3 Aussagenlogik

3.1 Syntax 3.1.1 Formeln

- **Definition 3.1** Ein **Alphabet** Σ ist eine endliche oder abzählbar unendlichen Menge. Die Elemente dieser Menge werden **Zeichen** genannt. Ohne Beschränkung der Allgemeinheit (oBdA) nehmen wir an, dass $\Lambda \not\in \Sigma$.

- **Definition 3.2** Sei Σ ein Alphabet. Die Menge der **Wörter** (oder **Zeichenreihen**) über Σ wird mit Σ^* bezeichnet und ist die kleinste Menge, die die folgenden Bedingungen erfüllt:

  1. $\Lambda \in \Sigma^*$.
  2. Wenn $w \in \Sigma^*$ und $a \in \Sigma$ ist, dann ist $aw \in \Sigma^*$.

  Λ wird **leeres Wort** oder **leere Zeichenreihe** genannt.

- **Beispiel** Sei $\Sigma = \{1, 2\}$. Wir können die folgenden Wörter bilden:

$$\Lambda,\ 1\Lambda,\ 2\Lambda,\ 11\Lambda,\ 12\Lambda,\ 21\Lambda,\ 22\Lambda,\ 111\Lambda,\ \ldots\ .$$

Das Alphabet der Aussagenlogik

- **Definition 3.3** Ein **Alphabet der Aussagenlogik** besteht aus
  - einer (abzählbar) unendlichen Menge $\mathcal{R} = \{p_1, p_2, \ldots\}$ von aussagenlogischen Variablen,
  - der Menge $\{\neg/1, \wedge/2, \vee/2, \rightarrow/2, \leftrightarrow/2\}$ von Junktoren und
  - den Menge $\{(,)\}$ der Sonderzeichen.
- Indexe von aussagenlogischen Variablen werden manchmal weggelassen.
- Wir werden manchmal auch andere Buchstaben zur Bezeichung von aussagenlogischen Variablen verwenden.
- Aussagenlogische Variable werden auch **0-stellige Relationssymbole** genannt.
- Verschiedene Alphabete der Aussagenlogik unterscheiden sich in $\mathcal{R}$.

Aussagenlogische Formeln

- **Definition 3.4** Eine (aussagenlogische) **atomare Formel**, auch kurz **Atom** genannt, ist eine aussagenlogische Variable.

- **Definition 3.5** Sei $\mathcal{R}$ eine Menge aussagenlogischer Variablen.
  Die Menge der (aussagenlogischen) **Formeln** ist die kleinste Menge $\mathcal{L}(\mathcal{R})$ von Zeichenreihen über $\mathcal{R}$, den Junktoren und den Sonderzeichen, die die folgenden Eigenschaften erfüllt:

  1. Wenn F eine atomare Formel ist, dann ist $F \in \mathcal{L}(\mathcal{R})$.
  2. Wenn $F \in \mathcal{L}(\mathcal{R})$, dann ist $\neg F \in \mathcal{L}(\mathcal{R})$.
  3. Wenn $\circ/2$ ein Junktor ist und $F,\ G \in \mathcal{L}(\mathcal{R})$ sind, dann ist $(F \circ G) \in \mathcal{L}(\mathcal{R})$.

- Gibt es eine solche kleinste Menge überhaupt?
  - Es gibt Mengen, die die drei Bedingungen erfüllen.
  - Der Durchschnitt von Mengen, die diese Bedingungen erfüllen, erfüllt wiederum diese Bedingungen.
  - Die kleinste Menge ist der Durchschnitt aller dieser Mengen.

Notation

- A (evtl. indiziert) bezeichnet ein Atom.
  F, G, H (evtl. indiziert) bezeichnen aussagenlogische Formeln.

Arithmetische Ausdrücke

- Ein Alphabet der Arithmetik besteht aus
  - der Menge der rationalen Zahlen $\mathbb{Q}$,
  - den Operatoren $+/2,\ -/2,\ \div/2$ und $\times/2$ sowie
  - den Sonderzeichen „(“ und „)“.

- Die Menge der arithmetischen Ausdrücke ist die kleinste Menge, die die folgenden Eigenschaften erfüllt:
  1. Wenn T eine rationale Zahl ist, dann ist T ein arithmetischer Ausdruck.
  2. Wenn $\circ/2$ ein Operator ist und $T_1,\ T_2$ arithmetische Ausdrücke sind, dann ist auch $(T_1 \circ T_2)$ ein arithmetischer Ausdruck.

Natürliche Zahlen in Nachfolgerdarstellung

- **Das Alphabet der natürlichen Zahlen besteht aus**
  - **dem Symbol 0,**
  - **einem einstelligen Operator $s/1$ sowie**
  - **den Sonderzeichen „(“ und „)“.**

- **Die Menge der natürlichen Zahlen ist die kleinste Menge, die die folgenden Bedingungen erfüllt:**
  1. **0 ist eine natürliche Zahl.**
  2. **Wenn N eine natürliche Zahl ist, dann ist auch $s(N)$ eine natürliche Zahl.**

3.1.2 Induktion und Rekursion

- Wie können wir Eigenschaften von Formeln beweisen?
- **Satz 3.6 (Prinzip der strukturellen Induktion)**
  Jede Formel besitzt eine Eigenschaft E, wenn folgende Bedingungen erfüllt sind:
  1. **Induktionsanfang**
     Jedes Atom besitzt die Eigenschaft E.
  2. **Induktionsschritte**
     Wenn F die Eigenschaft E besitzt, dann besitzt sie auch $\neg F$.
     Wenn $\circ/2$ ein Junktor ist und F und G die Eigenschaft E besitzen, dann besitzt auch $(F \circ G)$ die Eigenschaft E.
- **Beweis** Sei $\mathcal{E}$ die Menge aller Formeln, die die Eigenschaft E erfüllen.
  - $\mathcal{E} \subseteq \mathcal{L}(\mathcal{R})$
  - $\mathcal{E}$ erfüllt die drei Bedingungen der Definition 3.5.
  - Da $\mathcal{L}(\mathcal{R})$ die kleinste Menge ist, die diese Bedingungen erfüllt, muss $\mathcal{L}(\mathcal{R}) \subseteq \mathcal{E}$ gelten. **qed**

Strukturelle Induktion – Natürliche Zahlen

- **Jede natürliche Zahl besitzt eine Eigenschaft E, wenn folgende Bedingungen erfüllt sind:**

  1. **Induktionsanfang**
     Die 0 besitzt die Eigenschaft E.
  2. **Induktionsschritt**
     Wenn N eine beliebige natürliche Zahl ist und die Eigenschaft E besitzt, dann besitzt sie auch $s(N)$.

- **Beispiel** **Jede natürliche Zahl ist kleiner oder gleich ihrem Quadrat.**

Strukturelle Induktion – Zeichenreihen

- Sei Σ ein Alphabet. Jede Zeichenreihe über Σ besitzt eine Eigenschaft E, wenn folgende Bedingungen erfüllt sind:
  1. **Induktionsanfang**
     Λ besitzt die Eigenschaft E.
  2. **Induktionsschritte**
     Wenn $w \in \Sigma^*$ die Eigenschaft E besitzt und $a \in \Sigma$,
     dann besitzt auch aw die Eigenschaft E.

- **Beispiel** Sei $\Sigma = \{1, 2\}$.
  Für jede Zeichenreihe über Σ gilt: die 3 kommt in ihr nicht vor.

Strukturelle Rekursion

- **Wie können wir über Formelmengen Funktionen definieren?**
- **Satz 3.7 (Prinzip der strukturellen Rekursion)** **Sei $\mathcal{M}$ eine beliebige Menge. Weiterhin seien die folgenden Funktionen gegeben:**
  - $\mathsf{foo}_{\mathcal{R}} : \mathcal{R} \longrightarrow \mathcal{M}$,
  - $\mathsf{foo}_{\neg} : \mathcal{M} \longrightarrow \mathcal{M}$,
  - $\mathsf{foo}_{\circ} : \mathcal{M} \times \mathcal{M} \longrightarrow \mathcal{M}$ **für** $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

  Dann gibt es genau eine Funktion $\mathsf{foo} : \mathcal{L}(\mathcal{R}) \longrightarrow \mathcal{M}$, **die die folgenden Bedingungen erfüllt:**

  1. **Rekursionsanfang**
     $\mathsf{foo}(A) = \mathsf{foo}_{\mathcal{R}}(A)$ **für alle** $A \in \mathcal{R}$.
  2. **Rekursionsschritte**
     $\mathsf{foo}(\neg G) = \mathsf{foo}_{\neg}(\mathsf{foo}(G))$ **für alle** $G \in \mathcal{L}(\mathcal{R})$.
     $\mathsf{foo}((G_1 \circ G_2)) = \mathsf{foo}_{\circ}(\mathsf{foo}(G_1), \mathsf{foo}(G_2))$ **für alle** $G_1, G_2 \in \mathcal{L}(\mathcal{R})$.

Strukturelle Rekursion – Beispiel

- $\mathcal{M} = \mathbb{N}$.
- $\mathsf{foo}_{1\mathcal{R}}(A) = 0$ **für alle** $A \in \mathcal{R}$.
- $\mathsf{foo}_{1\neg}(X) = X$ **für alle** $X \in \mathcal{M}$.
- $\mathsf{foo}_{1\circ}(X, Y) = X + Y + 1$ **für alle** $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ **und alle** $X, Y \in \mathcal{M}$.
- **Somit erhalten wir:**

$$\mathsf{foo}_1(F) = \begin{cases} 0 & \text{wenn } F \text{ ein Atom ist,} \\ \mathsf{foo}_1(G) & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ \mathsf{foo}_1(G_1) + \mathsf{foo}_1(G_2) + 1 & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist.} \end{cases}$$

- foo **ist ein Funktionszeichen einer Metasprache.**

Strukturelle Rekursion – Weitere Beispiele

- $$\text{foo}_2(F) = \begin{cases} 1 & \text{wenn } F \text{ ein Atom ist,} \\ \text{foo}_2(G) & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ \text{foo}_2(G_1) + \text{foo}_2(G_2) & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist} \end{cases}$$

  zählt die Anzahl der Vorkommen von Atomen in F.

- $$\text{foo}_3(F) = \begin{cases} F & \text{wenn } F \text{ ein Atom ist,} \\ \neg\text{foo}_3(G) & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ \text{foo}_3(G_1) \circ \text{foo}_3(G_2) & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist} \end{cases}$$

  eliminiert die in F vorkommenden Klammern.

- $$\text{pos}(F) = \{\Lambda\} \cup \begin{cases} \emptyset & \text{wenn } F \text{ ein Atom ist,} \\ \{1\pi \mid \pi \in \text{pos}(G)\} & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ \{1\pi_1 \mid \pi_1 \in \text{pos}(G_1)\} \cup \{2\pi_2 \mid \pi_2 \in \text{pos}(G_2)\} & \\ & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist} \end{cases}$$

  berechnet die Menge der Positionen oder Vorkommen in F.

Strukturelle Rekursion – Natürliche Zahlen

- **Sei $\mathcal{M}$ eine beliebige Menge. Weiterhin seien die folgenden Funktionen gegeben:**
  - $\mathsf{foo}_0 : \{0\} \longrightarrow \mathcal{M}$,
  - $\mathsf{foo}_s : \mathcal{M} \longrightarrow \mathcal{M}$,

  Dann gibt es genau eine Funktion $\mathsf{foo} : \mathbb{N} \longrightarrow \mathcal{M}$,
  die die folgenden Bedingungen erfüllt:

  1. **Rekursionsanfang**
     $\mathsf{foo}(0) = \mathsf{foo}_0(0)$.
  2. **Rekursionsschritt**
     $\mathsf{foo}(s(N)) = \mathsf{foo}_s(\mathsf{foo}(N))$ **für alle** $N \in \mathbb{N}$.

- **Beispiel**

$$+2(N) = \begin{cases} s(s(0)) & \text{wenn } N = 0 \text{ ist,} \\ s(+2(N')) & \text{wenn } N \text{ von der Form } s(N') \text{ ist.} \end{cases}$$

Strukturelle Rekursion – Zeichenreihen

- **Strukturelle Rekursion**
  - **Auf die explizite Angabe von $\mathcal{M}$ und von den Funktionen $\mathsf{foo}_{\boldsymbol{X}}$ wird häufig verzichtet.**
  - **Informelle Darstellung der Rekursionssätze.**

- **Strukurelle Rekursion über Zeichenreihen** **Sei Σ ein Alphabet. Es gibt genau eine über Σ^* definierte Funktion foo, die die folgenden Bedingungen erfüllt:**

  1. **Rekursionsanfang**
     Der Wert von foo für Λ ist explizit definiert.
  2. **Rekursionsschritt**
     Der Wert von foo für $aw \in \Sigma^*$ ist ausschließlich in Abhängigkeit des Wertes von foo für w definiert.

- **Beispiel**

$$\mathsf{laenge}(w) = \begin{cases} 0 & \text{wenn } w = \Lambda \text{ ist,} \\ 1 + \mathsf{laenge}(w') & \text{wenn } w \text{ von der Form } aw' \text{ ist.} \end{cases}$$

Teilausdrücke

- Wir erinnern uns an arithmetische Ausdrücke und betrachten

$$((3 \times (18 \div 6)) + 7).$$

- Dieser Ausdruck hat die folgenden Teilausdrücke:

$$((3 \times (18 \div 6)) + 7),\ (3 \times (18 \div 6)),\ 7,\ 3,\ (18 \div 6),\ 18,\ 6.$$

- Sei T ein arithmetischer Ausdruck. Die Menge der Teilausdrücke von T ist die kleinste Menge $\mathcal{S}_T$ arithmetischer Ausdrücke, die die folgenden Bedingungen erfüllt:

  1. $T \in \mathcal{S}_T$.
  2. Wenn $(T_1 \circ T_2) \in \mathcal{S}_T$ ist,
     dann sind auch $T_1, T_2 \in \mathcal{S}_T$ für alle $\circ \in \{+,\ -,\ \times,\ \div\}$.

3.1.3 Teilformeln

- **Definition 3.8** Sei $F \in \mathcal{L}(\mathcal{R})$ eine aussagenlogische Formel.
  Die **Menge der Teilformeln** von F ist die kleinste Formelmenge $\mathcal{S}_F$, die die folgenden Bedingungen erfüllt:

  1. $F \in \mathcal{S}_F$.
  2. Wenn $\neg G \in \mathcal{S}_F$ ist, dann ist auch $G \in \mathcal{S}_F$.
  3. Wenn $(G_1 \circ G_2) \in \mathcal{S}_F$ ist, dann sind auch $G_1, G_2 \in \mathcal{S}_F$.

  Die **Menge $\mathcal{R}_F$ der in F vorkommenden Variablen** ist $\mathcal{S}_F \cap \mathcal{R}$.
  G heißt **Teilformel von F**, wenn es in $\mathcal{S}_F$ enthalten ist.

- **Beispiel** Sei $F = \neg((p_1 \rightarrow p_2) \vee p_1)$

$$\begin{array}{lcl} \mathcal{S}_F & = & \{\neg((p_1 \rightarrow p_2) \vee p_1),\ ((p_1 \rightarrow p_2) \vee p_1),\ (p_1 \rightarrow p_2),\ p_1,\ p_2\}, \\ \mathcal{R}_F & = & \{p_1, p_2\}. \end{array}$$

3.2 Semantik

- Was bedeutet $\neg((p_1 \rightarrow p_2) \vee p_1)$?
- Hier Formeln können entweder wahr oder falsch sein $\leadsto$ zweiwertige Logik.

Die Bedeutung arithmetischer Ausdrücke

- Was bedeutet $((3 \times (18 \div 6)) + 7)$?
- Der Ausdruck steht in der Regel für eine rationale Zahl: 16.
- Um diese Zahl zu berechnen wenden wir eine Auswertefunktion $\cdot^I$ an, die jedem arithmetischen Ausdruck eine rationale Zahl zuweist:

$$[((3 \times (18 \div 6)) + 7)]^I = 16.$$

- Diese Funktion können wir formal definieren.
- Beachten Sie, dass $((3 \times (18 \div 6)) + 7)$ eine Zeichenreihe ist.
- Sei $\mathcal{A}$ die Menge der arithmetischen Ausdrücke.
- Wir suchen eine Funktion $\cdot^I : \mathcal{A} \longrightarrow \mathbb{Q}$
- $\cdot^I$ kann mittels struktureller Rekursion definiert werden.

Die Struktur der rationalen Zahlen

- **Eine Struktur besteht aus einer Menge von Individuen und einer Menge darauf definierter Funktionen.**
- **Menge der Individuen: $\mathbb{Q}$.**
- **Darauf definierte zweistellige Funktionen:**
  - **Addition $+^* : \mathbb{Q}^2 \longrightarrow \mathbb{Q}$,**
  - **Subtraktion $-^* : \mathbb{Q}^2 \longrightarrow \mathbb{Q}$,**
  - **Multiplikation $\times^* : \mathbb{Q}^2 \longrightarrow \mathbb{Q}$,**
  - **Division $\div^* : \mathbb{Q} \times \mathbb{Q} \setminus \{0\} \longrightarrow \mathbb{Q}$.**
- **Beachte den Unterschied zwischen $\circ/2$ und $\circ^*/2$, $\circ \in \{+,\ -,\ \times,\ \div\}$.**

Die Bedeutung arithmetischer Ausdrücke – Fortsetzung

- Eine Interpretation der arithmetischen Ausdrücke besteht aus der Menge $\mathbb{Q}$ der rationalen Zahlen und einer Abbildung $\cdot^I : \mathcal{A} \longrightarrow \mathbb{Q}$ mit

$$[T]^I = \begin{cases} T & \text{wenn } T \in \mathbb{Q}, \\ ([T_1]^I \circ^* [T_2]^I) & \text{wenn } T \text{ von der Form } (T_1 \circ T_2) \text{ ist.} \end{cases}$$

- Somit erhalten wir

$$[((3 \times (18 \div 6)) + 7)]^I = ((3 \times^* (18 \div^* 6)) +^* 7) = 16.$$

3.2.1 Die Struktur der Wahrheitswerte

- Eine Struktur besteht aus einer Menge von Individuen und einer Menge darauf definierter Funktionen.
- Die Menge der Wahrheitswerte $\mathcal{W}$ ist die Menge $\{\top, \bot\}$.
- Einstellige Funktionen vom Typ $\mathcal{W} \to \mathcal{W}$:
  - Die Negation $\neg^*$: $\neg^*(\top) = \bot$ und $\neg^*(\bot) = \top$.
  - Die Identität.
  - Die konstanten Funktionen, die auf $\bot$ und $\top$ abbilden.
- Zweistellige Funktionen vom Typ $\mathcal{W} \times \mathcal{W} \to \mathcal{W}$:
  - Die Konjunktion $\wedge^*/2$.
  - Die Disjunktion $\vee^*/2$.
  - Die Implikation $\to^* /2$.
  - Das NAND $\uparrow^*/2$.
  - Das NOR $\downarrow^* /2$. Etc.

Die verschiedenen Funktionen über den Wahrheitswerten

		$\wedge^*$	$\vee^*$	$\rightarrow^*$	$\leftarrow^*$	$\uparrow^*$	$\downarrow^*$	$\not\rightarrow^*$	$\not\leftarrow^*$
$\top$	$\top$	$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\top$	$\top$	$\top$	$\top$	$\bot$	$\bot$

		$\leftrightarrow^*$	$\not\leftrightarrow^*$	$\prod^*$	$\coprod^*$	$\swarrow^*$	$\not\swarrow^*$	$\searrow^*$	$\not\searrow^*$
$\top$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\top$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\bot$	$\bot$	$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$	$\bot$	$\top$	$\bot$	$\bot$	$\top$	$\bot$	$\top$

▷ **Hier** Negation, Konjunktion, Disjunktion, Implikation, Äquivalenz.

3.2.2 Interpretationen

- **Definition 3.9** Eine (aussagenlogische) **Interpretation** $I = (\mathcal{W}, \cdot^I)$ besteht aus der Menge $\mathcal{W}$ der Wahrheitswerte und einer Abbildung $\cdot^I : \mathcal{L}(\mathcal{R}) \rightarrow \mathcal{W}$, welche die folgenden Bedingungen erfüllt:

$$[F]^I = \begin{cases} \neg^*[G]^I & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ ([G_1]^I \circ^* [G_2]^I) & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist.} \end{cases}$$

- **Notation** I (evtl. indiziert) bezeichnet eine Interpretation.

Abbildungen und Interpretationen

- **Proposition 3.10** **Für jede Abbildung $\mathrm{g} : \mathcal{R} \longrightarrow \mathcal{W}$ gibt es genau eine Interpretation $I = (\mathcal{W}, \cdot^I)$, so dass für alle $A \in \mathcal{R}$ gilt: $\mathrm{g}(A) = [A]^I$.**
- **Beweis** **Sei $\mathrm{g} : \mathcal{R} \longrightarrow \mathcal{W}$ gegeben.**
  - **Wir konstruieren:**

$$[F]^I = \begin{cases} \mathrm{g}(F) & \text{wenn } F \in \mathcal{R}, \\ \neg^*[G]^I & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ ([G_1]^I \circ^* [G_2]^I) & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist.} \end{cases}$$

  - **Nach Konstruktion gilt für alle $A \in \mathcal{R}$: $\mathrm{g}(A) = [A]^I$.**
  - **Nach Satz 3.7 ist $I = (\mathcal{W}, \cdot^I)$ eindeutig bestimmt und bildet alle $F \in \mathcal{L}(\mathcal{R})$ auf einen Wahrheitswert ab.**
  - **Folglich ist I eine Interpretation.** qed

Interpretationen und Variablen

- **Proposition 3.11** Sei $F \in \mathcal{L}(\mathcal{R})$
  und seien $I = (\mathcal{W}, \cdot^I)$ und $I' = (\mathcal{W}, \cdot^{I'})$ Interpretationen.
  Wenn für alle $A \in \mathcal{R}_F$ gilt: $[A]^I = [A]^{I'}$, dann gilt auch $[F]^I = [F]^{I'}$.
- **Beweis** $\rightsquigarrow$ Übungsaufgabe.

Notation

- Wir können eine Interpretation $I = (\mathcal{W}, \cdot^I)$ mit $\{A \mid [A]^I = \top\}$ identifizieren.
- **Beispiel** Sei $\mathcal{R} = \{p_i \mid i \in \mathbb{N}\}$ und $I = \{p_2, p_3, p_5\}$. Dann gilt:

$$[p_i]^I = \begin{cases} \top & \text{wenn } i \in \{2, 3, 5\}, \\ \bot & \text{sonst.} \end{cases}$$

- Wir schreiben häufig F^I anstelle von $[F]^I$.

Erfüllbarkeit von Formeln

- **Definition 3.12** Sei F eine aussagenlogische Formel.
  - F heißt erfüllbar,
    wenn es eine Interpretation $I = (\mathcal{W}, \cdot^I)$ mit $F^I = \top$ gibt.
  - F heißt allgemeingültig (oder F ist eine Tautologie),
    wenn für alle Interpretationen $I = (\mathcal{W}, \cdot^I)$ gilt: $F^I = \top$.
  - F heißt widerlegbar,
    wenn es eine Interpretation $I = (\mathcal{W}, \cdot^I)$ mit $F^I = \bot$ gibt.
  - F heißt unerfüllbar,
    wenn für alle Interpretationen $I = (\mathcal{W}, \cdot^I)$ gilt: $F^I = \bot$.

3.2.3 Wahrheitswertetabellen

- Wie können wir den Wert einer Formel F unter allen möglichen Interpretationen berechnen?
- Anlegen einer Wahrheitswertetabelle:

1. Sei $m = |\mathcal{S}_F|$ die Anzahl der Teilformeln von F.
2. Sei $n = |\mathcal{R}_F|$ die Anzahl der aussagenlogischen Variablen, die in F vorkommen.
3. Lege eine Tabelle mit 2^n Zeilen und m Spalten an, wobei die ersten n Spalten mit den n in F vorkommenden aussagenlogischen Variablen, die letzte Spalte mit F und die restlichen Spalten mit den verbliebenen Teilformeln von F markiert werden.
4. Fülle die ersten n Spalten mit $\top$ und $\bot$ wie folgt aus: In der ersten Spalte stehen abwechselnd $\top\bot\top\bot\ldots$, in der zweiten Spalte stehen abwechselnd $\top\top\bot\bot\ldots$, in der dritten Spalte stehen abwechselnd $\top\top\top\top\bot\bot\bot\bot\ldots$, usw.
5. Berechne die Werte in den restlichen Spalten unter Verwendung der bekannten Funktionen über der Menge der Wahrheitswerte.

Arbeiten mit einer Wahrheitswertetabelle

- Sei F eine Formel und $T(F)$ eine dazugehörige Wahrheitswertetabelle.
  Dann gilt:
  - F ist erfüllbar gdw. $T(F)$ enhält eine Zeile mit $\top$ in der letzten Spalte.
  - F ist allgemeingültig gdw. in allen Zeilen in $T(F)$ steht $\top$ in der letzten Spalte.
  - F ist widerlegbar gdw. $T(F)$ enhält eine Zeile mit $\perp$ in der letzten Spalte.
  - F ist unerfüllbar gdw. in allen Zeilen in $T(F)$ steht $\perp$ in der letzten Spalte.

3.2.4 Modelle

- **Definition 3.13** Eine Interpretation $I = (\mathcal{W}, \cdot^I)$ heißt **Modell** für eine aussagenlogische Formel F, symbolisch $I \models F$, wenn $F^I = \top$.
- **Abkürzungen**
  - Wenn die Interpretation I kein Modell für die Formel F ist, d.h., wenn $F^I = \bot$ ist, dann schreiben wir $I \not\models F$.
  - Wenn F allgemeingültig ist, dann schreiben wir $\models F$.

Allgemeingültigkeit und Unerfüllbarkeit

- **Satz 3.14** Eine Formel F ist allgemeingültig ($\models F$) gdw. $\neg F$ ist unerfüllbar.
- **Beweis** $\models F$ gdw. alle Interpretationen sind Modelle für F
  gdw. keine Interpretation ist Modell für $\neg F$
  gdw. $\neg F$ ist unerfüllbar. qed

Erfüllbarkeit einer Menge von Formeln

- **Definition 3.15** Sei $\mathcal{G}$ eine Menge von Formeln.
  - Eine Interpretation I heißt **Modell** für $\mathcal{G}$, symbolisch $I \models \mathcal{G}$, wenn I Modell für alle $F \in \mathcal{G}$ ist.
  - $\mathcal{G}$ ist **erfüllbar**, wenn es ein Modell für $\mathcal{G}$ gibt.
  - $\mathcal{G}$ ist **unerfüllbar**, wenn es kein Modell für $\mathcal{G}$ gibt.
  - $\mathcal{G}$ ist **widerlegbar**, wenn es eine Interpretation gibt, die kein Modell für $\mathcal{G}$ ist.
  - $\mathcal{G}$ ist **allgemeingültig**, wenn alle Interpretationen auch Modelle für $\mathcal{G}$ sind.

3.2.5 Logische Konsequenzen

- **Definition 3.16** Eine aussagenlogische Formel F ist genau dann eine (aussagen-) logische Konsequenz einer Menge von Formeln $\mathcal{G}$, symbolisch $\mathcal{G} \models F$, wenn für jede Interpretation $I = (\mathcal{W}, \cdot^I)$ gilt: wenn I Modell für $\mathcal{G}$ ist, dann ist I auch Modell für F.
- **Beispiele**
  - Gilt $\{p, (p \rightarrow q)\} \models q$?
  - Gilt $\{(p \vee q)\} \models q$?
  - Gilt $\{(p \wedge \neg p)\} \models q$?
- **Satz 3.17** Seien $F,\ F_1,\ \ldots,\ F_n$ aussagenlogische Formeln. $\{F_1,\ \ldots,\ F_n\} \models F$ gdw. $\models ((\ldots(F_1 \wedge F_2) \wedge \ldots \wedge F_n) \rightarrow F)$.
- **Beweis** $\rightsquigarrow$ Übungsaufgabe.

3.3 Äquivalenz und Normalformen

3.3.1 Semantische Äquivalenz

- **Definition 3.18** Zwei aussagenlogische Formeln F und G heißen **semantisch äquivalent**, symbolisch $F \equiv G$, wenn für alle Interpretationen I gilt: $I \models F$ gdw. $I \models G$.
- **Beachte** $\equiv$ ist eine Äquivalenzrelation:
  - $\equiv$ ist reflexiv: $F \equiv F$.
  - $\equiv$ ist symmetrisch: Wenn $F \equiv G$, dann $G \equiv F$.
  - $\equiv$ ist transitiv: Wenn $F \equiv G$ und $G \equiv H$, dann $F \equiv H$.

  Die Aussagen folgen unmittelbar aus Definition 3.18 $\leadsto$ Übungsaufgabe.

Bekannte semantische Äquivalenzen

- **Satz 3.19** Seien F, G und H aussagenlogische Formeln.
  Es gelten die folgenden Äquivalenzen:

$(F \wedge F)$	$\equiv$	F	
$(F \vee F)$	$\equiv$	F	Idempotenz
$(F \wedge G)$	$\equiv$	$(G \wedge F)$	
$(F \vee G)$	$\equiv$	$(G \vee F)$	Kommutativität
$((F \wedge G) \wedge H)$	$\equiv$	$(F \wedge (G \wedge H))$	
$((F \vee G) \vee H)$	$\equiv$	$(F \vee (G \vee H))$	Assoziativität
$((F \wedge G) \vee F)$	$\equiv$	F	
$((F \vee G) \wedge F)$	$\equiv$	F	Absorption
$(F \wedge (G \vee H))$	$\equiv$	$((F \wedge G) \vee (F \wedge H))$	
$(F \vee (G \wedge H))$	$\equiv$	$((F \vee G) \wedge (F \vee H))$	Distributivität

Satz 3.19 (Fortsetzung)

- **Es gelten die folgenden Äquivalenzen:**

$\neg\neg F$	$\equiv$	F	**Doppelte Negation**
$\neg(F \wedge G)$	$\equiv$	$(\neg F \vee \neg G)$	
$\neg(F \vee G)$	$\equiv$	$(\neg F \wedge \neg G)$	**de Morgan**
$(F \vee G)$	$\equiv$	F, **wenn** F **allgemeingültig**	
$(F \wedge G)$	$\equiv$	G, **wenn** F **allgemeingültig**	**Tautologie**
$(F \vee G)$	$\equiv$	G, **wenn** F **unerfüllbar**	
$(F \wedge G)$	$\equiv$	F, **wenn** F **unerfüllbar**	**Unerfüllbarkeit**
$(F \leftrightarrow G)$	$\equiv$	$((F \wedge G) \vee (\neg G \wedge \neg F))$	**Äquivalenz**
$(F \rightarrow G)$	$\equiv$	$(\neg F \vee G)$	**Implikation**

- **Beweis** $\rightsquigarrow$ **Übungsaufgabe.**

Positionen

- **Wir erinnern uns:**

$$\text{pos}(F) = \{\Lambda\} \cup \begin{cases} \emptyset & \text{wenn } F \text{ ein Atom ist,} \\ \{1\pi \mid \pi \in \text{pos}(G)\} & \text{wenn } F \text{ von der Form } \neg G \text{ ist,} \\ \{1\pi_1 \mid \pi_1 \in \text{pos}(G_1)\} \cup \{2\pi_2 \mid \pi_2 \in \text{pos}(G_2)\} & \\ & \text{wenn } F \text{ von der Form } (G_1 \circ G_2) \text{ ist.} \end{cases}$$

- **Definition 3.20** **Sei F eine Formel.**
  Die Menge der Positionen in F, symbolisch $\mathcal{P}_F$, ist $\text{pos}(F)$.
- **Positionen sind Zeichenreihen über $\{1, 2\}$.**

Teilformeln und Ersetzungen

- **Definition 3.21** Die Teilformel von F an der Position $\pi \in \mathcal{P}_F$, symbolisch $F\lceil \pi \rceil$, ist wie folgt definiert:
  1. $F\lceil \Lambda \rceil = F$.
  2. $F\lceil 1\pi \rceil = G\lceil \pi \rceil$, wenn F von der Form $\neg G$ ist.
  3. $F\lceil i\pi \rceil = G_i\lceil \pi \rceil$, wenn F von der Form $(G_1 \circ G_2)$ und $i \in \{1, 2\}$ ist.
- **Definition 3.22** Die Ersetzung der Teilformel von F an der Position $\pi \in \mathcal{P}_F$ durch H, symbolisch $F\lceil \pi \mapsto H \rceil$, ist wie folgt definiert:
  1. $F\lceil \Lambda \mapsto H \rceil = H$,
  2. $F\lceil 1\pi \mapsto H \rceil = \neg(G\lceil \pi \mapsto H \rceil)$, wenn F von der Form $\neg G$ ist.
  3. $F\lceil 1\pi \mapsto H \rceil = (G_1\lceil \pi \mapsto H \rceil \circ G_2)$, wenn F vdF $(G_1 \circ G_2)$ ist.
  4. $F\lceil 2\pi \mapsto H \rceil = (G_1 \circ G_2\lceil \pi \mapsto H \rceil)$, wenn F vdF $(G_1 \circ G_2)$ ist.

Das Ersetzungstheorem

- **Satz 3.23** Sei $F, H, G \in \mathcal{L}(\mathcal{R})$, $\pi \in \mathcal{P}_F$, $F\lceil\pi\rceil = G$ und $G \equiv H$.
  Dann gilt: $F \equiv F\lceil\pi \mapsto H\rceil$.
- **Beweis** Induktion über den Aufbau von π.
- **Induktionsanfang** Sei $\pi = \Lambda$.
  - $F = F\lceil\Lambda\rceil = G \equiv H = F\lceil\Lambda \mapsto H\rceil$. $\checkmark$
- **Induktionshypothese (IH)** Die Aussage gilt für π'.

Fortsetzung Beweis Ersetzungstheorem

- **Induktionsschritt** Sei $\pi = i\pi'$. Wir unterscheiden zwei Fälle:

$i = 1$ Da $\pi = 1\pi' \in \mathcal{P}_F$ muss F vdF $\neg F'$ oder $(G_1 \circ G_2)$ sein.

$\neg F'$ $F\lceil 1\pi' \mapsto H\rceil = (\neg F')\lceil 1\pi' \mapsto H\rceil = \neg(F'\lceil \pi' \mapsto H\rceil)$.

Wegen IH gilt: $F' \equiv F'\lceil \pi' \mapsto H\rceil$.

Damit gilt für alle Interpretationen I:

$$\begin{array}{lcll}
[F]^I & = & [\neg F']^I & \text{Annahme} \\
& = & \neg^*[F']^I & \text{Def } I \\
& = & \neg^*[F'\lceil \pi' \mapsto H\rceil]^I & \text{IH und Def } \equiv \\
& = & [\neg(F'\lceil \pi' \mapsto H\rceil)]^I & \text{Def } I \\
& = & [(\neg F')\lceil 1\pi' \mapsto H\rceil]^I & \text{Def Ersetzung} \\
& = & [F\lceil 1\pi' \mapsto H\rceil]^I & \text{Annahme}
\end{array}$$

Somit gilt: $F \equiv F\lceil 1\pi' \mapsto H\rceil$ $\checkmark$

$(G_1 \circ G_2)$ analog

$i = 2$ analog **qed**

Verabredung

- **Wenn $\pi \not\in \mathcal{P}_F$ dann sei $F\lceil\pi \mapsto H\rceil := F$.**
- **Sei $F\lceil\pi\rceil = G$. Wenn aus dem Kontext ersichtlich ist, welches Vorkommen der Teilformel G ersetzt werden soll, dann schreiben wir $F\lceil G \mapsto H\rceil$ anstelle von $F\lceil\pi \mapsto H\rceil$.**
- **Theorem 3.23 erlaubt alle Vorkommen der Junktoren $\leftrightarrow$ und $\longrightarrow$ zu ersetzen.**
  - **OBdA betrachten wir in der Folge nur noch Formeln über $\mathcal{R} \cup \{\neg, \wedge, \vee, (,)\}$.**

3.3.2 Negationsnormalform

- **Definition 3.24** Eine Formel F ist in **Negationsnormalform** wenn alle in F vorkommenden Negationszeichen $\neg$ unmittelbar vor aussagenlogischen Variablen stehen.
- **Proposition 3.25** Es gibt einen Algorithmus, der jede Formel in eine semantisch äquivalente Formel in Negationsnormalform transformiert.
- **Algorithmus** Gegeben F.
  Solange F nicht in Negationsnormalform ist, tue das Folgende:
  - Bestimme eine Teilformel der Form $\neg G$ von F mit $G \not\in \mathcal{R}$.
  - Wenn $\neg G = \neg\neg H$, dann ersetze $\neg G$ durch H.
  - Wenn $\neg G = \neg(G_1 \wedge G_2)$, dann ersetze $\neg G$ durch $(\neg G_1 \vee \neg G_2)$.
  - Wenn $\neg G = \neg(G_1 \vee G_2)$, dann ersetze $\neg G$ durch $(\neg G_1 \wedge \neg G_2)$.

Die Regeln des Algorithmus

- Wir wollen eine abkürzende Schreibweise für die Regeln einführen:

$$\frac{\neg\neg H}{H} \qquad \frac{\neg(G_1 \wedge G_2)}{(\neg G_1 \vee \neg G_2)} \qquad \frac{\neg(G_1 \vee G_2)}{(\neg G_1 \wedge \neg G_2)}$$

- Der Algorithmus ist (don't care) nicht deterministisch!
- Ein Beispiel:

$$\begin{array}{lcll} \neg(r \vee \neg(\neg p \wedge q)) & \equiv & (\neg r \wedge \neg\neg(\neg p \wedge q)) & \textbf{de Morgan} \\ & \equiv & (\neg r \wedge (\neg p \wedge q)) & \textbf{doppelte Negation} \end{array}$$

3.3.3 Klauselformen

- **Definition 3.26** Ein **Literal** ist eine aussagenlogische Variable (**positives Literal**) oder eine negierte aussagenlogische Variable (**negatives Literal**).
- **Notation**
  - L (möglicherweise indiziert) bezeichnet ein Literal.
  - **Verallgemeinerte Disjunktion**

$$[F_1, \ldots, F_n] = (\ldots((F_1 \vee F_2) \vee F_3) \vee \ldots \vee F_n)$$

  - **Verallgemeinerte Konjunktion**

$$\langle F_1, \ldots, F_n \rangle = (\ldots((F_1 \wedge F_2) \wedge F_3) \wedge \ldots \wedge F_n)$$

  - **Beachte** $[F] = F = \langle F \rangle$. Folglich gilt: $[F] \equiv F \equiv \langle F \rangle$.
  - $[\,]$ ist **leere verallgemeinerte Disjunktion** mit $[\,]^I = \bot$ für alle I.
  - $\langle\rangle$ ist **leere verallgemeinerte Konjunktion** mit $\langle\rangle^I = \top$ für alle I.
  - **Beachte** $(G \vee [\,]) \equiv G \equiv (G \wedge \langle\,\rangle)$.

Klauseln

- **Definition 3.27**
  - Eine **Klausel** ist eine verallgemeinerte Disjunktion $[L_1, \ldots, L_n]$, $n \geq 0$, wobei jedes L_i, $1 \leq i \leq n$, ein Literal ist.
  - Eine **duale Klausel** ist eine verallgemeinerte Konjunktion $\langle L_1, \ldots, L_n \rangle$, $n \geq 0$, wobei jedes L_i, $1 \leq i \leq n$, ein Literal ist.
  - Eine Formel ist in **konjunktiver Normalform** oder in **Klauselform**, **gdw.** sie von der Form $\langle C_1, \ldots, C_m \rangle$, $m \geq 0$, ist und jedes C_j, $1 \leq j \leq m$, eine Klausel ist.
  - Eine Formel ist in **disjunktiver Normalform** oder in **dualer Klauselform**, **gdw.** sie von der Form $[C_1, \ldots, C_m]$, $m \geq 0$, ist und jedes C_j, $1 \leq j \leq m$, eine duale Klausel ist.
- **Notation** C (möglicherweise indiziert) bezeichnet eine Klausel.

Eine Beobachtung

- Sei F eine Formel in Klauselform. Dann gilt:
  - F ist unerfüllbar wenn eine in F vorkommende Klausel unerfüllbar ist.
  - Eine Klausel ist unerfüllbar gdw. sie von der Form $[\,]$ ist.

Transformation in Klauselform

- **Satz 3.28**
  1. Es gibt einen Algorithmus, der jede Formel in eine semantisch äquivalente Formel in Klauselform transformiert.
  2. Es gibt einen Algorithmus, der jede Formel in eine semantisch äquivalente Formel in dualer Klauselform transformiert.
- **Beweis von 1**
  - Wir müssen den Algorithmus spezifizieren.
  - Wir müssen zeigen, dass der Algorithmus **korrekt** ist,
    d.h., wenn er bei gegebener Eingabe F die Ausgabe G generiert,
    dann muss G in Klauselform sein und $F \equiv G$ muss gelten.
  - Wir müssen zeigen, dass der Algorithmus **terminiert**,
    d.h., bei gegebener Eingabe F nach endlicher Zeit anhält.

Ein Algorithmus zur Transformation in Klauselform

- **Eingabe** Eine Formel F.
  Ausgabe Eine zu F semantisch äquivalente Formel in konjunktiver Normalform.
  $G := \langle [F] \rangle$. (G ist eine Konjunktion von Disjunktionen.)
  Solange G nicht in konjunktiver Normalform ist tue das Folgende:
  Wähle ein Element H aus G, das keine Klausel ist.
  Wähle ein Element K aus H, das kein Literal ist.
  Wende diejenige der folgenden Regeln an, die anwendbar ist.

$$\frac{\neg\neg D}{D} \quad \frac{(D_1 \land D_2)}{D_1 \mid D_2} \quad \frac{\neg(D_1 \land D_2)}{\neg D_1, \neg D_2} \quad \frac{(D_1 \lor D_2)}{D_1, D_2} \quad \frac{\neg(D_1 \lor D_2)}{\neg D_1 \mid \neg D_2}$$

- Eine Regel $\frac{E}{E'}$ ist **anwendbar** auf K wenn K von der Form E ist.
  Bei Anwendung wird K durch E' ersetzt.
- Eine Regel $\frac{E}{E_1 \mid E_2}$ ist **anwendbar** auf K, wenn K von der Form E ist.
  Bei Anwendung wird H durch zwei Disjunktionen ersetzt:
  Die erste erhält man aus H indem das Vorkommen von E durch E_1 ersetzt wird.
  Die zweite erhält man aus H indem das Vorkommen von E durch E_2 ersetzt wird.

Ein Beispiel und ein Lemma

- **Das Beispiel**

$$\langle[\neg(p \vee (\neg(p \wedge q) \wedge \neg r))]\rangle$$
$$\langle[\neg p],\ [\neg(\neg(p \wedge q) \wedge \neg r)]\rangle$$
$$\langle[\neg p],\ [\neg\neg(p \wedge q), \neg\neg r]\rangle$$
$$\langle[\neg p],\ [(p \wedge q), \neg\neg r]\rangle$$
$$\langle[\neg p],\ [(p \wedge q),\ r]\rangle$$
$$\langle[\neg p],\ [p,\ r],\ [q,\ r]\rangle$$

- **Lemma 3.29** **Wenn G eine Konjunktion von Disjunktionen ist und G' aus G durch die Anwendung einer der im Algorithmus zur Transformation in Klauselform verwendeten Ersetzungsregel erhalten wurde, dann gilt: G' ist eine Konjunktion von Disjunktionen und $G \equiv G'$.**
- **Beweis** $\rightsquigarrow$ **Übung.**

Induktionsprinzip für Schleifen

- Eine **Schleifeninvariante** für eine Schleife W ist eine Aussage E mit der folgenden Eigenschaft: Wenn E wahr ist, dann ist E auch nach dem einmaligen Ausführen des Rumpfes von W wahr.
- **Satz 3.30 (Induktionsprinzip für Schleifen)** Wenn E vor dem Eintritt in eine Schleife W wahr und eine Schleifeninvariante für W ist, dann ist E auch nach Verlassen von W wahr (so W verlassen wird).
- **Beweis** siehe z.B. Gumm und Sommer: Einführung in die Informatik, Oldenburg Verlag (1998).

Korrektheit des Algorithmus

- Sei F die gegebene Formel und sei E die folgende Aussage:
  G ist eine Konjunktion von Disjunktionen und es gilt $F \equiv G$.
  - Der Algorithmus definiert G anfangs als $\langle [F] \rangle$.
  - Da $F \equiv \langle [F] \rangle$ gilt, ist E vor Eintritt in die Schleife wahr.
  - Lemma 3.29 sagt aus,
    dass E eine Invariante für die Schleife des Algorithmus ist.
  - Nach Satz 3.30 gilt E auch nach Verlassen der Schleife.
  - Die Schleife wird nur verlassen, wenn G in konjunktiver Normalform ist.
  - $\leadsto$ Der Algorithmus ist korrekt!

Terminierung des Algorithmus

- **Wann terminiert ein nicht deterministischer Algorithmus?**
  - **Schwache Terminierung** **es gibt mindestens eine Art, den Algorithmus auszuführen, die zur Terminierung des Algorithmus führt.**
  - **Starke Terminierung** **der Algorithmus terminiert unabhängig davon, welche Wahl wir bei den nicht deterministischen Entscheidungen treffen.**
- **Definition 3.31** **Die Funktion rng, Rang einer Formel genannt, bildet jede aussagenlogische Formel $H \in \mathcal{L}(\mathcal{R})$ auf eine natürliche Zahl wie folgt ab:**

$$
\mathsf{rng}(H) = \begin{cases} 0 & \text{wenn } H \text{ ein Literal ist,} \\ \mathsf{rng}(F) + 1 & \text{wenn } H \text{ von der Form } \neg\neg F \text{ ist,} \\ \mathsf{rng}(F) + \mathsf{rng}(G) + 1 & \text{wenn } H \text{ von der Form } (F \land G) \\ & \text{oder } (F \lor G) \text{ ist,} \\ \mathsf{rng}(\neg F) + \mathsf{rng}(\neg G) + 1 & \text{wenn } H \text{ von der Form } \neg(F \land G) \\ & \text{oder } \neg(F \lor G) \text{ ist.} \end{cases}
$$

Multimengen

- Eine **Multimenge** ist vergleichbar zu einer Menge, aber die einzelnen Elemente dürfen mehrfach in einer Multimenge vorkommen.
- **Hier** Multimengen natürlicher Zahlen:
  - $\dot{\{}1, 1, 2, 2, 2, 3\dot{\}}$.
  - $M_1 \succ M_2$ gilt **gdw** M_2 geht aus M_1 hervor, indem eine Zahl n aus M_1 gestrichen und durch eine endliche Anzahl von Zahlen, die alle kleiner als n sind, ersetzt wird.
  - $\dot{\{}1, 1, 2, 2, 2, 3\dot{\}} \succ \dot{\{}1, 1, 1, 1, 2, 2, 2, 2\dot{\}}$.
  - $\succ$ ist nicht transitiv und damit keine Ordnungsrelation!
  - **Beobachtung** Über endlichen Multimengen natürlicher Zahlen gibt es keine unendlich lange Folge $(M_i \mid i \geq 0)$ mit $M_1 \succ M_2 \succ \ldots$.
    Beweis siehe: Dershowitz, Manna: Proving Termination with Multiset Orderings, Communications of the ACM 22, 465-475 (1979).

Beweis der Terminierung

- Sei $G = \langle [H_{11}, \ldots, H_{1n_1}], \ldots, [H_{m1}, \ldots, H_{mn_m}] \rangle$. Wir definieren:

$$\mathsf{f}(G) \;=\; \dot{\{} \sum_{j=1}^{n_1} \mathsf{rng}(H_{1j}), \ldots, \sum_{j=1}^{n_m} \mathsf{rng}(H_{mj}) \dot{\}}$$

- **Beobachtung** Bei jedem Schleifendurchlauf werden die assoziierten Multimengen kleiner bzgl. $\succ/2$ (Beweis $\leadsto$ Übungsaufgabe) $\leadsto$ Terminierung. qed

$$\begin{array}{lr}
\langle [\neg(p \vee (\neg(p \wedge q) \wedge \neg r))] \rangle & \dot{\{}5\dot{\}} \\
\langle [\neg p],\; [\neg(\neg(p \wedge q) \wedge \neg r)] \rangle & \dot{\{}0, 4\dot{\}} \\
\langle [\neg p],\; [\neg\neg(p \wedge q), \neg\neg r] \rangle & \dot{\{}0, 3\dot{\}} \\
\langle [\neg p],\; [(p \wedge q), \neg\neg r] \rangle & \dot{\{}0, 2\dot{\}} \\
\langle [\neg p],\; [(p \wedge q),\; r] \rangle & \dot{\{}0, 1\dot{\}} \\
\langle [\neg p],\; [p,\; r],\; [q,\; r] \rangle & \dot{\{}0, 0, 0\dot{\}}
\end{array}$$

- **Beobachtung** Wenn G in Klauselform, dann $\mathsf{f}(G) = \dot{\{}0, \ldots, 0\dot{\}}$ und und die Anzahl der Vorkommen von Klauseln in G ist identisch zu der Anzahl der Vorkommen von 0 in $\mathsf{f}(G)$.

3.4 Beweisverfahren

- $\{F_1, \ldots, F_n\} \models F$
  gdw. $(\langle F_1, \ldots, F_n\rangle \rightarrow F)$ ist allgemeingültig
  gdw. $\neg(\langle F_1, \ldots, F_n\rangle \rightarrow F)$ unerfüllbar
  gdw. $\langle F_1, \ldots, F_n, \neg F\rangle$ unerfüllbar.
- bisher Wahrheitswertetabelle
- 3.4.1 Resolution
  3.4.2 Semantische Tableaus
  3.4.3 Der Kalkül des natürlichen Schließens
  3.4.4 Weitere Beweisverfahren und Kalküle
  - Hilbert Systeme
  - Sequenzenkalkül
  - Konnektionsmethode
  - Davis-Putnam-Logemann-Loveland-Verfahren

3.4.1 Resolution

- Resolution ist ein Verfahren zum Nachweis der Unerfüllbarkeit beliebiger Formeln.
- hier Formeln in Klauselform.
- Eine Formel in Klauselform ist unerfüllbar, wenn
  - sie die leere Klausel enthält
  - oder in eine semantische äquivalente Formel umgeformt werden kann, die die leere Klausel enthält.
- Resolution ist Suche nach der leeren Klausel unter Verwendung einer geeigneten Ableitungsregel.

Ein Beispiel

- **Einige Fakten**

  K_1 Wenn es heiß und schwül ist, dann wird es regnen.
  K_2 Wenn es schwül ist, dann ist es heiß.
  K_3 Es ist jetzt schwül.

- **Frage**

  K_4 Wird es regnen?

- **Wir führen die folgenden aussagenlogischen Variablen ein**

  p es ist heiß
  q es ist schwül
  r es wird regnen.

- **Formalisierung**

  F_1 $((p \wedge q) \longrightarrow r)$
  F_2 $(q \longrightarrow p)$
  F_3 q
  F_4 r

Fortsetzung des Beispiels

$$\{((p \land q) \to r),\ (q \to p),\ q\} \models r$$

gdw

$(\langle((p \land q) \to r),\ (q \to p),\ q\rangle \to r)$ ist allgemeingültig

gdw

$\neg(\langle((p \land q) \to r),\ (q \to p),\ q\rangle \to r)$ ist unerfüllbar

gdw

$\neg(\neg\langle(\neg(p \land q) \lor r),\ (\neg q \lor p),\ q\rangle \lor r)$ ist unerfüllbar

gdw

$(\neg\neg\langle(\neg(p \land q) \lor r),\ (\neg q \lor p),\ q\rangle \land \neg r)$ ist unerfüllbar

gdw

$(\langle(\neg(p \land q) \lor r),\ (\neg q \lor p),\ q\rangle \land \neg r)$ ist unerfüllbar

gdw

$\langle[\neg(p \land q) \lor r],\ [\neg q \lor p],\ [q],\ [\neg r]\rangle$ ist unerfüllbar

gdw

$\langle[\neg(p \land q),\ r],\ [\neg q,\ p],\ [q],\ [\neg r]\rangle$ ist unerfüllbar

gdw

$\langle[\neg p, \neg q, r],\ [\neg q, p],\ [q],\ [\neg r]\rangle$ ist unerfüllbar

Wie können wir Unerfüllbarkeit nachweisen?

- **Wir erinnern uns**

$$\langle [\neg p, \neg q, r],\ [\neg q, p],\ [q],\ [\neg r] \rangle$$

- **Beobachtung**

$$\{[\neg p,\ \neg q, r],\ [q]\} \models [\neg p, r]$$

- **Folglich**

$$\langle [\neg p, \neg q, r],\ [\neg q, p],\ [q],\ [\neg r] \rangle \equiv \langle [\neg p, \neg q, r],\ [\neg q, p],\ [q],\ [\neg r],\ [\neg p, r] \rangle$$

Die Resolutionsregel

- **Definition 3.32** Sei C_1 eine Klausel, in der das Atom A als Element vorkommt, und C_2 eine Klausel, in der das negierte Atom $\neg A$ als Element vorkommt. Sei C das Resultat der Ausführung der folgenden Schritte:

  1. Entferne alle Elemente der Form A aus C_1.
  2. Entferne alle Elemente der Form $\neg A$ aus C_2.
  3. Verknüpfe die so erhaltenen Klauseln disjunktiv.

  C ist durch Anwendung der (aussagenlogischen) Resolutionsregel auf C_1 und C_2 entstanden, wobei A das Atom ist, über das resolviert wurde. Wir nennen C auch die Resolvente von C_1 und C_2 bzgl. A.

- C kann die Resolvente von C_1 und C_1 sein.

Resolutionsableitungen und Resolutionswiderlegungen

- **Definition 3.33** Sei $F = \langle C_1, \ldots, C_n \rangle$ eine Formel in Klauselform.
  1. Die Folge $(C_i \mid 1 \leq i \leq n)$ ist eine Resolutionsableitung für F.
  2. Wenn $(C_i \mid 1 \leq i \leq m)$ eine Resolutionsableitung für F ist und C_{m+1} durch Anwendung der Resolutionsregel auf zwei Elemente aus $(C_i \mid 1 \leq i \leq m)$ enstanden ist, dann ist $(C_i \mid 1 \leq i \leq m+1)$ eine Resolutionsableitung für F.
  3. Eine Resolutionsableitung für F, die die leere Klausel $[\,]$ enthält heißt Resolutionswiderlegung für F.
- F kann bereits $[\,]$ enthalten.
- Es genügt Ableitungen zu betrachten in denen $[\,]$ nur einmal vorkommt.
- OBdA können wir annehmen, dass $[\,]$ die letzte Klausel in einer Ableitung ist.

Beispiel (Fortsetzung)

1	$[\neg p, \neg q, r]$	
2	$[\neg q, p]$	
3	$[q]$	
4	$[\neg r]$	
5	$[\neg q, \neg q, r]$	*res*$(1, 2)$
6	$[r]$	*res*$(3, 5)$
7	$[\,]$	*res*$(4, 6)$

Resolutionsbeweise

- **Definition 3.34** Sei F eine aussagenlogische Formel und G eine zu $\neg F$ äquivalente Formel in Klauselform. Ein **aussagenlogischer Resolutionsbeweis** für F ist eine Resolutionswiderlegung für G. F heißt **Theorem** des Resolutionskalküls, wenn es einen Resolutionsbeweis für F gibt.
  Letzteres notieren wir mit $\vdash_r F$.
- **Forderungen**
  - **Korrektheit** Wenn $\vdash_r F$, dann $\models F$.
  - **Vollständigkeit** Wenn $\models F$, dann $\vdash_r F$.
- **Beobachtung**
  - Sei F eine Formel mit n aussagenlogischen Variablen.
  - $(F \wedge (p \wedge \neg p))$ ist unerfüllbar.
  - Der Beweis besteht aus einem einzigen Resolutionsschritt!

3.4.3 Der Kalkül des natürlichen Schließens

- **Gentzen 1935: Wie können mathematische Schlüsse formalisiert werden?**
  - **Kalkül des natürlichen Schließens.**
- **Die Menge der aussagenlogischen Variablen ist $\mathcal{R}_n := \mathcal{R} \cup \{[\,]\}$.**
- $[\,]^I := \perp$ **für alle Interpretionen I.**
- **Die Sprache ist $\mathcal{L}(\mathcal{R}_n)$.**

Ein einführendes Beispiel

- Angenommmen wir wollen zeigen, dass

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

  allgemeingültig ist.

- Ein Beweis könnte wie folgt aussehen:

  Angenommen $(p \vee (q \wedge r))$ gilt. Wir unterscheiden zwei Fälle:

  (i) Angenommen p gilt.
  Dann gilt auch $(p \vee q)$.

  (ii) Angenommen $(q \wedge r)$ gilt.
  Dann gilt auch q und folglich muss auch $(p \vee q)$ gelten.

  Ergo gilt $(p \vee q)$ in jedem Fall. (1)

  Analog folgern wir, dass auch $(p \vee r)$ gelten muss. (2)

  Aus (1) und (2) folgt die Gültigkeit von $((p \vee q) \wedge (p \vee r))$.

  Wir können nun die intiale Annahme auslösen und erhalten so einen Beweis für $((p \vee (q \wedge r)) \rightarrow ((p \vee q) \wedge (p \vee r)))$.

Ableitungsregeln - Beispiele

- Elimination der Implikation

$$\frac{G \qquad (G \rightarrow F)}{F}\ (\rightarrow E)$$

- Einführung (Introduction) der Implikation

$$\frac{\begin{array}{c}\lfloor G \rfloor \\ \vdots \\ F\end{array}}{(G \rightarrow F)}\ (\rightarrow I)$$

- Schemata, die instanziiert werden müssen, z.B.,

$$\frac{(p \wedge q) \qquad ((p \wedge q) \rightarrow (q \wedge p))}{(q \wedge p)}\ (\rightarrow E)$$

Natürliches Schließen - Ableitungsregeln

- **Negation**

$$\frac{[\,]}{G}\,(f) \qquad \frac{\begin{array}{c}\lfloor \neg F \rfloor \\ \vdots \\ [\,]\end{array}}{F}\,\textit{(raa)} \qquad \frac{\begin{array}{c}\lfloor F \rfloor \\ \vdots \\ [\,]\end{array}}{\neg F}\,(\neg I) \qquad \frac{F \qquad \neg F}{[\,]}\,(\neg E)$$

- **Konjunktion**

$$\frac{F \qquad G}{(F \wedge G)}\,(\wedge I) \qquad \frac{(F \wedge G)}{F}\,(\wedge E) \qquad \frac{(F \wedge G)}{G}\,(\wedge E)$$

- **Disjunktion**

$$\frac{F}{(F \vee G)}\,(\vee I) \qquad \frac{G}{(F \vee G)}\,(\vee I) \qquad \frac{(F \vee G) \qquad \begin{array}{c}\lfloor F \rfloor \\ \vdots \\ H\end{array} \qquad \begin{array}{c}\lfloor G \rfloor \\ \vdots \\ H\end{array}}{H}\,(\vee E)$$

Natürliches Schließen - Ableitungsregeln (Fortsetzung)

- **Implikation**

$$\frac{\begin{array}{c}\lfloor G \rfloor\\ \vdots \\ F\end{array}}{(G \rightarrow F)}\ (\rightarrow I) \qquad \frac{\begin{array}{c}\lfloor \neg F \rfloor\\ \vdots \\ \neg G\end{array}}{(G \rightarrow F)}\ (\rightarrow I) \qquad \frac{G \qquad (G \rightarrow F)}{F}\ (\rightarrow E)$$

- **Äquivalenz**

$$\frac{\begin{array}{c}\lfloor G \rfloor\\ \vdots \\ F\end{array} \qquad \begin{array}{c}\lfloor F \rfloor\\ \vdots \\ G\end{array}}{(G \leftrightarrow F)}\ (\leftrightarrow I) \qquad \frac{G \qquad (G \leftrightarrow F)}{F}\ (\leftrightarrow E) \qquad \frac{F \qquad (G \leftrightarrow F)}{G}\ (\leftrightarrow E)$$

Ableitungsbäume

- Ableitungen sind endliche Bäume, wobei
  - Knoten mit Formeln markiert sind,
  - Kanten mit Ableitungsregeln markiert sind,
  - Blätter zusätzlich mit $\lfloor\ \rfloor$ und einem Index markiert sein können,
  - Kanten zusätzlich mit einem Index markiert sein können,

  und die gemäß der nachfolgenden Vorschriften konstruiert sind.
- Formeln, die Blätter markieren, werden **Hypothesen** oder **Annahmen** genannt.
  - Wenn ein Blatt mit H und $\lfloor\ \rfloor$ (kurz mit $\lfloor H \rfloor$) markiert ist,
    dann ist dieses Vorkommen von H **ausgelöst**;
    sonst ist es **nicht ausgelöst**.
  - Eine Hypothese in einem Ableitungsbaum ist **ausgelöst**,
    wenn alle ihre Vorkommen in dem Baum ausgelöst sind.
- Ein Ableitungsbaum, dessen Wurzel mit F markiert ist und
  dessen Menge nicht ausgelöster Hypothesen $\{F_1, \ldots, F_m\}$ ist, heißt
  Ableitung von F aus $\{F_1, \ldots, F_m\}$, symbolisch $\{F_1, \ldots, F_m\} \vdash_n F$.

Ableitungsbäume - Notation

- $\bigtriangledown_F$ bezeichnet einen Ableitungsbaum, dessen Wurzel mit F markiert ist.
- $\bigtriangledown_F^G$ bezeichnet einen Ableitungsbaum, dessen Wurzel mit F markiert ist und der eine nicht ausgelöste Hypothese G enthält.
- Sei j ein Index.
  $\bigtriangledown_F^{\lfloor G \rfloor^j}$ bezeichnet den Baum, den man aus $\bigtriangledown_F^G$ erhält, indem mindestens ein nicht ausgelöstes Vorkommen der Hypothese G mit $\lfloor\ \rfloor^j$ markiert wird.

Ableitungsbäume - Formale Definition (1)

- **Definition 3.38** Die Menge der **Ableitungsbäume im Kalkül des natürlichen Schließens** ist die kleinste Menge $\mathcal{X}$ mit folgenden Eigenschaften:

  1. Jeder Baum, der nur aus einem einzigen, mit einer Formel $F \in \mathcal{L}(\mathcal{R}_n)$ markiertem Knoten besteht, ist in $\mathcal{X}$.
  2. Wenn $\bigtriangledown_{H_1} \in \mathcal{X}$ und
  $$\frac{H_1}{H_2}\, r$$
  eine Instanz einer Regel $r \in \{(f),\ (\wedge E),\ (\vee I)\}$ ist, dann ist
  $$\frac{\bigtriangledown_{H_1}}{H_2}\, r$$
  ein Ableitungsbaum in $\mathcal{X}$.

Ableitungsbäume - Formale Definition (2)

3. **Wenn $\nabla^{H_1}_{H_2} \in \mathcal{X}$, j ein neuer Index und**

$$\dfrac{\begin{array}{c}\lfloor H_1 \rfloor \\ \vdots \\ H_2\end{array}}{H_3}\, r$$

eine Instanz einer Regel $r \in \{$*(raa)*, $(\neg I)$, $(\rightarrow I)\}$ ist, dann ist

$$\dfrac{\nabla^{\lfloor H_1 \rfloor^j}_{H_2}}{H_3}\, r^j$$

ein Ableitungsbaum in $\mathcal{X}$.

Ableitungsbäume - Formale Definition (3)

4. Wenn $\bigtriangledown_{H_1},\ \bigtriangledown_{H_2} \in \mathcal{X}$ und

$$\frac{H_1 \qquad H_2}{H_3}\, r$$

eine Instanz einer Regel $r \in \{(\neg E),\ (\wedge I),\ (\rightarrow E),\ (\leftrightarrow E)\}$ ist, dann ist

$$\frac{\bigtriangledown_{H_1} \qquad \bigtriangledown_{H_2}}{H_3}\, r$$

ein Ableitungsbaum in $\mathcal{X}$.

Ableitungsbäume - Formale Definition (4)

5. **Wenn $\nabla_{(F \vee G)}$, ∇_H^F, $\nabla_H^G \in \mathcal{X}$ und j ein neuer Index ist, dann ist**

$$\frac{\nabla_{(F \vee G)} \qquad \nabla_H^{\lfloor F \rfloor^j} \qquad \nabla_H^{\lfloor G \rfloor^j}}{H} \, (\vee E)^j$$

ein Ableitungsbaum in $\mathcal{X}$.

6. **Wenn ∇_F^G, $\nabla_G^F \in \mathcal{X}$ und j ein neuer Index ist, dann ist**

$$\frac{\nabla_F^{\lfloor G \rfloor^j} \qquad \nabla_G^{\lfloor F \rfloor^j}}{(G \leftrightarrow F)} \, (\leftrightarrow I)^j$$

ein Ableitungsbaum in $\mathcal{X}$.

Ableitungen und Beweise

- **Definition 3.39** Sei $\bigtriangledown_F$ ein Ableitungsbaum und $\{F_1, \ldots, F_m\}$ die Menge der in $\bigtriangledown_F$ vorkommenden, nicht ausgelösten Hypothesen. Dann heißt $\bigtriangledown_F$ **Ableitung von F aus** $\{F_1, \ldots, F_m\}$ und wir schreiben dafür $\{F_1, \ldots, F_m\} \vdash_n F$.
- **Definition 3.40** Ein **Beweis** für eine aussagenlogische Formel F **im Kalkül des natürlichen Schließens** ist eine Ableitung von F aus der leeren Mengen von Hypothesen. Statt $\emptyset \vdash_n F$ schreiben wir $\vdash_n F$, wenn F einen Beweis im Kalkül des natürlichen Schließens hat.
- **Ein einfaches Beispiel** Ein Beweis von $(p \longrightarrow p)$:

$$\frac{\lfloor p \rfloor^1}{(p \longrightarrow p)}\,(\longrightarrow I)^1$$

Das einführende Beispiel

$$
\dfrac{
\dfrac{
\lfloor(p \lor (q \land r))\rfloor^1 \quad
\dfrac{\lfloor p\rfloor^2}{(p \lor q)}\,(\lor I) \quad
\dfrac{\dfrac{\lfloor(q \land r)\rfloor^2}{q}\,(\land E)}{(p \lor q)}\,(\lor I)
}{(p \lor q)}\,(\lor E)^2
\qquad
\dfrac{
\lfloor(p \lor (q \land r))\rfloor^1 \quad
\dfrac{\lfloor p\rfloor^3}{(p \lor r)}\,(\lor I) \quad
\dfrac{\dfrac{\lfloor(q \land r)\rfloor^3}{r}\,(\land E)}{(p \lor r)}\,(\lor I)
}{(p \lor r)}\,(\lor E)^3
}{
\dfrac{((p \lor q) \land (p \lor r))}{((p \lor (q \land r)) \to ((p \lor q) \land (p \lor r)))}\,(\to I)^1
}\,(\land I)
$$

- **Bitte vergleichen Sie diesen formalen Beweis mit dem zuvor betrachteten informellen Beweis.**

Lemmata (1)

- Manche Ableitungsbäume treten immer wieder auf, z.B., $\{\neg\neg F\} \vdash_n F$ bzw.

$$\dfrac{\dfrac{\neg\neg F \qquad \lfloor\neg F\rfloor^1}{[\,]}\,(\neg E)}{F}\,(raa)^1$$

- Idee Man erzeuge eine solchen Ableitungsbaum einmal, spezifiziere eine korrespondierende Ableitungsregel, Lemma genannt, und wende das Lemma zusätzlich zu den sonstigen Ableitungsregeln an.
- Im Beispiel erhalten wir das Lemma:

$$\dfrac{\neg\neg F}{F}\,(l1)$$

Lemmata (2)

- **Das Lemma**

$$\frac{\neg(F \wedge G) \qquad F}{\neg G}\,(l2)$$

- **und sein Ableitungsbaum**

$$\dfrac{\dfrac{\neg(F \wedge G) \qquad \dfrac{F \qquad \lfloor G \rfloor^1}{(F \wedge G)}\,(\wedge I)}{[\,]}\,(\neg E)}{\neg G}\,(\neg I)^1$$

Lemmata (3)

- **Das Lemma**

$$\frac{\neg(F \wedge G) \qquad G}{\neg F}\,(l3)$$

- **und sein Ableitungsbaum**

$$\dfrac{\dfrac{\neg(F \wedge G) \qquad \dfrac{\lfloor F \rfloor^1 \qquad G}{(F \wedge G)}\,(\wedge I)}{[\,]}\,(\neg E)}{\neg F}\,(\neg I)^1$$

Lemmata (4)

- **Das Lemma**

$$\frac{\neg(F \vee G)}{(\neg F \wedge \neg G)}\,(l4)$$

- **und sein Ableitungsbaum**

$$\dfrac{\dfrac{\dfrac{\neg(F \vee G) \qquad \dfrac{\lfloor F \rfloor^{1}}{(F \vee G)}\,(\vee I)}{[\,]}\,(\neg E)}{\neg F}\,(\neg I)^{1} \qquad \dfrac{\dfrac{\neg(F \vee G) \qquad \dfrac{\lfloor G \rfloor^{2}}{(F \vee G)}\,(\vee I)}{[\,]}\,(\neg E)}{\neg G}\,(\neg I)^{2}}{(\neg F \wedge \neg G)}\,(\wedge I)$$

Ein Beispiel für die Benutzung von Lemmata

- **Ein Beweis von** $(p \vee \neg p)$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\lfloor\neg(p \vee \neg p)\rfloor^1}{(\neg p \wedge \neg\neg p)}\,(l4)}{\neg\neg p}\,(\wedge E)}{p}\,(l1) \qquad \dfrac{\dfrac{\lfloor\neg(p \vee \neg p)\rfloor^1}{(\neg p \wedge \neg\neg p)}\,(l4)}{\neg p}\,(\wedge E)}{[\,]}\,(\neg E)}{(p \vee \neg p)}\,(\textit{raa})^1
$$

Einige Bemerkungen zum natürlichen Schließen

- **Lemmatas verkürzen Beweise, vergrößern aber den Suchraum.**
- **Der Kalkül des natürlichen Schließens ist korrekt und vollständig.**
  (siehe z.B. van Dalen: Logic and Structure. Springer 1997).
- **Für einen Menschen lesbare Beweise oder mechanisch generierte Beweise.**
- **Sequenzenkalül.**
- **Beweistheorie.**

3.6 Eigenschaften

3.6.1 Der Endlichkeitssatz - Vorbemerkung

- Wie testen wir die Erfüllbarkeit einer möglicherweise unendlich großen Menge von Formeln?
- Idee Es reicht aus, alle endlichen Teilmengen zu betrachten.
- Wir erinnern uns $\equiv$ ist eine Äquivalenzrelation auf $\mathcal{L}(\mathcal{R})$.
- Sei $\mathcal{L}(\mathcal{R}, n) \subseteq \mathcal{L}(\mathcal{R})$ die Menge der aussagenlogischen Formeln, in denen höchstens die aussagenlogischen Variablen $p_1, \ldots, p_n$ vorkommen.
- Dann finden wir 2^n verschiedene Interpretationen für $\mathcal{L}(\mathcal{R}, n)$.
- Es gibt 2^{2^n} verschiedene durch $\equiv$ auf $\mathcal{L}(\mathcal{R}, n)$ definierte Äquivalenzklassen.

Der Endlichkeitssatz

- **Satz 3.45 (Endlichkeitssatz)** Eine Menge $\mathcal{G}$ von Formeln der Aussagenlogik ist genau dann erfüllbar, wenn jede endliche Teilmenge $\mathcal{H} \subseteq \mathcal{G}$ erfüllbar ist.
- **Beweis** Sei $\mathcal{G}$ eine (möglicherweise unendlich große) Menge von Formeln.

  Zu zeigen ist:

  (i) Wenn $\mathcal{G}$ erfüllbar ist, dann ist jede endliche Teilmenge $\mathcal{H} \subseteq \mathcal{G}$ erfüllbar.

  (ii) Wenn jede endliche Teilmenge $\mathcal{H} \subseteq \mathcal{G}$ erfüllbar ist, dann ist $\mathcal{G}$ erfüllbar.

  zu (i) Dies folgt unmittelbar aus der Definition der Erfüllbarkeit von Mengen.

  zu (ii) Ausgehend von den Modellen für jede endliche Teilmenge $\mathcal{H} \subseteq \mathcal{G}$ müssen wir die Existenz eines Modells für $\mathcal{G}$ nachweisen.

Beweis Fall (ii) des Endlichkeitssatzes

- Angenommen, jede endliche Teilmenge von $\mathcal{G}$ ist erfüllbar.
- Sei $\mathcal{G}_n := \mathcal{G} \cap \mathcal{L}(\mathcal{R}, n)$.
- Es gibt maximal $k \leq 2^{2^n}$ verschiedene durch $\equiv$ auf $\mathcal{G}_n$ definierte Äquivalenzklassen.
- Seien $G_1, \ldots, G_k$ Repräsentanten dieser Äquivalenzklassen.
- Somit gibt es für alle $G \in \mathcal{G}_n$ ein i, $1 \leq i \leq k$, mit $G \equiv G_i$.
- Folglich ist jedes Modell für $\{G_1, \ldots, G_k\}$ auch ein Modell für $\mathcal{G}_n$.
- Da $\{G_1, \ldots, G_k\}$ eine endliche Teilmenge von $\mathcal{G}$ ist, besitzt sie ein Modell.
- Sei I_n dieses Modell.
- Wegen $\mathcal{G}_1 \subseteq \mathcal{G}_2 \subseteq \ldots \subseteq \mathcal{G}_n$ ist I_n auch ein Modell für alle $\mathcal{G}_j$, $1 \leq j \leq n$.

Fortsetzung Beweis Fall (ii) des Endlichkeitssatzes

- Wir konstruieren ein Modell I für $\mathcal{G}$ wie folgt:

  Setze $I := \emptyset$, $K_0 := \mathbb{N}$ und $n = 1$.
  Tue das Folgende:
  Wenn es unendlich viele $j \in K_{n-1}$ mit $[p_n]^{I_j} = \top$ gibt, dann setze
  $I := I \cup \{p_n\}$ und $K_n := K_{n-1} \setminus \{j \mid [p_n]^{I_j} = \bot\}$, $\quad (\top)$
  sonst setze
  $K_n := K_{n-1} \setminus \{j \mid [p_n]^{I_j} = \top\}$. $\quad (\bot)$
  Setze $n := n + 1$.
  Gehe zu "Tue das Folgende".

- Da I jedem p_i einen Wahrheitswert zuweist ist I eine Interpretation.
- Mittels vollständiger Induktion lässt sich die folgende Aussage $E(n)$ beweisen:

  Es gibt in K_n noch unendlich viele Elemente und
  für alle $m \in K_n$ gilt: $[p_i]^{I_m} = [p_i]^I$ für alle $1 \leq i \leq n$.

  Beweis $\rightsquigarrow$ Übungsaufgabe.

Fortsetzung Beweis Fall (ii) des Endlichkeitssatzes

- Zu zeigen I ist ein Modell für $\mathcal{G}$.
- Sei F ein beliebiges, aber festes Element aus $\mathcal{G}$.
- In F können nur endlich viele aussagenlogische Variable vorkommen.
- Sei davon p_n die Variable mit dem höchsten Index.
- Dann ist $F \in \mathcal{G}_n \subseteq \mathcal{G}_{n+1} \subseteq \ldots$
  und jede Interpretation $I_n, \; I_{n+1}, \; \ldots$ ist Modell für F.
- Wegen $E(n)$ gibt es
  - noch unendlich viele Elemente in K_n und
  - für alle $m \in K_n$ gilt: $[p_i]^{I_m} = [p_i]^I$ für alle $1 \leq i \leq n$.
- Wähle $m \in K_n$ mit $m \geq n$.
- Da I_m Modell für F ist und in F nur die Variablen $p_1, \ldots, p_n$ vorkommen, muss auch I Modell für F sein.
- Da F ein beliebiges Element aus $\mathcal{G}$ ist, muss I auch Modell für $\mathcal{G}$ sein. qed

Folgerungen aus dem Endlichkeitssatz

- Der Beweis ist nicht konstruktiv.
- Wir können die linke und die rechte Seite des Endlichkeitssatzes negieren.
- Korollar 3.46 Eine Menge von Formeln der Aussagenlogik ist unerfüllbar gdw eine ihrer endlichen Teilmengen ist unerfüllbar.
- Verfahren zum Nachweis der Unerfüllbarkeit von $\mathcal{F}$:
  - Wir generieren systematisch alle endlichen Teilmengen von $\mathcal{F}$ und testen auf Unerfüllbarkeit.

3.6.2 Korrektheits- und Vollständigkeitssätze

- **Lemma 3.47 (Aussagenlogisches Resolutionslemma)** Sei $F = \langle C_1, \ldots, C_n \rangle$ eine aussagenlogische Formel in Klauselform mit den Klauseln C_i, $1 \leq i \leq n$, und sei D eine Resolvente zweier Klauseln aus F. Dann gilt $F \equiv (F \wedge D)$.
- **Beweis** Z.z.: für alle Interpretationen I gilt: $I \models (F \wedge D)$ gdw. $I \models F$.
- "$\Rightarrow$" gilt unmittelbar.

Fortsetzung Beweis des Resolutionslemmas

- "$\Leftarrow$" Es gelte $I \models F$.
  Sei D die Resolvente von C_i und C_j bzgl. A, $1 \leq i, j \leq n$.
  - Seien $C_i' = C_i$ "ohne" A und $C_j' = C_j$ "ohne" $\neg A$.
  - Dann ist $D = (C_i' \vee C_j')$.
  - **Fall 1** $I \models A$.
    Dann $I \not\models \neg A$.
    Wegen $I \models C_j$ folgt dann $I \models C_j'$.
    Somit $I \models D$.
  - **Fall 2** $I \not\models A$.
    Wegen $I \models C_i$ folgt dann $I \models C_i'$.
    Somit $I \models D$.

qed

Eine Folgerung aus dem Resolutionslemma

- **Korollar 3.48** Sei $F = \langle C_1, \ldots, C_n \rangle$ eine aussagenlogische Formel in Klauselform mit den Klauseln C_i, $1 \leq i \leq n$, und seien $D_1, \ldots, D_m$ die in einer Resolutionsableitung von F berechneten Resolventen. Dann gilt: $F \equiv \langle F, D_1, \ldots, D_m \rangle$.
- **Beweis** Induktion über m $\leadsto$ Übungsaufgabe.

Resolutionsverfahren

- **Satz 3.49**
  (Korrektheit und Vollständigkeit des aussagenlog. Resolutionsverfahrens)
  Sei F eine aussagenlogische Formel. $\models F$ gdw. $\vdash_r F$.
- **Beweis Korrektheit Z.z: Wenn $\vdash_r F$, dann $\models F$.**
  - **Es sei $\vdash_r F$.**
  - **Nach Satz 3.28 gibt es eine zu $\neg F$ semantisch äquivalente Formel G in Klauselform.**
  - **Nach Definition 3.34 finden wir eine Resolutionswiderlegung für G, d.h., nach Definition 3.33 eine Resolutionsableitung für G mit leerer Klausel $[\,]$ als letzte Zeile.**
  - **Seien nun $D_1, \ldots, D_m, [\,]$ alle in der Ableitung berechneten Resolventen.**
  - **Nach Korollar 3.48 gilt: $G \equiv \langle G, D_1, \ldots, D_m, [\,] \rangle$.**
  - **Da $[\,]$ unerfüllbar ist, folgt wegen Satz 3.19 $G \equiv [\,]$, d.h., G ist unerfüllbar.**
  - **Wegen $G \equiv \neg F$ und Satz 3.14 gilt somit $\models F$.**

Vollständigkeit des Resolutionsverfahrens

- **Beweis Vollständigkeit Z.z.: Wenn $\models F$, dann $\vdash_r F$.**
  - **Es gelte $\models F$.**
  - **Nach Satz 3.28 finden wir eine Formel G in Klauselform mit $G \equiv \neg F$.**
  - **Nach Satz 3.14 ist $\neg F$ und folglich auch G unerfüllbar.**
  - **Z.z. es gibt Resolutionswiderlegung für G**
  - **Beweis mittels Induktion über die Anzahl n der in G vorkommenden aussagenlogischen Variablen.**
- **Induktionsanfang ($n = 0$) Dann $G = \langle [\,], \ldots, [\,] \rangle$ und wir sind fertig.**
- **Induktionshypothese Die Aussage gelte für n, d.h., wenn G unerfüllbar ist und in G nur n verschiedene aussagenlogischen Variablen vorkommen, dann gibt es eine Resolutionswiderlegung für G.**
  - **OBdA dürfen wir annehmen, dass $p_1, \ldots, p_n$ die n in G vorkommenden Variablen sind $\rightsquigarrow$ Übungsaufgabe.**

Vollständigkeit – Induktionsschritt

- **Induktionsschritt** Sei G' eine Formel in Klauselform, in der die Variablen $p_1, \ldots, p_{n+1}$ vorkommen.
  - $G'_\top$ entstehe aus G' indem
    - jede Klausel, in der p_{n+1} vorkommt, gestrichen wird,
    - und jedes Vorkommen von $\neg p_{n+1}$ in den Klauseln gestrichen wird.
  - $G'_\bot$ entstehe aus G' indem
    - jede Klausel, in der $\neg p_{n+1}$ vorkommt, gestrichen wird
    - und jedes Vorkommen von p_{n+1} in den Klauseln gestrichen wird.
  - Es gilt: $G'_\top$ und $G'_\bot$ sind unerfüllbar, wenn G' unerfüllbar ist $\rightsquigarrow$ **Übungsaufgabe**.

Vollständigkeit – Induktionsschritt (Fortsetzung)

- Nach Induktionsvoraussetzung finden wir Resolutionswiderlegungen für $G'_\perp$ und $G'_\top$.
- Resolventen $G'_\top$ $\rightsquigarrow$ Resolventen G'.
  - $\rightsquigarrow$ **1. Fall** Resolutionswiderlegung für G'.
  - $\rightsquigarrow$ **2. Fall** Resolutionsableitung mit $[\neg p_{n+1}, \ldots \neg p_{n+1}]$ als letzter Zeile.
- Resolventen $G'_\perp$ $\rightsquigarrow$ Resolventen G'.
  - $\rightsquigarrow$ **1. Fall** Resolutionswiderlegung für G'.
  - $\rightsquigarrow$ **2. Fall** Resolutionsableitung mit $[p_{n+1}, \ldots, p_{n+1}]$ als letzter Zeile.
- Wenn jeweils der 2. Fall eingetreten ist, dann resolviere $[p_{n+1}, \ldots, p_{n+1}]$ mit $[\neg p_{n+1}, \ldots, \neg p_{n+1}]$ $\rightsquigarrow$ Resolutionswiderlegung für G'.

► Eine Anwendung des Induktionsprinzips liefert das gewünschte Ergebnis. **qed**