und "falsch" geklärt werden. Dazu ist eine Formalisierung des Wahrheitsbegriffes nötig.

1.1 Definition (Sprache der Aussagenlogik). Sei $\Sigma = V \cup O \cup K$ ein *Alphabet*, wobei $V = \{p_1, p_2, \ldots\}$ eine abzählbare Menge von *Aussagevariablen* ist, $O = \{\wedge, \vee, \neg, \rightarrow, \ldots\}$ eine Menge von *Verknüpfungen (Junktoren)* bezeichnet und $K = \{(,)\}$ die Klammern beinhaltet. Die Menge der *Aussageformen* $F \subseteq \Sigma^\star$ (auch *Formeln* der Aussagenlogik genannt) wird induktiv definiert durch

1. $V \subseteq F$, die Menge der atomaren Aussagen,
2. falls $A, B \in F$, dann $(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B) \in F$ und
3. F ist die kleinste Menge von Elementen aus $\Sigma^\star$, die V enthält und 2. erfüllt.

Zur Vereinfachung der Schreibweise werden äußere Klammern gelegentlich weggelassen.

1.2 Bemerkung. Eigenschaften von F werden mit Hilfe der "strukturellen Induktion", das heißt einer Induktion über den Aufbau von F bewiesen. Beispiele für Eigenschaften von F sind:

1. Für $A \in F$ gilt: A ist atomar oder beginnt mit "(" und endet mit ")".
2. Sei $f(A, i)$ die Anzahl der "(" minus der Anzahl der ")" in den ersten i Buchstaben von $A \in F$. Dann gilt $f(A, i) > 0$ für $1 \leq i < |A|$ und $f(A, i) = 0$ für $i = |A|$.

Ist $U = \Sigma^\star$, so kann F auch als Erzeugnis einer Relation $R \subseteq U^\star \times U$ angegeben werden (F wird frei von einer solchen Relation erzeugt, d.h. für alle $u, v \in F^\star$ und $A \in F$ gilt: Aus uRA und vRA folgt $u = v$).

Man kann zeigen, dass es eine eindeutige kontextfreie Grammatik gibt, die F erzeugt. F ist entscheidbar.

1.3 Satz (Eindeutigkeitssatz). Jede Aussageform $A \in F$ ist entweder atomar oder sie lässt sich eindeutig darstellen als $A \equiv (\neg A_1)$ oder $A \equiv (A_1 \star A_2)$ mit $\star \in \{\vee, \wedge, \rightarrow\}$ und $A_1, A_2 \in F$.

Beweis. Induktion über den Aufbau von F.

Ind. Anf.: Sei $A \in V$, d.h. A ist atomar. $\surd$

Ind. Schritt : Zu zeigen ist, dass man zu einer gegebenen Darstellung von $A \in F \backslash V$ keine weitere Darstellung von A finden kann, die mit dieser nicht übereinstimmt.

1. Fall: $A \equiv (\neg B), B \in F$.

   (a) Ist $A \equiv (\neg C)$ mit $C \in F$ eine weitere Darstellung von A, dann ist die Darstellung von C nach Induktionsvoraussetzung gleich der Darstellung von B.

   (b) Gäbe es eine andere Darstellung für A, müßte sie von der Gestalt $(D \star E)$ sein, mit $D, E \in F$ und $\star \in \{\wedge, \vee, \rightarrow\}$. Das zweite Zeichen "$\neg$" von A müßte dann auch erstes Zeichen von D sein. Das widerspricht aber der Definition von F, wonach D entweder eine Aussagevariable ist oder eine Formel, die mit "(" beginnt (s. 1.2). Diese Darstellung von A ist also eindeutig.

2. Fall: $A \equiv (B \star C)$ mit $B, C \in F, \star \in \{\wedge, \vee, \rightarrow\}$.

   (a) Eine andere Darstellung von A der Gestalt $(\neg D), D \in F$, führt analog Fall 1.(b) zu einem Widerspruch zur Definition der Formeln.

   (b) Sei $A \equiv (D \star_1 E)$ eine andere Darstellung für A mit $D, E \in F$ und $\star_1 \in \{\wedge, \vee, \rightarrow\}$. Falls $|D| = |B|$ ist, muss $\star_1 = \star$ sein und nach Induktionsvoraussetzung dann auch $D = B$ und $E = C$ gelten. Für den Fall $|D| \neq |B|$ sei o.B.d.A. $|B| > |D|$, so dass folgende Situation entsteht:

   $$\begin{array}{lcl} A & \equiv & (\underline{\qquad\qquad B \qquad\qquad} \star \underline{\qquad C \qquad}) \\ A & \equiv & (\underline{\qquad D \qquad} \star_1 \underline{\qquad\qquad E \qquad\qquad}) \\ & & \qquad\qquad\quad\;\uparrow \end{array}$$

   Betrachte die Anzahl der nicht geschlossenen, öffnenden Klammern $f(A, 1 + |D|)$ in Formel A an der markierten Stelle (f aus 1.2). Es gilt offensichtlich $f(A, 1 + |D|) = f(D, |D|) + 1 = 1$. Da D Präfix von B ist und $f(B, |D|) \geq 1$, muss außerdem gelten $1 = f(A, 1 + |D|) = 1 + f(B, |D|) \geq 2$, was die Annahme einer zweiten Darstellung von A widerlegt.

■

1.2 Die Semantik der Aussagenlogik

1.4 Definition. Eine *Bewertung* der Aussageformen ist eine Funktion $\varphi : F \rightarrow \mathbb{B} := \{0, 1\}$ mit

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

Man sagt "A ist 'falsch' unter φ", falls $\varphi(A) = 0$ und " 'wahr' unter φ", falls $\varphi(A) = 1$.
Eine mögliche Darstellung für eine Bewertung sind die sogenannten "Wahrheitstafeln":

$\varphi(A)$	$\varphi(\neg A)$
0	1
1	0

$\varphi(A)$	$\varphi(B)$	$\varphi(A \vee B)$	$\varphi(A \wedge B)$	$\varphi(A \to B)$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	1

Eine *Belegung* der aussagenlogischen Variablen V ist eine Funktion $\varphi_0 : V \to \mathbb{B}$. Jede Bewertung auf F induziert eine Belegung von V. Umgekehrt gilt:

1.5 Lemma. Jede Belegung $\varphi_0 : V \to \mathbb{B}$ lässt sich auf genau eine Weise zu einer Bewertung $\varphi : F \to \mathbb{B}$ fortsetzen.

Der Beweis folgt unmittelbar aus Satz 1.3 und Definition 1.4.

1.6 Folgerung. Jede Bewertung $\varphi : F \to \mathbb{B}$ wird eindeutig durch die Werte von φ auf V festgelegt. 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 $\varphi(A) = 1$.

Es stellt sich die Frage, welche Werte $\varphi(A)$ annehmen kann, 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:
Beispiel: Für die drei Variablen p, q und r aus A im obigen Beispiel gibt es 8 Belegungen, die betrachtet werden müssen:

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

Man sieht, dass $\varphi(A) = 1$ für jede Bewertung $\varphi : F \to \mathbb{B}$ gilt. Die Beobachtung, dass es Aussageformen gibt, die "wahr" sind, unabhängig davon wie ihre Variablen belegt werden, legt die folgende Definition nahe.

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

1. (a) A heißt *Tautologie*, falls $\varphi(A) = 1$ für jede Bewertung φ gilt. (Schreibweise "$\models A$")
   (b) A ist *allgemeingültig*, falls A Tautologie ist.
   (c) A ist *erfüllbar*, falls es eine Bewertung φ gibt, mit $\varphi(A) = 1$.
   (d) A ist *widerspruchsvoll*, falls $\varphi(A) = 0$ für jede Bewertung φ.
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 $\Sigma = \{A_1, \ldots, A_n\}$, ist die Kurzschreibweise "$A_1, \ldots, A_n \models A$" üblich.
   (c) Die Menge $\mathrm{Folg}(\Sigma)$ der Folgerungen aus Σ ist definiert durch:
   $$\mathrm{Folg}(\Sigma) := \{A \mid A \in F \text{ und } \Sigma \models A\}.$$

1.8 Bemerkungen und Beispiele.

1. $(p \vee (\neg p))$, $((p \to q) \vee (q \to r))$ und A aus Folgerung 1.6 sind Tautologien. $(p \wedge (\neg p))$ ist widerspruchsvoll. $(p \wedge q)$ ist erfüllbar jedoch keine Tautologie. Die Mengen
   $$\mathrm{Taut} := \{A \mid \ A \in F \text{ und } \models A\}$$
   und
   $$\mathrm{Sat} := \{A \mid \ A \in F \text{ und } A \text{ ist erfüllbar}\}$$
   sind <u>entscheidbar</u>.

2. (a) Ist $\Sigma = \emptyset$, dann gilt $\Sigma \models A$ genau dann, wenn A Tautologie ist, d.h. $\text{Folg}(\emptyset) = \text{Taut}$.
   (b) Ist Σ nicht erfüllbar, dann gilt $\Sigma \models A$ für alle $A \in F$, d.h. $\text{Folg}(\Sigma) = F$.
   (c) Sei $\Sigma = \{p\}$ und $A \equiv p \vee q$. 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.
   (d) Sei $\Sigma \subseteq \Sigma'$. Ist Σ' erfüllbar, dann ist auch Σ erfüllbar.
   (e) Es gilt $\Sigma \subseteq \text{Folg}(\Sigma)$ und $\text{Folg}(\text{Folg}(\Sigma)) = \text{Folg}(\Sigma)$.
   (f) Falls $\Sigma \subseteq \Sigma'$, dann gilt $\text{Folg}(\Sigma) \subseteq \text{Folg}(\Sigma')$.
3. $\Sigma \models A$ gilt genau dann, wenn $\Sigma \cup \{\neg A\}$ nicht erfüllbar ist. Ist Σ endlich, dann ist es entscheidbar, ob Σ erfüllbar ist, und die Menge $\text{Folg}(\Sigma)$ ist entscheidbar.

1.9 Lemma (Deduktionstheorem und Modus-Ponens-Regel).

a) Deduktionstheorem: $\Sigma, A \models B$ gilt genau dann, wenn $\Sigma \models (A \to B)$ gilt.
(Σ, A ist Kurzschreibweise für $\Sigma \cup \{A\}$)

b) Modus-Ponens-Regel: Es gilt $\{A, A \to B\} \models B$. Insbesondere ist B eine Tautologie, falls A und $(A \to B)$ Tautologien sind.

Beweis. zu (a):
"$\Longrightarrow$": Voraussetzung: $\Sigma, A \models B$. Sei $\varphi : F \to \mathbb{B}$ eine Bewertung, die Σ erfüllt. Ist $\varphi(A) = 0$, dann ist $\varphi(A \to B) = 1$. Ist $\varphi(A) = 1$, dann gilt nach Voraussetzung $\varphi(B) = 1$, also auch $\varphi(A \to B) = 1$.
"$\Longleftarrow$": analog.
zu (b):
Ist φ eine Bewertung mit $\varphi(A) = \varphi(A \to B) = 1$, dann ist $\varphi(B) = 1$. ■
Übliche Notationen für Regeln der Form "$A_1, \ldots, A_n \models B$" sind:

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

1.10 Satz (Kompaktheitssatz der Aussagenlogik). $\Sigma \subseteq F$ ist erfüllbar genau dann, wenn jede endliche Teilmenge von Σ erfüllbar ist. Insbesondere gilt $\Sigma \models A$ genau dann, wenn es eine endliche Teilmenge $\Sigma_0 \subseteq \Sigma$ gibt mit $\Sigma_0 \models A$.

Beweis. Σ heißt *endlich erfüllbar (e.e.)*, wenn jede endliche Teilmenge von Σ erfüllbar ist. Zu zeigen ist also: Σ ist endlich erfüllbar genau dann, wenn Σ erfüllbar ist.

"$\Longleftarrow$": folgt unmittelbar aus der Bemerkung 1.8 2.(d).

"$\Longrightarrow$": Sei Γ e.e. und sei $A \in F$. Dann ist $\Gamma \cup \{A\}$ oder $\Gamma \cup \{\neg A\}$ e.e. Denn angenommen $\Gamma \cup \{A\}$ ist nicht e.e., dann gibt es eine endliche Teilmenge $\Gamma_0 \subseteq \Gamma$, so dass $\Gamma_0 \cup \{A\}$ nicht erfüllbar ist.

Sei $\Gamma_1 \subseteq \Gamma \cup \{\neg A\}$ endlich. Dann ist $\Gamma_2 := (\Gamma_1 \cup \Gamma_0) \backslash \{\neg A\} \subseteq \Gamma$ endlich und also auch erfüllbar. Es gibt somit eine Belegung φ, die Γ_2 und damit auch Γ_0 erfüllt. Dann ist aber $\varphi(A) = 0$, d.h. $\varphi(\neg A) = 1$, und φ erfüllt $\Gamma_2 \cup \{\neg A\}$. Damit erfüllt φ aber auch Γ_1, eine beliebige endliche Teilmenge von $\Gamma \cup \{\neg A\}$, also ist $\Gamma \cup \{\neg A\}$ endlich erfüllbar.

Konstruiere eine <u>maximale</u> endlich erfüllbare Menge, die Σ enthält wie folgt: Sei $\{A_n \mid n \in \mathbb{N}\}$ eine Aufzählung der Aussageformen. Für $n \in \mathbb{N}$ definiere Δ_n durch $\Delta_0 := \Sigma$ und

$$\Delta_{n+1} \quad = \quad \begin{cases} \Delta_n \cup \{A_{n+1}\} \ , & \text{falls } \Delta_n \cup \{A_{n+1}\} \text{ endl. erfüllbar,} \\ \Delta_n \cup \{\neg A_{n+1}\}, & \text{sonst.} \end{cases}$$

Δ_n ist e.e. für alle $n \geq 0$. Sei $\Delta = \bigcup_{n \geq 0} \Delta_n$. Dann gilt: (i) $\Sigma \subseteq \Delta$, (ii) Δ ist e.e. und (iii) für jede Aussageform A gilt $A \in \Delta$ oder $\neg A \in \Delta$, wegen der endlichen Erfüllbarkeit von Δ jedoch nicht beides gleichzeitig. Definiere $\varphi : V \to \mathbb{B}$ durch

$$\varphi(p) = \begin{cases} 1, & \text{falls } p \in \Delta \\ 0, & \text{falls } \neg p \in \Delta. \end{cases}$$

φ ist eine wohldefinierte Belegung. Nach Lemma 1.5 lässt sich φ eindeutig zu einer Bewertung, die wir auch mit φ bezeichnen, fortsetzen. Durch Induktion über den Aufbau von F macht man sich schnell klar:

Für alle $A \in F$ gilt genau dann $\varphi(A) = 1$, wenn $A \in \Delta$ gilt. (Beispiel: Falls $\varphi(A \to B) = 1$, dann ist $\varphi(A) = 0$ oder $\varphi(B) = 1$, d.h. $\neg A \in \Delta$ oder $B \in \Delta$, also wurde $(A \to B)$ in Δ aufgenommen. Ist andererseits $\varphi(A \to B) = 0$, dann ist $\varphi(A) = 1$ und $\varphi(B) = 0$, d.h. $A \in \Delta$ und $\neg B \in \Delta$, also $\neg(A \to B) \in \Delta$ und wegen der endlichen Erfüllbarkeit von Δ ist $(A \to B) \notin \Delta$.) Also gilt auch $\varphi(A') = 1$ für alle $A' \in \Sigma$, also ist Σ erfüllbar. ∎

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

Betrachte die Menge $\Sigma' := \{\neg A \mid \ A \in \Sigma\}$. Nach Voraussetzung ist sie unerfüllbar. Also gibt es eine endliche nichtleere Teilmenge $\{\neg A_1, \ldots, \neg A_n\}$ von Σ', die unerfüllbar ist. Also gibt es für jede Bewertung φ ein i mit $\varphi(\neg A_i) = 0$. Dann ist aber $\varphi(A_i) = 1$ und daher auch $\varphi(A_1 \vee \ldots \vee A_n) = 1$.

1.12 Definition. $A, B \in F$ heißen *logisch äquivalent* mit der Schreibweise $A \models\!=\!\mid B$, 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. $A \models\!=\!\mid \neg(\neg A)$,

2. $A \wedge B \models\!=\!\mid B \wedge A$ und $A \vee B \models\!=\!\mid B \vee A$,

3. $A \wedge (B \wedge C) \models\!=\!\mid (A \wedge B) \wedge C$ und $A \vee (B \vee C) \models\!=\!\mid (A \vee B) \vee C$,

4. $A \wedge (B \vee C) \models\!=\!\mid (A \wedge B) \vee (A \wedge C)$ und
   $A \vee (B \wedge C) \models\!=\!\mid (A \vee B) \wedge (A \vee C)$

5. $\neg(A \wedge B) \models\!=\!\mid (\neg A) \vee (\neg B)$ und $\neg(A \vee B) \models\!=\!\mid (\neg A) \wedge (\neg B)$

6. $A \to B \models\!=\!\mid (\neg A) \vee B$, $A \wedge B \models\!=\!\mid \neg(A \to (\neg B))$ und $A \vee B \models\!=\!\mid (\neg A) \to B$.

Man beachte, dass $\models\!=\!\mid$ reflexiv, transitiv und symmetrisch, d.h. eine Äquivalenzrelation ist.
Nimmt man als zusätzlichen Junktor "$\leftrightarrow$" hinzu mit

$$\varphi(A \leftrightarrow B) = \begin{cases} 1, & \text{falls } \varphi(A) = \varphi(B) \\ 0, & \text{sonst,} \end{cases}$$

sind offenbar

- $\models (A \leftrightarrow B)$,
- $A \models\!=\!\mid B$,
- $A \models B$ und $B \models A$ und
- $\mathrm{Folg}(A) = \mathrm{Folg}(B)$

äquivalent.

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

1. $A \models\!=\!\mid B$, B enthält nur $\to$ und $\neg$ als log. Verknüpfungen

2. $A \models\!=\!\mid C$, C enthält nur $\wedge$ und $\neg$ als log. Verknüpfungen

3. $A \models\!=\!\mid D$, D enthält nur $\vee$ und $\neg$ als log. Verknüpfungen

1.14 Definition. Eine Menge $\mathrm{OP} \subseteq \{\neg, \vee, \wedge, \to, \leftrightarrow, \ldots\}$ von Operatoren (Junktoren) heißt *vollständig,* falls es zu jedem $A \in F$ eine logisch äquivalente Aussageform $B \in F(\mathrm{OP})$ gibt.

Vollständige Operatormengen für die Aussagenlogik sind z.B.: $\{\neg, \to\}$, $\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \vee, \wedge\}$ und $\{\text{false}, \to\}$. Dabei ist false eine Konstante (nullstelliger Operator) mit $\varphi(\text{false}) = 0$ für jede Bewertung φ. Offenbar gilt

$$\neg A \models\!=\!\mid (A \to \text{false}).$$

Jede Aussageform $A(p_1, \ldots, p_n)$ stellt in natürlicher Form eine Bool'sche Funktion $f_A : \mathbb{B}^n \to \mathbb{B}$ dar, nämlich durch die Festlegung $f_A(b_1, \ldots, b_n) = \varphi_{\vec{b}}(A)$ mit einer Bewertung $\varphi_{\vec{b}}$ mit $\varphi_{\vec{b}}(p_i) = b_i$ für $1 \leq i \leq n$.

1.3 Das deduktive System $\mathcal{F}_0$

Bisher wurde die Semantik einer Sprache der Aussagenlogik mit Hilfe einer Bewertungsfunktion φ erklärt, die jeder syntaktisch korrekten Formel einen Wahrheitswert zuordnete. Der nächste Abschnitt beschäftigt sich mit einem axiomatischen Aufbau der Aussagenlogik mittels eines "Deduktiven Systems". Eine syntaktisch korrekte Formel in einem Deduktiven System wird "Theorem" genannt, wenn sie durch rein mechanische Anwendungen der Regeln des Systems auf die Axiome des Systems "abgeleitet" werden kann. Man kann deduktive Systeme angeben, in denen aussagenlogische Formeln genau dann Theoreme sind, wenn sie auch Tautologien sind.

1.15 Definition. 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 $\frac{A_1, \ldots, A_n}{A}$, $n \geq 0$.

Die Mengen F, Ax und R sind im allgemeinen rekursiv.
Die Menge $T = T(\mathcal{F})$ der *Theoreme* ist definiert durch:

1. $\mathrm{Ax} \in T$ (d.h. alle Axiome sind Theoreme)
2. Sind $A_1, \ldots, A_n \in T$ und ist die Regel $\frac{A_1, \ldots, A_n}{A}$ 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".
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.

1.16 Bemerkungen.

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: $B_i \in \mathrm{Ax}$ 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* 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.

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

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

ist rekursiv.

$T = \{A \mid \vdash A\} = \{A \mid \text{Es gibt Beweis } B_1, \ldots, B_n \text{ mit } B_n = A\}$.

Beachte: Beweise sind im allgemeinen nicht eindeutig. Es wird im allgemeinen nicht verlangt, dass T von R frei erzeugt wird.

3. Im Zusammenhang mit Deduktiven Systemen liegt die Frage nach einer automatischen Beweisfindung nahe: Ist T rekursiv entscheidbar? Oder speziell: 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 Axiom $(A \to (B \to A))$ die Menge $\{A_0 \mid \text{es gibt } A, B \in F \text{ mit } A_0 \equiv (A \to (B \to A))\}$ und die Regel $\frac{A, A \to B}{B}$ beschreibt die Menge

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

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

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

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

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

Dabei beschreiben Ax1, Ax2 und Ax3 disjunkte Formelmengen. Die Regelmenge R wird beschrieben durch das Regelschema

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

Beachte: Es genügen Axiome für Formeln in $\to$ und $\neg$, da alle anderen Formeln zu einer Formel in $\to$ und $\neg$ logisch äquivalent sind ($\{\neg, \to\}$ ist vollständig):

$$\begin{aligned} A \wedge B &\models\!\!\!\!= \!\!\!\!\!\mid\; \neg(A \to (\neg B)) \\ A \vee B &\models\!\!\!\!= \!\!\!\!\!\mid\; (\neg A) \to B \\ A \leftrightarrow B &\models\!\!\!\!= \!\!\!\!\!\mid\; (A \to B) \wedge (B \to A) \end{aligned}$$

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: Für jedes $A \in F_0$ gilt $\vdash (A \to A)$.

Beweis.

$B_0 \equiv (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	Ax2
$B_1 \equiv A \to ((A \to A) \to A)$	Ax1
$B_2 \equiv (A \to (A \to A)) \to (A \to A)$	$\mathrm{MP}(B_0, B_1)$
$B_3 \equiv A \to (A \to A)$	Ax1
$B_4 \equiv A \to A$	$\mathrm{MP}(B_2, B_3)$

■

1.18 Definition (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 $\Sigma \vdash_{\mathcal{F}_0} A$ oder einfach $\Sigma \vdash A$.

   $B_0, \ldots, B_n$ 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 $B_k \equiv B_j \to B_i$.

2. Σ heißt *konsistent*, falls für keine Formel $A \in F_0$ gilt $\Sigma \vdash A$ und $\Sigma \vdash \neg A$.

1.19 Folgerungen und Bemerkungen.

1. Gilt $\Sigma \vdash A$, so folgt unmittelbar aus der Definition 1.18, dass es eine endliche Teilmenge $\Sigma_0 \subseteq \Sigma$ gibt mit $\Sigma_0 \vdash A$. Das 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. Aus $\Sigma \vdash A$ und $\Gamma \vdash B$ für alle $B \in \Sigma$ folgt $\Gamma \vdash A$. Gilt $\Gamma \vdash \Sigma$ (d.h. $\Gamma \vdash A$ für alle $A \in \Sigma$) und $\Sigma \vdash \Delta$, dann gilt $\Gamma \vdash \Delta$. Beweise lassen sich also zusammensetzen.

1.20 Satz (Deduktionstheorem). Sei $\Sigma \subseteq F_0$ und seien $A, B \in F_0$.
Es gilt genau dann $\Sigma, A \vdash B$, wenn $\Sigma \vdash (A \to B)$ gilt.

Beweis.
"$\Longleftarrow$": klar wegen Modus Ponens.
"$\Longrightarrow$": Sei $B_0, \ldots, B_m$ ein Beweis für $\Sigma, A \vdash B$, also $B_m \equiv B$. Für $i = 0, \ldots, m$ gilt $\Sigma \vdash (A \to B_i)$. $(\star)$.
Aus $(\star)$ folgt die Behauptung.
Beweis von $(\star)$:

1. $B_i \equiv A$: Nach dem Beispiel zur Definition 1.17 gilt dann $\vdash A \to B_i$ und somit aber auch $\Sigma \vdash A \to B_i$.

2. $B_i \in \mathrm{Ax} \cup \Sigma$: dann gilt $\Sigma \vdash (A \to B_i)$ wegen der Beweissequenz:

B_i	Axiom ($B_i \in \mathrm{Ax}$) oder Hypothese ($B_i \in \Sigma$)
$B_i \to (A \to B_i)$	Axiom
$A \to B_i$	MP

3. B_i entsteht aus B_j, B_k mit MP, d.h. $B_k \equiv B_j \to B_i$ mit $j, k < i$, und $\Sigma \vdash A \to B_j$ und $\Sigma \vdash A \to (B_j \to B_i)$ sind bereits bekannt, dann ist ein Beweis für $\Sigma \vdash A \to B_i$:

$(A \to (B_j \to B_i)) \to ((A \to B_j) \to (A \to B_i))$	Ax2
$\vdots$ (Beweis für $\Sigma \vdash A \to (B_j \to B_i)$)	
$(A \to B_j) \to (A \to B_i)$	MP
$\vdots$ (Beweis für $\Sigma \vdash A \to B_j$)	
$A \to B_i$	MP

■

1.21 Beispiele. $B_1, \ldots, B_n$ 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. $\vdash (A \to A)$ folgt aus dem Deduktionstheorem, da $A \vdash A$ gilt.

2. Um $A \to B, B \to C \vdash A \to C$ zu zeigen, zeige $A, A \to B, B \to C \vdash C$.

3. $\neg\neg A \vdash A$
   Beweis:

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

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:

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

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

1.22 Satz (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.

Beweis.

Korrektheit: Alle Axiome (Schemata) sind Tautologien. Sind A und $A \to B$ Tautologien, so ist auch B eine Tautologie, d.h. Tautologien sind abgeschlossen gegenüber Modus-Ponens-Regel (s. Lemma 1.9).

Vollständigkeit: Zeige: Gilt $\models A$ dann ist A in $\mathcal{F}_0$ herleitbar, d.h. $\vdash A$.

Lemma: 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

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

$(1 \le i \le n)$, 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 $\varphi'(p_n) = 0$, erhält man $P_1, \ldots, P_{n-1}, \neg p_n \vdash A$.

Durch Anwenden des Deduktionstheorems entstehen daraus

$$P_1, \ldots, P_{n-1} \vdash p_n \to A \text{ und } P_1, \ldots, P_{n-1} \vdash (\neg p_n) \to A.$$

Gleichzeitig gilt nach dem 10. Beispiel von 1.21 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

$$P_1, \ldots, P_{n-1} \vdash A.$$

Das kann man für jedes i machen, d.h. in der Herleitung von A wird kein p_i verwendet, also $\vdash A$.

Beweis des Lemma. Induktion über den Aufbau der Formel A:

$A \equiv p_1 \in V$**:** $\varphi(A) = \varphi(p_1)$ und folglich $p_1 \vdash A'$ wegen $A' = A$.

$A \equiv \neg C$**:** Ist $\varphi(A) = 1$, dann ist $\varphi(C) = 0$ und $C' \equiv \neg C$. Nach Induktionsvoraussetzung gilt $P_1, \ldots, P_n \vdash C'$ mit $C' \equiv \neg C \equiv A$.

Ist $\varphi(A) = 0$, dann ist $\varphi(C) = 1$, $C' \equiv C$ und $A' \equiv \neg A \equiv \neg\neg C$. Nach Induktionsvoraussetzung gilt $P_1, \ldots, P_n \vdash C'$ und nach dem 7. Beispiel von 1.21 gilt $P_1, \ldots, P_n \vdash (C \to \neg\neg C)$. Durch Anwenden der Modus-Ponens Regel erhält man $P_1, \ldots, P_n \vdash \neg\neg C$.

$A \equiv B \to C$ **:** Ist $\varphi(A) = 0$, dann ist $\varphi(B) = 1$ und $\varphi(C) = 0$. Ferner gilt dann $A' \equiv \neg A \equiv \neg(B \to C)$, $B' \equiv B$ und $C' \equiv \neg C$. Nach Induktionsvoraussetzung gilt $P_1, \ldots, P_n \vdash B'$ und $P_1, \ldots, P_n \vdash C'$. Zusammen mit $P_1, \ldots, P_n \vdash B \to (\neg C \to \neg(B \to C))$ von 9. Beispiel in 1.21 und zweimaligem Anwenden des MP folgt $P_1, \ldots, P_n \vdash A'$.

Ist $\varphi(A) = 1$ dann ist $\varphi(C) = 1$ oder $\varphi(B) = 0$. Ferner gilt dann $A' \equiv B \to C$. Nach Induktionsvoraussetzung gilt $P_1, \ldots, P_n \vdash C$ oder $P_1, \ldots, P_n \vdash \neg B$. Gilt $P_1, \ldots, P_n, B \vdash C$, folgt nach Deduktionstheorem auch $P_1, \ldots, P_n \vdash B \to C$. Ist andererseits $P_1, \ldots, P_n, \neg C \vdash \neg B$ und somit $P_1, \ldots, P_n \vdash (\neg C \to \neg B)$. Nach dem 8. Beispiel von 1.21 gilt dann $P_1, \ldots, P_n \vdash B \to C$.

■

1.23 Folgerung. 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.

Beweis.

1.

$$\begin{aligned}
\Sigma \vdash A \quad &\overset{1.19}{\iff} \quad \text{Es gibt } A_1, \ldots, A_n \in \Sigma \text{ mit } A_1, \ldots, A_n \vdash_{\mathcal{F}_0} A \\
&\overset{\text{D.T.}}{\iff} \quad \text{Es gibt } A_1, \ldots, A_n \in \Sigma \text{ mit } \vdash_{\mathcal{F}_0} (A_1 \to (A_2 \to \ldots (A_n \to A) \ldots) \\
&\overset{1.22}{\iff} \quad \text{Es gibt } A_1, \ldots, A_n \in \Sigma \text{ mit } \models (A_1 \to (A_2 \to \ldots (A_n \to A) \ldots) \\
&\overset{\text{D.T.}}{\iff} \quad \text{Es gibt } A_1, \ldots, A_n \in \Sigma \text{ mit } A_1, \ldots, A_n \models A \\
&\overset{\text{K.S.}}{\iff} \quad \Sigma \models A
\end{aligned}$$

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.

■

1.4 Das Gentzen-Sequenzenkalkül

Es gibt andere deduktive Systeme, für die Satz 1.22 gilt. Das deduktive System $\mathcal{F}_0$ wurde von S.C. Kleene eingeführt. Das folgende deduktive System geht auf G. Gentzen zurück.

1.24 Definition. Das *Gentzen-Sequenzenkalkül*: Eine Sequenz ist eine Zeichenreihe der Form $\Gamma \Rightarrow \Delta$ mit zwei endlichen Mengen von Formeln Γ und Δ. Seien $\Gamma, \Delta \subseteq F$ endliche Mengen von Formeln und $A, B \in F$.

$\Gamma \vdash_G \Delta$ wird definiert durch:

die Axiome Ax1: $\Gamma, A \Rightarrow A, \Delta$

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

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

die Regeln R1: $\dfrac{\Gamma, A, B \Rightarrow \Delta}{\Gamma, A \wedge B \Rightarrow \Delta}$

R2: $\dfrac{\Gamma \Rightarrow A, B, \Delta}{\Gamma \Rightarrow (A \vee B), \Delta}$

R3: $\dfrac{\Gamma, A \Rightarrow \Delta, B}{\Gamma \Rightarrow (A \rightarrow B), \Delta}$

R4a: $\dfrac{\Gamma, A \Rightarrow \Delta}{\Gamma \Rightarrow \neg A, \Delta}$

R4b: $\dfrac{\Gamma \Rightarrow A, \Delta}{\Gamma, \neg A \Rightarrow \Delta}$

R5: $\dfrac{\Gamma \Rightarrow A, \Delta; \quad \Gamma \Rightarrow B, \Delta}{\Gamma \Rightarrow (A \wedge B), \Delta}$

R6: $\dfrac{\Gamma, A \Rightarrow \Delta; \quad \Gamma, B \Rightarrow \Delta}{\Gamma, (A \vee B) \Rightarrow \Delta}$

R7: $\dfrac{\Gamma \Rightarrow A, \Delta; \quad \Gamma, B \Rightarrow \Delta}{\Gamma, (A \rightarrow B) \Rightarrow \Delta}$

$\Gamma \vdash_G \Delta$ bedeutet, dass es ein $r \in \mathbb{N}$ und eine Folge von Sequenzen

$$\Gamma_1 \Rightarrow \Delta_1, \ldots, \Gamma_r \Rightarrow \Delta_r$$

gibt, für die folgendes gilt:

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

1.25 Bemerkung. 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 $\Delta = \{B_1, \ldots, B_m\}$ entspricht dies also der Formel $A_1 \wedge \cdots \wedge A_n \rightarrow (B_1 \vee \cdots \vee B_m)$.

1.26 Beispiel. $p \vee q, (\neg p) \vee r \vdash_G q \vee r$

Beweis:

$B_1 \equiv q, r \Rightarrow q, r$	Ax1
$B_2 \equiv q, \neg p \Rightarrow q, r$	Ax1
$B_3 \equiv q, (\neg p) \vee r \Rightarrow q, r$	R6(1,2)
$B_4 \equiv p, r \Rightarrow q, r$	Ax1
$B_5 \equiv \neg p, p \Rightarrow q, r$	Ax2
$B_6 \equiv p, (\neg p) \vee r \Rightarrow q, r$	R6(4,5)
$B_7 \equiv p \vee q, (\neg p) \vee r \Rightarrow q, r$	R6(3,6)
$B_8 \equiv p \vee q, (\neg p) \vee r \Rightarrow q \vee r$	R2(6)

1.27 Bemerkung.

1. Aus $\Gamma \vdash_G \Delta$ folgt $\Gamma \models \Delta$. (Korrektheit)
2. Aus $\Gamma \models A$ folgt $\Gamma \vdash_G A$. (Vollständigkeit)

1.5 Semantische Tableaux

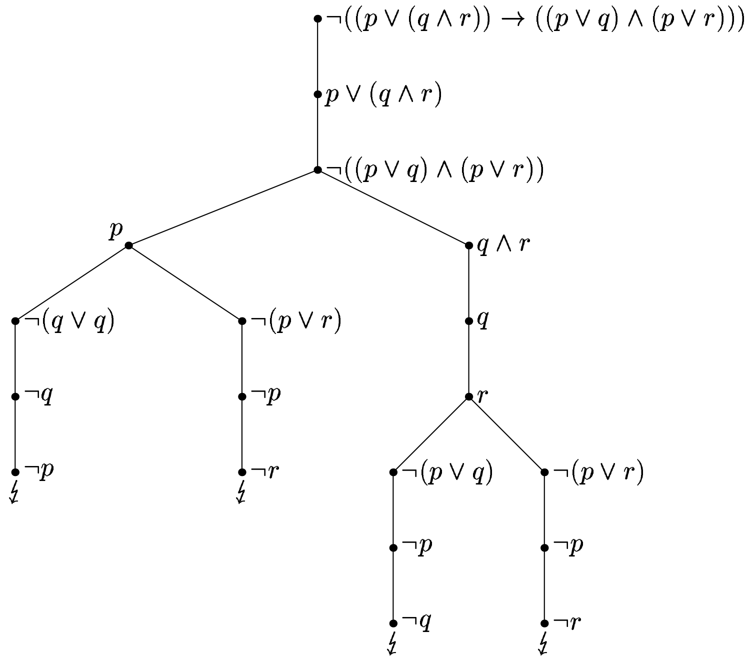
Wie erreicht man eine Systematisierung des Beweisens in einem deduktiven System? Gibt es eine Möglichkeit "automatisch" einen Beweis zu finden, ohne dazu alle Beweise der Reihe nach aufzuzählen?

Nach einer denotationalen und axiomatischen Definition der Semantik der Aussagenlogik wird im folgenden ein algorithmischer Aufbau betrachtet: Um zu entscheiden, ob $\Sigma \vdash A$ für eine gegebene (endliche) Formelmenge Σ und eine Aussageform A gilt, wird ein Algorithmus angegeben. Da in Σ und A nur endlich viele Variablen vorkommen, braucht der Algorithmus nur systematisch alle möglichen Belegungen zu prüfen.

1.28 Beispiel. Mit der Idee "$\Sigma \vdash A \iff \Sigma \cup \{\neg A\}$ ist nicht erfüllbar" versucht man, um die Allgemeingültigkeit einer Formel A zu zeigen, einen binären Baum für $\neg A$ zu konstruieren, dessen Knoten jeweils eine Klasse möglicher Belegungen repräsentieren. Die Wurzel des Baumes repräsentiert alle möglichen Belegungen und die Vereinigung der Klassen der Söhne eines inneren Knotens des Baumes ist die Klasse der Belegungen, die der Knoten repräsentiert. Gelingt es, einen solchen Baum derart zu konstruieren, dass sämtliche Blätter des Baumes zu einem Widerspruch zu der Annahme führen, eine Klasse von Belegungen, die durch Knoten auf dem Weg von der Wurzel zu dem entsprechenden Blatt repräsentiert wird, enthalte Belegungen, die $\neg A$ erfüllen, ist gezeigt, dass es keine Belegung gibt, die $\neg A$ erfüllt. Somit gilt, dass A Tautologie ist.

$\models (p \vee (q \wedge r) \rightarrow (p \vee q) \wedge (p \vee r))$ gilt genau dann, wenn $\neg((p \vee (q \wedge r)) \rightarrow$

$((p \vee q) \wedge (p \vee r)))$ unerfüllbar ist.



Da alle Äste zu Widersprüchen führen, gibt es keine Belegung, die die Formel erfüllt!

Man unterscheidet zwei Arten von Formeln, nämlich solche, die zu Verzweigungen führen (β-Formeln), und solche, die nicht zu Verzweigungen führen (α-Formeln).

Folgende Formeln sind α-Formeln, die zu Knoten mit den Markierungen α_1 und α_2 führen:

α	$\neg\neg A$	$A_1 \wedge A_2$	$\neg(A_1 \vee A_2)$	$\neg(A_1 \to A_2)$
α_1	A	A_1	$\neg A_1$	A_1
α_2	(A)	A_2	$\neg A_2$	$\neg A_2$

Folgende Formeln sind β-Formeln, die zu Verzweigungen führen mit Knotenmarkierungen β_1 und

β		$\neg(A_1 \wedge A_2)$		$A_1 \vee A_2$		$A_1 \to A_2$	
β_1	β_2	$\neg A_1$	$\neg A_2$	A_1	A_2	$\neg A_1$	A_2

Beachte: Jede Aussageform ist entweder atomar (d.h. eine Variable) oder die Negation einer atomaren Formel oder eine α- oder eine β-Formel, und genau von einem dieser Typen.

Es gilt: Eine α-Formel ist genau dann erfüllbar, wenn beide Komponenten α_1 und α_2 erfüllbar sind. Eine β-Formel ist genau dann erfüllbar, wenn eine der Komponenten β_1 oder β_2 erfüllbar ist.

Insbesondere gilt für $\Gamma \subseteq F$ und α-Formel α mit Komponenten α_1 und α_2 und β-Formel β mit Komponenten β_1 und β_2: Genau dann ist $\Gamma \cup \{\alpha\}$ erfüllbar, wenn $\Gamma \cup \{\alpha_1, \alpha_2\}$ erfüllbar ist und genau dann ist $\Gamma \cup \{\beta\}$ erfüllbar, wenn $\Gamma \cup \{\beta_1\}$ oder $\Gamma \cup \{\beta_2\}$ erfüllbar ist.

1.29 Definition. *Tableaux* sind binäre Bäume mit Knoten, die mit Formeln aus F markiert sind. Sei $\Sigma \subseteq F$.

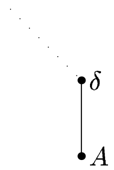
1. Die Menge der Tableaux τ_Σ für Σ wird induktiv definiert durch:

   (a) $\tau_{\{A\}}$ ist der Baum mit einem Knoten, der mit A markiert ist. In diesem Fall schreibt man auch τ_A statt $\tau_{\{A\}}$. Graphisch:

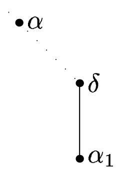
   $$\bullet A$$

   (b) Ist τ Tableau für Σ und δ Marke eines Blattes von τ, so lässt sich τ wie folgt zu einem Tableau τ' für Σ fortsetzen: τ' entsteht aus τ indem man als Nachfolger von δ:

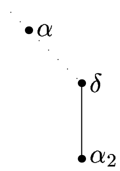
   (Σ) einen Knoten hinzufügt, der mit einer Formel $A \in \Sigma$ markiert ist. (A soll nicht bereits als Marke im Ast von δ vorkommen.) Graphisch:



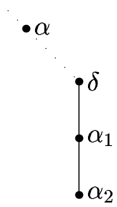
   (α) einen Knoten hinzufügt, der mit α_1 oder α_2 markiert ist, falls eine α-Formel α auf dem Ast zu δ vorkommt und α_1 und α_2 die Komponenten von α sind. Graphisch:



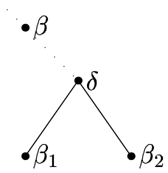
oder



   In der Praxis werden jedoch δ nacheinander Knoten für beide Komponenten hinzugefügt:



(β) zwei Knoten hinzufügt, die mit den Komponenten β_1 bzw. β_2 einer β-Formel β markiert sind, falls β auf dem Ast zu δ vorkommt. Graphisch:



Entsteht τ' aus τ durch Anwendung einer der Regeln $(\Sigma), (\alpha)$ oder (β), so heißt τ' *direkte Fortsetzung* von τ.

(c) $\tau \in \mathcal{T}_\Sigma$ genau dann, wenn $\tau = \tau_A$ für ein $A \in \Sigma$ oder es gibt eine Folge $\tau_0, \dots, \tau_n (= \tau)$, $n \in \mathbb{N}$, so dass τ_{j+1} eine direkte Fortsetzung von τ_j ist für $j = 0, \dots, n-1$ und $\tau_0 = \tau_A$ für ein $A \in \Sigma$.

2. Ein *Ast* eines Tableaus τ heißt *abgeschlossen*, falls er zwei konjugierte Formeln enthält (d.h. für ein $A \in F$ sowohl A als auch $(\neg A)$ enthält), sonst heißt der Ast *offen*. Ein Tableau τ heißt *abgeschlossen*, wenn jeder Ast von τ abgeschlossen ist. τ heißt *erfüllbar*, wenn τ einen *erfüllbaren Ast* (d.h. die Marken entlang des Ast bilden eine erfüllbare Formelmenge) enthält.

3. Sei $\Gamma \subseteq F, A \in F$. Dann ist A Tableau-Folgerung aus Γ ($\Gamma \vdash_\tau A$) genau dann, wenn für $\Sigma = \Gamma \cup \{\neg A\}$ jedes Tableau aus $\mathcal{T}_\Sigma$ sich zu einem abgeschlossenen Tableau aus $\mathcal{T}_\Sigma$ fortsetzen lässt.

1.30 Bemerkungen und Beispiele. Ziel ist es zu zeigen: $\Gamma \vdash_\tau A \iff \Gamma \models A$.

1. Abgeschlossene Äste sind nicht erfüllbar. Abgeschlossene Tableaux sind nicht erfüllbar.

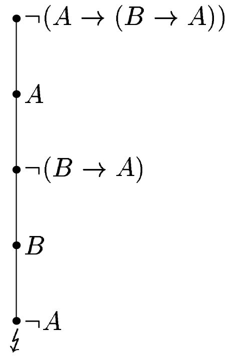
2. Ist Γ erfüllbar, so ist jedes Tableau aus $\mathcal{T}_\Gamma$ erfüllbar (und insbesondere nicht abgeschlossen).

3. Gilt $\Gamma \vdash_\tau A$, so ist $\Sigma = \Gamma \cup \{\neg A\}$ nicht erfüllbar. Insbesondere sind Tableau-Folgerungen korrekt (d.h. aus $\Gamma \vdash_\tau A$ folgt $\Gamma \models A$).

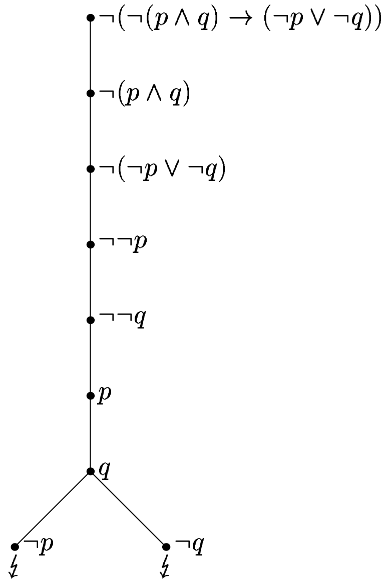
4. Gibt es ein abgeschlossenes Tableau in $\mathcal{T}_\Gamma$, so lässt sich jedes Tableau aus $\mathcal{T}_\Gamma$ zu einem abgeschlossenen Tableau fortsetzen.

5. Beispiele:

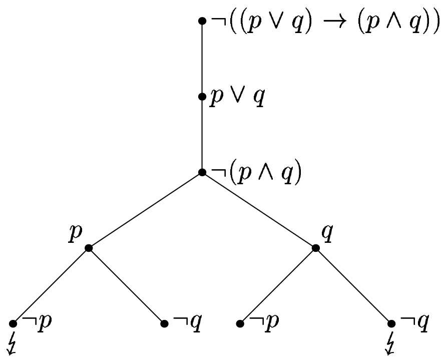
(a) $\vdash_\tau A \to (B \to A)$:



(b) $\vdash_\tau \neg(p \wedge q) \to (\neg p \vee \neg q)$:



(c) $\vdash_\tau (p \vee q) \to (p \wedge q)$ gilt nicht:



Es gibt Belegungen, die $\neg((p \vee q) \to (p \wedge q))$ erfüllen, nämlich φ mit $\varphi(p) = 1$ und $\varphi(q) = 0$ und φ' $\varphi'(p) = 0$ und $\varphi'(q) = 1$. Also gilt nicht $\vdash_\tau (p \vee q) \to (p \wedge q)$.

1.31 Definition. Sei $\Sigma \subseteq F, \tau \in \mathcal{T}_\Sigma$ und σ ein Ast von τ, bzw. die Menge der Formeln, die in dem Ast vorkommen. σ heißt *vollständig*, falls für jede α-Formel $\alpha \in \sigma$ stets $\{\alpha_1, \alpha_2\} \subseteq \sigma$ gilt und für jede β-Formel $\beta \in \sigma$ entweder $\beta_1 \in \sigma$ oder $\beta_2 \in \sigma$ gilt. τ heißt *vollständig*, falls gilt: Jeder Ast von τ ist entweder abgeschlossen oder "vollständig und enthält Σ". (Beachte: Falls Σ unendlich ist, sind unendliche Bäume zugelassen.)

1.32 Bemerkungen.

1. Ist Σ endlich, so lässt sich jedes Tableau aus $\mathcal{T}_\Sigma$ zu einem vollständigen Tableau für Σ mit Hilfe von Σ-, α- und β-Regeln erweitern. Beachte, dass α- und β- Regeln nur Teilformeln einführen und dass eine Formel nur endlich viele Teilformeln enthalten kann.

2. Sei σ die Menge der Formeln eines <u>vollständigen offenen</u> Astes von τ. Dann gilt:

   (a) Es gibt kein $p \in V$ mit $\{p, \neg p\} \subseteq \sigma$.

   (b) Ist $\alpha \in \sigma$, so auch $\alpha_1, \alpha_2 \in \sigma$.

   (c) Ist $\beta \in \sigma$, so ist $\beta_1 \in \sigma$ oder $\beta_2 \in \sigma$.

1.33 Lemma. Jede Menge Σ von Formeln, die (a), (b) und (c) aus der Bemerkung 1.32.2 genügt, ist erfüllbar. Insbesondere sind vollständige offene Äste von Tableaux erfüllbar.

Beweis. Definiere:

$$\varphi(p) = \begin{cases} 0, & \neg p \in \Sigma \\ 1, & \text{sonst} \end{cases}$$

Offensichtlich ist φ wohldefiniert.

Beh.: Falls $A \in \Sigma$, dann $\varphi(A) = 1$.

Induktion über den Aufbau von A :

A atomare oder negierte atomare Formel $\checkmark$

Sei A eine α-Formel und $A \in \Sigma$, dann sind nach 1.32.2.a die Teilformeln α_1 und α_2 von A in Σ. Nach Induktionsvoraussetzung gilt $\varphi(\alpha_1) = \varphi(\alpha_2) = 1$ woraus $\varphi(A) = 1$ folgt.

Sei A eine β-Formel und $A \in \Sigma$. Dann ist die Teilformel β_1 oder β_2 nach 1.32.2.c in Σ. Nach Induktionsvoraussetzung gilt $\varphi(\beta_1) = 1$ oder $\varphi(\beta_2) = 1$. Somit folgt $\varphi(A) = 1$. ∎

1.34 Satz. Sei $\Gamma \subseteq F$. Dann gilt:

1. Genau dann ist Γ nicht erfüllbar, wenn $\mathcal{T}_\Gamma$ ein abgeschlossenes Tableau enthält.

2. Äquivalent sind
   - $\Gamma \models A$,
   - $\Gamma \vdash A$ und
   - $\tau_{\{\Gamma, \neg A\}}$ enthält ein abgeschlossenes Tableau.
3. Äquivalent sind
   - $\models A$,
   - $\vdash A$ und
   - $\tau_{\neg A}$ enthält ein abgeschlossenes Tableau.

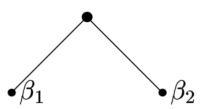
Beachte: Der Kompaktheitssatz (1.10) folgt aus 1., denn ist Γ nicht erfüllbar, enthält τ_Γ ein abgeschlossenes Tableau und abgeschlossene Tableaux sind stets endliche Bäume, d.h. eine endliche Teilmenge von Γ ist nicht erfüllbar.

Beweis. zu 1.
"$\Longleftarrow$": siehe 1.30.2.
"$\Longrightarrow$": Jedes vollständige Tableau τ für Γ ist abgeschlossen, sonst enthält τ einen vollständigen offenen Ast, der ganz Γ enthält und somit wäre Γ nach 1.33 erfüllbar. ■

Gibt es immer vollständige Tableaux in τ_Γ für $\Gamma \subseteq F$? Falls Γ endlich ist, dann siehe 1.32.1. Was sind aber vollständige Tableaux, wenn Γ unendlich ist? Dazu zunächst ein systematisches Verfahren zur Tableaukonstruktion.

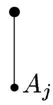
Systematische Tableaukonstruktion: Sei $\Gamma \subseteq F$, dann ist Γ abzählbar. Sei also $\Gamma = \{A_1, A_2, \ldots\}$. Konstruktion einer Folge von Tableaux τ_n $(n \in \mathbb{N})$:

1. $\tau_1 \equiv A_1$. Ist A_1 (negierte) atomare Formel, dann wird der Knoten markiert.
2. Sind alle Äste von τ_n abgeschlossen, dann Stopp!
3. τ_{n+1} entsteht aus τ_n wie folgt:
   (a) Ist Y die erste unmarkierte α-Formel in τ_n, durch die ein offener Ast geht, so markiere Y und erweitere jeden offenen Ast, der durch Y geht, um die Teilformeln α_1 und α_2 von Y. α_1 und α_2 werden markiert, falls sie atomare oder negierte atomare Formeln sind. Dadurch werden möglicherweise Äste abgeschlossen. sonst:
   (b) Ist Y die erste unmarkierte β-Formel in τ_n, durch die ein offener Ast geht, so markiere Y und erweitere jeden offenen Ast, der durch Y geht, um



   Markiere β_1 und/oder β_2, falls diese (negierte) atomare Formeln sind. Dadurch werden möglicherweise Äste abgeschlossen. sonst:

(c) Gibt es eine Formel $A_j \in \Gamma$, die noch nicht in jedem offenen Ast vorkommt, so erweitere alle diese Äste um:



Falls möglich, Knoten markieren und Äste abschließen.

Gehe zu Schritt (2).

Aus τ_n ($n \geq 1$) erhält man kein weiteres Tableau, falls τ_n abgeschlossen ist oder alle Formeln von τ_n markiert sind und Γ endlich ist.

Setze $\tau_\infty := \bigcup_{n \in \mathbb{N}} \tau_n$. Dann ist τ_∞ ein binärer Baum. Behauptung: τ_∞ ist vollständig! Beweis:

1. $\tau_\infty = \tau_k$ für ein $k \in \mathbb{N}$.

   Ist τ_k abgeschlossen, gilt die Behauptung.

   Ist τ_k nicht abgeschlossen, ist τ_k vollständig: Alle Formeln sind markiert und Γ muss endlich sein. Alle Formeln von Γ sind in offenen Ästen von τ_k. Somit ist Γ nach Lemma 1.33 erfüllbar.

2. Es gibt kein $k \in \mathbb{N}$ mit $\tau_\infty = \tau_k$. Dann ist τ_∞ ein unendlicher Baum. Es gibt eine Folge von Knoten $\{Y_n\}, n \in \mathbb{N}$, die unendlich viele Nachfolger haben: Setze $Y_1 = A_1$, die Wurzel mit unendlich vielen Nachfolgerknoten. Ist Y_n bereits gefunden, dann hat Y_n entweder einen oder zwei direkte Nachfolger, von denen einer unendlich viele Nachfolger hat. Wähle als Y_{n+1} diesen Knoten. Dann ist der Ast $\{Y_n | n \in \mathbb{N}\}$ in τ_∞, offen, vollständig und enthält Γ, d.h. Γ ist erfüllbar.

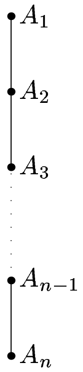
1.35 Bemerkung und Folgerung.

1. Ist Γ eine rekursiv aufzählbare Menge, so ist das Hinzufügen einer Formel $A_n \in \Gamma$ zu einem Tableau effektiv, d.h. falls Γ rekursiv aufzählbar aber nicht erfüllbar ist, so stoppt die systematische Tableau-Konstruktion. Insbesondere stoppt die systematische Tableau-Konstruktion immer, wenn Γ endlich ist. Sie liefert dann entweder: Γ ist nicht erfüllbar, d.h. es gibt eine $n \in \mathbb{N}$, so dass τ_n abgeschlossen ist, oder: Γ ist erfüllbar und die (offenen) Äste von τ_n liefern alle Belegungen, die Γ erfüllen.

   Die systematische Tableau-Konstruktion liefert also für endliche Mengen alle Belegungen der wesentlichen Variablen, die Γ erfüllen.

2. Zur Vereinfachung der systematischen Tableau-Konstruktion für eine Men-

ge $\Gamma = \{A_1, \dots, A_n\}$ beginne mit



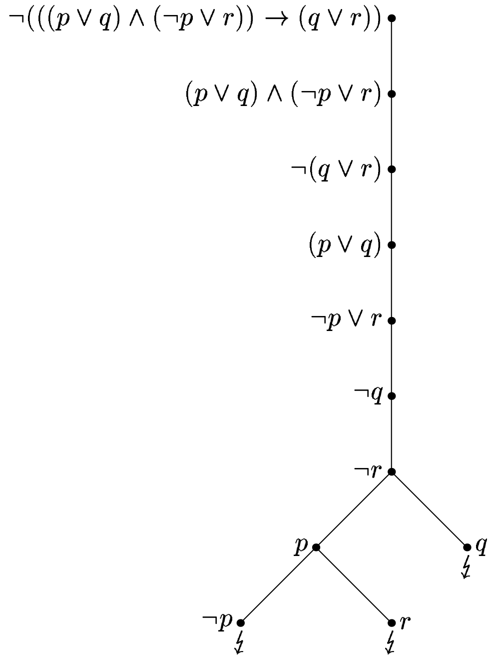
als Anfangsbaum.

3.

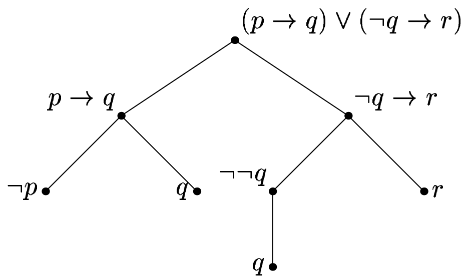
$$\begin{aligned} \Gamma \models A &\iff \Gamma \cup \{\neg A\} \text{ unerfüllbar} \\ &\iff \tau_{\{\Gamma, \neg A\}} \text{ enthält abgeschlossenes Tableau} \\ &\iff \Gamma \vdash_\tau A \end{aligned}$$

4. Beispiele:

(a) $\models ((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$ oder $(p \vee q) \wedge (\neg p \vee r) \models (q \vee r)$



(b) Bestimme alle Belegungen, die $A \equiv (p \to q) \vee (\neg q \to r)$ erfüllen!



Demnach ist $\{\varphi \mid \varphi$ ist Bewertung mit $\varphi(p) = 0$ oder $\varphi(q) = 1$ oder $\varphi(r) = 1\}$ die Menge aller Belegungen, die A erfüllen. An den Blättern des Baumes lässt sich auch die äquivalente Disjunktive Normalform (DNF) zur Formel A ablesen, nämlich $\neg p \vee q \vee r$.