Karlsruher Institut für Technologie

Grundbegriffe der Informatik

Kapitel 5: Aussagenlogik

Mattias Ulbrich
(basierend auf Folien von Thomas Worsch)

KIT · Institut für Theoretische Informatik

Wintersemester 2023/2024

Themen dieses Kapitels

Karlsruher Institut für Technologie

informellen Anmerkungen	nach ein paar einleitenden zu Aussagen und ihrer Gültigkeit
Syntax	definieren wir die aussagenlogischer Formeln.
Boolesche Funktionen	ermöglichen dann die
Semantik	Definition der aussagenlogischer Formeln.
Beweisbarkeit	Im Abschnitt über geht es um ein syntaktisches Äquivalent zum semantischen Begriff der Allgemeingültigkeit.

Wo sind wir?

Informelles

Syntax aussagenlogischer Formeln

Semantik aussagenlogischer Formeln

Boolesche Funktionen

Beweisbarkeit

Beweisen auf der Metaebene

User Ziel: Formales Logisches Schließen

$R \vee S \rightarrow K$

- **Unter der Annahme, dass gilt:**
  «Wenn es regnet oder schneit, dann ist es kalt draußen.»

$\neg K$

- **Für die Beobachtung:**
  «Es ist warm draußen.»

$\Longrightarrow \quad \neg R$

- **Daraus kann man schließen:**
  «Es regnet nicht.»

Aussagen — «objektiv» wahr oder falsch

- Beispielaussagen
  - «Die Zahl 42 ist gerade.»
  - «Die Zahl 43 ist gerade.»

Aussagen — «objektiv» wahr oder falsch

- Beispielaussagen
  - «Die Zahl 42 ist gerade.» **wahr**
  - «Die Zahl 43 ist gerade.»

Aussagen — «objektiv» wahr oder falsch

- Beispielaussagen
  - «Die Zahl 42 ist gerade.» **wahr**
  - «Die Zahl 43 ist gerade.» **falsch**

Aussagen — «objektiv» wahr oder falsch

- Beispielaussagen
  - «Die Zahl 42 ist gerade.» **wahr**
  - «Die Zahl 43 ist gerade.» **falsch**

- hängt i.A. von einem *Interpretations*-Kontekt ab:
  «Es regnet.» ist weder immer wahr noch immer falsch.

Aussagen — «objektiv» wahr oder falsch

- Beispielaussagen
  - «Die Zahl 42 ist gerade.» **wahr**
  - «Die Zahl 43 ist gerade.» **falsch**

- hängt i.A. von einem *Interpretation*s-Kontekt ab:
  «Es regnet.» ist weder immer wahr noch immer falsch.

- Das Folgende scheint eine Aussage, ist aber keine Aussage, da weder wahr noch falsch
  - «Dieser Satz ist *nicht* wahr.»
  - Ist der Satz wahr, dann ist er nicht wahr.
  - Ist der Satz nicht wahr, dann ist er wahr.

Aussagen aus elementaren Aussagen zusammensetzen

- Es seien P und Q zwei Aussagen.
- Dann erlauben wir diese Konstruktionen:
  - **Negation:** «Nicht P»
  - **logisches Und:** «P und Q»
  - **logisches Oder:** «P oder Q»
  - **logische Folgerung:** «P impliziert Q»
    «Wenn P, dann Q»

Grundlagen der klassischen Aussagenlogik

- Zweiwertigkeit
  Jede Aussage ist entweder falsch oder wahr.
- Elementare Aussagen haben keine weitere Unterstruktur.
- Wahrheitswert zusammengesetzter Aussagen
  durch Wahrheitswerte der Teilaussagen
  eindeutig festgelegt
  - *keine* Abhängigkeit vom konkreten Inhalt der Aussagen
  - auch nicht beim «Wenn …, dann …»

Grundlagen der klassischen Aussagenlogik

- Zweiwertigkeit
  Jede Aussage ist entweder falsch oder wahr.
- Elementare Aussagen haben keine weitere Unterstruktur.
- Wahrheitswert zusammengesetzter Aussagen
  durch Wahrheitswerte der Teilaussagen
  eindeutig festgelegt
  - *keine* Abhängigkeit vom konkreten Inhalt der Aussagen
  - auch nicht beim «Wenn …, dann …»
- Beispiel
  - P: *«2014 in Japan etwa 4.7 Mio. Pkw neu zugelassen.»*
  - Q: *«1999 gab es in Deutschland etwa 11.2 Mio. Internet-Nutzer»*
  - «Wenn P, dann Q»

Grundlagen der klassischen Aussagenlogik

- Zweiwertigkeit
  Jede Aussage ist entweder falsch oder wahr.
- Elementare Aussagen haben keine weitere Unterstruktur.
- Wahrheitswert zusammengesetzter Aussagen
  durch Wahrheitswerte der Teilaussagen
  eindeutig festgelegt
  - *keine* Abhängigkeit vom konkreten Inhalt der Aussagen
  - auch nicht beim «Wenn …, dann …»
- Beispiel
  - P: *«2014 in Japan etwa 4.7 Mio. Pkw neu zugelassen.»*
  - Q: *«1999 gab es in Deutschland etwa 11.2 Mio. Internet-Nutzer»*
  - «Wenn P, dann Q»
    - P und Q sind nicht kausal verknüpft
    - Tatsächlich eine *wahre* Aussage
    - Fehlende Kausalität irrelavant

Wo sind wir?

Informelles

Syntax aussagenlogischer Formeln

Semantik aussagenlogischer Formeln

Boolesche Funktionen

Beweisbarkeit

Beweisen auf der Metaebene

Alphabet der Aussagenlogik

- Aussagevariable: $Var_{AL} = \{\mathtt{P}_0, \mathtt{P}_1, \mathtt{P}_2, \mathtt{P}_3, \ldots, \mathtt{P}_n\}$
  für bessere Lesbarkeit häufig auch $\mathtt{P}$, $\mathtt{Q}$, $\mathtt{R}$, $\mathtt{S}$
- aussagenlogische Verknüpfungen: $\neg$, $\wedge$, $\vee$, $\rightarrow$
- Alphabet

$$A_{AL} = \{\,(,), \neg, \wedge, \vee, \rightarrow\,\} \cup Var_{AL}\ .$$

- **Ziel im Folgenden:**
  Die formale Sprache $For_{AL} \subseteq A_{AL}^*$ der syntaktisch korrekten aussagenlogischen Formeln definieren.

Lesarten

$\neg G$ «nicht G»

$(G \wedge H)$ «G und H»

$(G \vee H)$ «G oder H»

$(G \rightarrow H)$ «G impliziert H» (oder «aus G folgt H»)

Konstruktionsabbildungen

- Eine Abbildung für jede Verknüpfung,
  z.B. $f_\wedge : A_{AL}^* \times A_{AL}^* \to A_{AL}^*, \qquad (G, H) \mapsto (G \wedge H)$

- analog für die anderen Verknüpfungen

- Darüber kann für eine Menge von Wörten M gebaut werden:

  $$Ver(M) = \{\neg G, \quad (G \wedge H), \quad (G \vee H), \quad (G \to H) \mid G, H \in M\}$$

  $Ver(M)$ ist die Menge der „einmal logisch verknüpften Wörter aus M“.

Syntax — Konstruktion immer größerer Formeln

- induktiv

$$M_0 = Var_{AL}$$

$$\text{für jedes } n \in \mathbb{N}_0 : M_{n+1} = Ver(M_n) \cup M_n$$

- alle Formeln zusammen: $For_{AL} = \bigcup_{i \in \mathbb{N}_0} M_i$

- **Typische Formulierung:**
  Die Menge der aussagenlogischen Formeln For_{AL} ist die kleinste Menge, für die gilt:
  - $Var_{AL} \subseteq For_{AL}$
  - Wenn $G \in For_{AL}$, dann ist $\neg G \in For_{AL}$
  - Wenn $G, H \in For_{AL}$, dann ist $(G \wedge H) \in For_{AL}$
  - Wenn $G, H \in For_{AL}$, dann ist $(G \vee H) \in For_{AL}$
  - Wenn $G, H \in For_{AL}$, dann ist $(G \rightarrow H) \in For_{AL}$

Konstruktion — ein Beispiel

- Es sei $Var_{AL} = \{\mathtt{P}, \mathtt{Q}\}$.
- $M_0 = \{\mathtt{P}, \mathtt{Q}\}$

Konstruktion — ein Beispiel

- Es sei $Var_{AL} = \{\mathtt{P}, \mathtt{Q}\}$.
- $M_0 = \{\mathtt{P}, \mathtt{Q}\}$
- also $M_1 = \{$ $\mathtt{P}$, $\mathtt{Q}$,

$$\begin{aligned}
&\neg\mathtt{P},\ \neg\mathtt{Q},\\
&(\mathtt{P} \land \mathtt{P}),\ (\mathtt{P} \land \mathtt{Q}),\ (\mathtt{Q} \land \mathtt{P}),\ (\mathtt{Q} \land \mathtt{Q}),\\
&(\mathtt{P} \lor \mathtt{P}),\ (\mathtt{P} \lor \mathtt{Q}),\ (\mathtt{Q} \lor \mathtt{P}),\ (\mathtt{Q} \lor \mathtt{Q}),\\
&(\mathtt{P} \rightarrow \mathtt{P}),\ (\mathtt{P} \rightarrow \mathtt{Q}),\ (\mathtt{Q} \rightarrow \mathtt{P}),\ (\mathtt{Q} \rightarrow \mathtt{Q})\ \}
\end{aligned}$$

Regeln zur Einsparung von Klammern

- Abkürzungen — «offizielle» Syntax bleibt gleich
  - äußere Klammern darf man weglassen:
    - $P \to Q$ statt $(P \to Q)$
  - mehrfach gleiches Konnektiv: «implizite Linksklammerung»
    - $P \land Q \land R$ statt $((P \land Q) \land R)$
  - verschiedene Konnektive ohne Klammern — verschiedene «Bindungsstärken»:
    - $\neg$ bindet am stärksten
    - $\land$ bindet am zweitstärksten
    - $\lor$ bindet am drittstärksten
    - $\to$ bindet am viertstärksten
    - $\leftrightarrow$ bindet am schwächsten

    Beispiel
    - $P \lor R \to \neg Q \land R$ statt $((P \lor R) \to (\neg Q \land R))$

Pingo Quiz!

s.kit.edu/
gbi-pingo

Welche der folgenden Zeichenfolge ist/sind *keine* AL-Formel?
(Gemäß der Konstruktionsregeln, ohne Klammern-weglassen)

Option A $(P \wedge ())$

Option B $\neg(\neg P)$

Option C $(((P)))$

Option D $((P \to P) \to (P \to P))$

Wo sind wir?

Informelles

Syntax aussagenlogischer Formeln

Semantik aussagenlogischer Formeln

Boolesche Funktionen

Beweisbarkeit

Beweisen auf der Metaebene

Ziel: Bedeutung einer aussagenlogischen Formel — eine boolesche Funktion

P_1	P_2	P_3
$\mathbf{f}$	$\mathbf{f}$	$\mathbf{f}$
$\mathbf{f}$	$\mathbf{f}$	$\mathbf{w}$
$\mathbf{f}$	$\mathbf{w}$	$\mathbf{f}$
$\mathbf{f}$	$\mathbf{w}$	$\mathbf{w}$
$\mathbf{w}$	$\mathbf{f}$	$\mathbf{f}$
$\mathbf{w}$	$\mathbf{f}$	$\mathbf{w}$
$\mathbf{w}$	$\mathbf{w}$	$\mathbf{f}$
$\mathbf{w}$	$\mathbf{w}$	$\mathbf{w}$

- «Wahrheitswerte»: $\mathbb{B} = \{\mathbf{w}, \mathbf{f}\}$
- Es sei V eine Menge von Aussagevariablen
- Interpretation $I : V \longrightarrow \mathbb{B}$,
  belegt die Aussagevariablen mit Wahrheitswerten.
- Darstellung z. B. in Tabellenform
  - jede Zeile eine Interpretation

Auswertung von Formeln

- Es sei $I : V \longrightarrow \mathbb{B}$ eine Interpretation.
- Auswertungsfunktion von AL-Formeln: $val_I : For_{AL} \longrightarrow \mathbb{B}$
- für jedes $X \in V$ sei $val_I(X) = I(X)$
- für jede $G, H \in For_{AL}$ sei

$$val_I(\neg G) = \begin{cases} \mathbf{w} & \text{falls } val_I(G) = \mathbf{f} \\ \mathbf{f} & \text{falls } val_I(G) = \mathbf{w} \end{cases}$$

$$val_I(G \wedge H) = \begin{cases} \mathbf{w} & \text{falls } val_I(G) = \mathbf{w} \text{ und } val_I(H) = \mathbf{w} \\ \mathbf{f} & \text{sonst} \end{cases}$$

$$val_I(G \vee H) = \begin{cases} \mathbf{w} & \text{falls } val_I(G) = \mathbf{w} \text{ oder } val_I(H) = \mathbf{w} \\ \mathbf{f} & \text{sonst} \end{cases}$$

$$val_I(G \rightarrow H) = \begin{cases} \mathbf{w} & \text{falls: Wenn } val_I(G) = \mathbf{w} \text{ dann } val_I(H) = \mathbf{w} \\ \mathbf{f} & \text{falls } val_I(G) = \mathbf{w} \text{ und } val_I(H) = \mathbf{f} \end{cases}$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\texttt{P}) = \mathbf{w}$ und $I(\texttt{Q}) = \mathbf{f}$
- Formel $G = \texttt{Q} \lor \neg(\texttt{P} \land \texttt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \vee \neg(\mathtt{P} \wedge \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$val_I(G) =$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \lor \neg(\mathtt{P} \land \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$\begin{aligned} val_I(G) &= \\ val_I(\mathtt{Q}) &= \\ val_I(\neg(\mathtt{P} \land \mathtt{Q})) &= \end{aligned}$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \lor \neg(\mathtt{P} \land \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$\begin{aligned} val_I(G) &= \\ val_I(\mathtt{Q}) &= \\ val_I(\neg(\mathtt{P} \land \mathtt{Q})) &= \\ val_I(\mathtt{P} \land \mathtt{Q}) &= \end{aligned}$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \lor \neg(\mathtt{P} \land \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$
\begin{aligned}
val_I(G) &= \\
val_I(\mathtt{Q}) &= \\
val_I(\neg(\mathtt{P} \land \mathtt{Q})) &= \\
val_I(\mathtt{P} \land \mathtt{Q}) &= \\
val_I(\mathtt{P}) &= \\
val_I(\mathtt{Q}) &=
\end{aligned}
$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \vee \neg(\mathtt{P} \wedge \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$
\begin{aligned}
val_I(G) &= \\
val_I(\mathtt{Q}) &= \mathbf{f} \\
val_I(\neg(\mathtt{P} \wedge \mathtt{Q})) &= \\
val_I(\mathtt{P} \wedge \mathtt{Q}) &= \\
val_I(\mathtt{P}) &= \mathbf{w} \\
val_I(\mathtt{Q}) &= \mathbf{f}
\end{aligned}
$$

Auswertung von Formeln — ein Beispiel

Karlsruher Institut für Technologie

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \vee \neg(\mathtt{P} \wedge \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$
\begin{aligned}
val_I(G) &= \\
val_I(\mathtt{Q}) &= \mathbf{f} \\
val_I(\neg(\mathtt{P} \wedge \mathtt{Q})) &= \\
val_I(\mathtt{P} \wedge \mathtt{Q}) &= \mathbf{f} \\
val_I(\mathtt{P}) &= \mathbf{w} \\
val_I(\mathtt{Q}) &= \mathbf{f}
\end{aligned}
$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \vee \neg(\mathtt{P} \wedge \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$
\begin{aligned}
val_I(G) &= \\
val_I(\mathtt{Q}) &= \mathbf{f} \\
val_I(\neg(\mathtt{P} \wedge \mathtt{Q})) &= \mathbf{w} \\
val_I(\mathtt{P} \wedge \mathtt{Q}) &= \mathbf{f} \\
val_I(\mathtt{P}) &= \mathbf{w} \\
val_I(\mathtt{Q}) &= \mathbf{f}
\end{aligned}
$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \lor \neg(\mathtt{P} \land \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$
\begin{aligned}
val_I(G) &= \\
val_I(\mathtt{Q}) &= \mathbf{f} \\
val_I(\neg(\mathtt{P} \land \mathtt{Q})) &= \mathbf{w} \\
val_I(\mathtt{P} \land \mathtt{Q}) &= \mathbf{f} \\
val_I(\mathtt{P}) &= \mathbf{w} \\
val_I(\mathtt{Q}) &= \mathbf{f}
\end{aligned}
$$

Auswertung von Formeln — ein Beispiel

- Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$
- Formel $G = \mathtt{Q} \vee \neg(\mathtt{P} \wedge \mathtt{Q})$
- berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

$$\begin{aligned}
val_I(G) &= \mathbf{w} \\
val_I(\mathtt{Q}) &= \mathbf{f} \\
val_I(\neg(\mathtt{P} \wedge \mathtt{Q})) &= \mathbf{w} \\
val_I(\mathtt{P} \wedge \mathtt{Q}) &= \mathbf{f} \\
val_I(\mathtt{P}) &= \mathbf{w} \\
val_I(\mathtt{Q}) &= \mathbf{f}
\end{aligned}$$

Auswertung einer Formel für alle Interpretationen

- oft in Tabellenform
- Beispiel

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$
f	**f**	**w**	**w**	**w**	**f**	**w**
f	**w**	**w**	**f**	**w**	**f**	**w**
w	**f**	**f**	**w**	**w**	**f**	**w**
w	**w**	**f**	**f**	**f**	**w**	**f**

Auswertung einer Formel für alle Interpretationen

- oft in Tabellenform
- Beispiel

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$P \wedge Q$	$\neg(P \wedge Q)$
f	f	w	w	w	f	w
f	w	w	f	w	f	w
w	f	f	w	w	f	w
w	w	f	f	f	w	f

- vergleiche drittletzte und letzte Spalte

Äquivalente Formeln

- zwei Formeln G und H heißen äquivalent
  wenn für jede Interpretation I gilt: $val_I(G) = val_I(H)$.
  - geschrieben $G \equiv H$
- Beispiele:

$$\neg P \lor \neg Q \equiv \neg(P \land Q)$$

$$\neg\neg P \equiv P$$

$$P \to Q \equiv (\neg P) \lor Q$$

- informelle Überlegung zum letzten Fall
  - «Gegenteil» von $P \to Q$: $(P \land \neg Q)$
  - also $P \to Q$ äquivalent zu $\neg(P \land \neg Q)$
  - äquivalent zu $(\neg P) \lor (\neg\neg Q)$
  - äquivalent zu $(\neg P) \lor Q$

Modelle

- Interpretation I *Modell* einer Formel G, wenn $val_I(G) = \mathbf{w}$ ist.
- Interpretation I *Modell* für Formelmenge Γ, wenn I Modell jeder Formel $G \in \Gamma$ ist.
- $\Gamma \models G$: jedes Modell von Γ auch Modell von G
  - $H \models G$ statt $\{H\} \models G$
- $\models G$ statt $\{\} \models G$
  - G für *alle* Interpretationen wahr

Wichtige Spezialfälle aussagenlogischer Formeln

- Formel G *Tautologie* oder *allgemeingültig*,
  wenn *jede* Interpretation Modell
  - $\models G$
  - z. B. $\mathtt{P} \vee \neg \mathtt{P}$
  - z. B. $\mathtt{P} \to (\mathtt{Q} \to \mathtt{P})$

  das ist ein *semantischer* Begriff

- Formel G *erfüllbar*, wenn für mindestens ein I wahr

Tautologien — viele Beispiele auf ein Mal

- betrachte $G \leftrightarrow H$: Abkürzung für $(G \rightarrow H) \wedge (H \rightarrow G)$

- Wertetabelle für $G \leftrightarrow H$:

G	H	$G \rightarrow H$	$H \rightarrow G$	$G \leftrightarrow H$
f	**f**	**w**	**w**	**w**
f	**w**	**w**	**f**	**f**
w	**f**	**f**	**w**	**f**
w	**w**	**w**	**w**	**w**

$$val_I(G \leftrightarrow H) = \begin{cases} \mathbf{w} & \text{falls } val_I(G) = val_I(H) \\ \mathbf{f} & \text{sonst} \end{cases}$$

- **Erinnerung:** $G \equiv H$ bedeutet $val_I(G) = val_I(H)$ für jedes I

zwei Äquivalenz«begriffe» die zusammenpassen

eben überlegt:

Lemma

Wenn $G \equiv H$ ist, dann ist $G \leftrightarrow H$ Tautologie.

zwei Äquivalenz«begriffe» die zusammenpassen

eben überlegt:

Lemma

Wenn $G \equiv H$ ist, dann ist $G \leftrightarrow H$ Tautologie.

umgekehrt gilt auch

Lemma

Wenn $G \leftrightarrow H$ Tautologie ist, dann ist $G \equiv H$.

hier zahlt es sich aus, dass wir «wenn» und «dann» sagen und dafür nicht auch noch Pfeile malen …

Tautologien — konkrete Beispiele

für $G, H, K \in For_{AL}$ sind Tautologien:

- $\neg\neg G \leftrightarrow G$
- $(G \rightarrow H) \leftrightarrow (\neg G \vee H)$
- $(G \rightarrow H) \leftrightarrow (\neg H \rightarrow \neg G)$
- $(G \wedge H) \leftrightarrow \neg(\neg G \vee \neg H)$ und $(G \vee H) \leftrightarrow \neg(\neg G \wedge \neg H)$
- $\neg(G \wedge H) \leftrightarrow (\neg G \vee \neg H)$ und $\neg(G \vee H) \leftrightarrow (\neg G \wedge \neg H)$
- $G \wedge G \leftrightarrow G$ und $G \vee G \leftrightarrow G$
- $G \wedge H \leftrightarrow H \wedge G$ und $G \vee H \leftrightarrow H \vee G$
- $(G \wedge H) \wedge K \leftrightarrow G \wedge (H \wedge K)$ und $(G \vee H) \vee K \leftrightarrow G \vee (H \vee K)$

Tautologien — konkrete Beispiele

für $G, H, K \in For_{AL}$ sind Tautologien:

Doppelnegation	$\neg\neg G \leftrightarrow G$
	$(G \to H) \leftrightarrow (\neg G \vee H)$
Kontraposition	$(G \to H) \leftrightarrow (\neg H \to \neg G)$
	$(G \wedge H) \leftrightarrow \neg(\neg G \vee \neg H)$ und $(G \vee H) \leftrightarrow \neg(\neg G \wedge \neg H)$
De Morgan	$\neg(G \wedge H) \leftrightarrow (\neg G \vee \neg H)$ und $\neg(G \vee H) \leftrightarrow (\neg G \wedge \neg H)$
Idempotenz	$G \wedge G \leftrightarrow G$ und $G \vee G \leftrightarrow G$
Kommutativität	$G \wedge H \leftrightarrow H \wedge G$ und $G \vee H \leftrightarrow H \vee G$
Assoziativität	$(G \wedge H) \wedge K \leftrightarrow G \wedge (H \wedge K)$ und $(G \vee H) \vee K \leftrightarrow G \vee (H \vee K)$

Tautologien — konkrete Beispiele

für $G, H, K \in For_{AL}$ sind Tautologien:

Doppelnegation	■ $\neg\neg G \leftrightarrow G$
	■ $(G \to H) \leftrightarrow (\neg G \lor H)$
Kontraposition	■ $(G \to H) \leftrightarrow (\neg H \to \neg G)$
	■ $(G \land H) \leftrightarrow \neg(\neg G \lor \neg H)$ und $(G \lor H) \leftrightarrow \neg(\neg G \land \neg H)$
De Morgan	■ $\neg(G \land H) \leftrightarrow (\neg G \lor \neg H)$ und $\neg(G \lor H) \leftrightarrow (\neg G \land \neg H)$
Idempotenz	■ $G \land G \leftrightarrow G$ und $G \lor G \leftrightarrow G$
Kommutativität	■ $G \land H \leftrightarrow H \land G$ und $G \lor H \leftrightarrow H \lor G$
Assoziativität	■ $(G \land H) \land K \leftrightarrow G \land (H \land K)$ und $(G \lor H) \lor K \leftrightarrow G \lor (H \lor K)$

Ähnlichkeit zur Mengenlehre kein Zufall ($\longrightarrow$ *Boolesche Algebra*)

Tautologien anderer Bauart

für $G, H, K \in For_{AL}$ sind Tautologien:

- $G \to G$
- $\neg G \vee G$
- $G \to (H \to G)$
- $(G \wedge H) \to G$
- $(G \to (H \to K)) \to ((G \to H) \to (G \to K))$
- $(\neg H \to \neg G) \to ((\neg H \to G) \to H)$
- **FALSCH** $\to G$ (worin **FALSCH** $:= \mathtt{P} \wedge \neg \mathtt{P}$)

Tautologien anderer Bauart

für $G, H, K \in For_{AL}$ sind Tautologien:

- $G \rightarrow G$
- **Tertium non datur** $\neg G \vee G$
- $G \rightarrow (H \rightarrow G)$
- $(G \wedge H) \rightarrow G$
- $(G \rightarrow (H \rightarrow K)) \rightarrow ((G \rightarrow H) \rightarrow (G \rightarrow K))$
- $(\neg H \rightarrow \neg G) \rightarrow ((\neg H \rightarrow G) \rightarrow H)$
- **Ex falso quod libet** $\textbf{FALSCH} \rightarrow G$ (worin $\textbf{FALSCH} := \mathtt{P} \wedge \neg \mathtt{P}$)

Pingo Quiz!

s.kit.edu/
gbi-pingo

Welche Option gilt für die beiden Symbolen $\equiv$ und $\leftrightarrow$? Wie unterscheiden sie sich?

Option A $G \leftrightarrow H$ kann wahr und falsch ergeben, $G \equiv H$ kann nicht falsch sein.

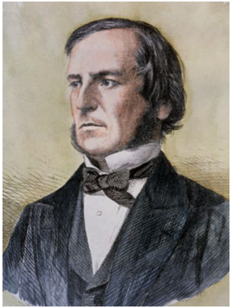
Option B $G \equiv H$ kann wahr und falsch ergeben, $G \leftrightarrow H$ kann nicht falsch sein.

Option C $G \leftrightarrow H$ ist eine Formel, $G \equiv H$ ist eine Aussage über Formeln.

Option D $G \equiv H$ ist eine Formel, $G \leftrightarrow H$ ist eine Aussage über Formeln.

Wo sind wir?

George Boole



public domain, commons.wikimedia.org/ wiki/

File:George_Boole_color.jpg

- George Boole (2.11.1815 – 8.12.1864)
- englischer Mathematiker und Philosoph
- Professor in Cork (Irland)
- Buch (1854):
  An Investigation of the Laws of Thought
  on Which are Founded the Mathematical Theories
  of Logic and Probabilities

Boolesche Funktionen

Karlsruher Institut für Technologie

- **Erinnerung:** «Wahrheitswerte»: $\mathbb{B} = \{\mathbf{w}, \mathbf{f}\}$
- boolesche Funktionen $f : \mathbb{B}^k \to \mathbb{B}$
- **Übliche Notationen für Boolesche Operatoren**

	math. geprägt	*techn. geprägt*	
$b_{\neg}(x)$	$\neg x$	$\overline{x}$	Negation bzw. Nicht
$b_{\wedge}(x, y)$	$x \wedge y$	$x \cdot y$	Und
$b_{\vee}(x, y)$	$x \vee y$	$x + y$	Oder
$b_{\rightarrow}(x, y)$	$x \rightarrow y$		Implikation

- bei Verwendung von $+$, $\cdot$ und meist auch 0 statt $\mathbf{f}$ und 1 statt $\mathbf{w}$

Beispiele für boolesche Funktionen

x_1	x_2	x_3	$x_1 \wedge x_2$ $x_1 \cdot x_2$	$x_1 \vee x_2 \vee x_3$ $x_1 + x_2 + x_3$	$f_{???}(x_1, x_2, x_3)$
f	**f**	**f**	**f**	**f**	**f**
f	**f**	**w**	**f**	**w**	**f**
f	**w**	**f**	**f**	**w**	**f**
f	**w**	**w**	**f**	**w**	**w**
w	**f**	**f**	**f**	**w**	**f**
w	**f**	**w**	**f**	**w**	**w**
w	**w**	**f**	**w**	**w**	**w**
w	**w**	**w**	**w**	**w**	**w**

Ausdrucksstärke der Aussagenlogik

Karlsruher Institut für Technologie

Für jede Boolesche Funktion $f : \mathbb{B}^n \to \mathbb{B}$
gibt es eine erzeugende Formel $F \in For_{AL}$ mit:

$$f(x_1, \ldots, x_n) = val_{I^{x_1,\ldots,x_n}}(F)$$

- *Argument Boolescher Funktion*: Tupel $x_1, \ldots, x_n \in \mathbb{B}^n$.
- *Formel-Auswertung*: Interpretation $I : V \to \mathbb{B}$

$\Longrightarrow$ *Lösung*: Boolesches Tupel als Interpretation verstehen:

$$I^{x_1,\ldots,x_n}(\mathtt{P}_i) = x_i \quad \text{für } i \in \{1, \ldots, n\}$$

Pingo Quiz!

Karlsruher Institut für Technologie

s.kit.edu/
gbi-pingo

Welche der folgenden Formeln erzeugt die Boolesche Funktion f_{min2} mit

$$f_{min2}(x_1, x_2, x_3) = \mathbf{w} \iff \text{wenigstens 2 Argumente sind } \mathbf{w} \; ?$$

Äquivalent dazu:
Welche Formel ist genau dann wahr, wenn wenigstens zwei der Variablen $\mathtt{P}$, $\mathtt{Q}$, $\mathtt{R}$ zu wahr ausgewertet werden?

Option A $\mathtt{P} \vee \mathtt{Q} \vee \mathtt{R}$

Option B $(\mathtt{P} \wedge \mathtt{Q}) \vee (\mathtt{Q} \wedge \mathtt{R}) \vee (\mathtt{R} \wedge \mathtt{P})$

Option C $(\mathtt{P} \rightarrow \mathtt{Q}) \wedge (\mathtt{Q} \rightarrow \mathtt{R}) \wedge (\mathtt{R} \rightarrow \mathtt{P})$

Option D $\neg\neg\mathtt{P} \wedge \neg\neg\mathtt{Q} \wedge \neg\neg\mathtt{R}$

Wo sind wir?

Kalkül — ein System für Beweise

nun ein rein *syntaktisches* «Spiel mit Bauklötzchen»

- allgemein
  - Alphabet A
  - syntaktisch korrekte Formeln $For \subseteq A^*$
  - *Axiome* $Ax \subseteq For$,
  - *Schlussregeln*

- **Sprachlich:** Der Kalkül (m.) für eine Logik, aber «Das Kalkül (n.) geht nicht auf.»

Schlussregeln

$$\frac{V_1 \quad V2 \quad \ldots \quad V_n}{C}\text{(R)}$$

- Endliche Menge an Voraussetzungen $\{V_1, V_2, \ldots, V_n\}$

Beispiele:

Formal ist eine Regel R ein Tupel $R \in \mathit{For}_{AL}^{*} \times \mathit{For}_{AL}$.

Schlussregeln

$$\frac{V_1 \quad V2 \quad \dots \quad V_n}{C}\,(\mathrm{R})$$

- Endliche Menge an Voraussetzungen $\{V_1, V_2, \dots, V_n\}$
- Genau eine Folgerung (Conclusio) C

Beispiele:

Formal ist eine Regel R ein Tupel $R \in \mathit{For}_{AL}^{*} \times \mathit{For}_{AL}$.

Schlussregeln

$$\frac{V_1 \quad V2 \quad \dots \quad V_n}{C}\,(\mathrm{R})$$

- Endliche Menge an Voraussetzungen $\{V_1, V_2, \dots, V_n\}$
- Genau eine Folgerung (Conclusio) C
- **Korrektheit:** Regel R heißt korrekt, wenn gilt:
  wenn alle Voraussetzungen Tautologien sind, dann ist auch C eine Tautologie.

Beispiele:

Formal ist eine Regel R ein Tupel $R \in For_{AL}^{*} \times For_{AL}$.

Schlussregeln

$$\frac{V_1 \quad V2 \quad \dots \quad V_n}{C}\,(\mathrm{R})$$

- Endliche Menge an Voraussetzungen $\{V_1, V_2, \dots, V_n\}$
- Genau eine Folgerung (Conclusio) C
- **Korrektheit:** Regel R heißt korrekt, wenn gilt:
  wenn alle Voraussetzungen Tautologien sind, dann ist auch C eine Tautologie.

Beispiele:

- $\dfrac{A \wedge B}{A}$ und $\dfrac{A \wedge B}{B}$ und $\dfrac{A \quad B}{A \wedge B}$

Formal ist eine Regel R ein Tupel $R \in \mathit{For}_{AL}^{*} \times \mathit{For}_{AL}$.

Schlussregeln

$$\frac{V_1 \quad V2 \quad \dots \quad V_n}{C}(\mathrm{R})$$

- Endliche Menge an Voraussetzungen $\{V_1, V_2, \dots, V_n\}$
- Genau eine Folgerung (Conclusio) C
- **Korrektheit:** Regel R heißt korrekt, wenn gilt:
  wenn alle Voraussetzungen Tautologien sind, dann ist auch C eine Tautologie.

Beispiele:

- $\frac{A \wedge B}{A}$ und $\frac{A \wedge B}{B}$ und $\frac{A \quad B}{A \wedge B}$
- $\frac{A \rightarrow B \quad \neg A \rightarrow B}{B}$ und $\frac{\neg A \rightarrow \textbf{Falsch}}{A}$

Formal ist eine Regel R ein Tupel $R \in For_{AL}^* \times For_{AL}$.

Schlussregeln

$$\frac{V_1 \quad V2 \quad \dots \quad V_n}{C}\,(R)$$

- Endliche Menge an Voraussetzungen $\{V_1, V_2, \dots, V_n\}$
- Genau eine Folgerung (Conclusio) C
- **Korrektheit:** Regel R heißt korrekt, wenn gilt:
  wenn alle Voraussetzungen Tautologien sind, dann ist auch C eine Tautologie.

Beispiele:

- $\dfrac{A \wedge B}{A}$ und $\dfrac{A \wedge B}{B}$ und $\dfrac{A \quad B}{A \wedge B}$
- $\dfrac{A \to B \quad \neg A \to B}{B}$ und $\dfrac{\neg A \to \textbf{Falsch}}{A}$
- $\dfrac{A \to B \quad A}{B}$

Formal ist eine Regel R ein Tupel $R \in For^*_{AL} \times For_{AL}$.

Natürliches Schließen

$$\frac{A \quad B}{A \wedge B}\ (\wedge \mathrm{I}) \qquad \frac{A \wedge B}{A}\ (\wedge \mathrm{E}_l) \qquad \frac{A \wedge B}{B}\ (\wedge \mathrm{E}_r)$$

$$\frac{A}{A \vee B}\ (\vee \mathrm{I}_l) \qquad \frac{B}{A \vee B}\ (\vee \mathrm{I}_r) \qquad \frac{A \vee B \quad A \to C \quad B \to C}{C}\ (\vee \mathrm{E})$$

$$\frac{A \vdash B}{A \to B}\ (\to \mathrm{I}) \qquad \frac{A \quad A \to B}{B}\ (\mathrm{MP})\ (\to \mathrm{E})$$

$$\frac{A \to \texttt{FALSCH}}{\neg A}\ (\neg \mathrm{I}) \qquad \frac{A \quad \neg A}{\texttt{FALSCH}}\ (\neg \mathrm{E}) \qquad \frac{\neg\neg A}{A}\ (\neg\neg \mathrm{E})$$

$$\frac{\neg A \to \texttt{FALSCH}}{A}\ (\mathrm{RAA}) \qquad \frac{}{A \vdash A}\ (\mathrm{Ax})$$

- „natürlich“ weil dem menschlichen Schließen nahe liegend.
- **Kalkül korrekt:** Jede Regel ist korrekt
- **Kalkül vollständig:** Jede aussagenlog. Tautologie kann abgleitet werden.

Jakowski
Gentzen (1934)

Formeln mit Bedingungen

Tritt auf in:

$$\frac{A \vdash B}{A \to B}\ (\to E)$$

$$\frac{}{A \vdash A}\ (Ax)$$

- Beweis für Formel $F \in For_{AL}$ bezgl. Voraussetzungen $\Gamma \subseteq For_{AL}$: $\Gamma \vdash F$
- Schlussregeln eigentlich:

$$\frac{\Gamma_1 \vdash V_1 \quad \Gamma_2 \vdash V_2 \quad \dots \quad \Gamma_n \vdash V_n}{\bigcup_{i=1}^{n} \Gamma_i \vdash C}\ (R)$$

- Regel $(\to I)$ ist die Möglichkeit Voraussetzungen „loszuwerden“.

Beispielbeweise

Beispiel:

Beweise: $\models (\mathtt{P} \land \mathtt{Q}) \to (\mathtt{P} \lor \mathtt{Q})$

Beispielbeweise

Beispiel:

Beweise: $\models (P \wedge Q) \rightarrow (P \vee Q)$

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{P \wedge Q \vdash P \wedge Q}\,(\mathrm{Ax})}{P \wedge Q \vdash P}\,(\wedge \mathrm{E})}{P \wedge Q \vdash P \vee Q}\,(\vee \mathrm{I}_l)}{P \wedge Q \;\rightarrow\; P \vee Q}\,(\rightarrow \mathrm{I})
$$

Beispielbeweise

Beispiel:

Beweise: $\models (P \land Q) \to (P \lor Q)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \land Q \vdash P \land Q}\,(\text{Ax})}{P \land Q \vdash P}\,(\land\text{E})}{P \land Q \vdash P \lor Q}\,(\lor\text{I}_l)}{P \land Q \;\to\; P \lor Q}\,(\to\text{I})$$

Beispiel:

Beweise: $\models (P \land Q) \to (Q \land P)$

Beispielbeweise

Beispiel:

Beweise: $\models (P \land Q) \rightarrow (P \lor Q)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \land Q \vdash P \land Q}\,(\mathrm{Ax})}{P \land Q \vdash P}\,(\land\mathrm{E})}{P \land Q \vdash P \lor Q}\,(\lor\mathrm{I}_l)}{P \land Q \rightarrow P \lor Q}\,(\rightarrow\mathrm{I})$$

Beispiel:

Beweise: $\models (P \land Q) \rightarrow (Q \land P)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \land Q \vdash P \land Q}\,(\mathrm{Ax})}{P \land Q \vdash Q}\,(\land\mathrm{E}_r) \qquad \dfrac{\dfrac{}{P \land Q \vdash P \land Q}\,(\mathrm{Ax})}{P \land Q \vdash P}\,(\land\mathrm{E}_l)}{P \land Q \vdash Q \land P}\,(\land\mathrm{I})}{P \land Q \rightarrow Q \land P}\,(\rightarrow\mathrm{I})$$

Abschreckendes Beispiel

Beweise: $\boxed{\models P \lor \neg P}$

Abschreckendes Beispiel

Beweise:

$$\boxed{\models P \lor \neg P}$$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$\neg(P \lor \neg P) \vdash \neg(P \lor \neg P)$}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$\neg(P \lor \neg P) \vdash \neg(P \lor \neg P)$}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$P \vdash P$}
\RightLabel{($\lor I_l$)}
\UnaryInfC{$P \vdash P \lor \neg P$}
\RightLabel{($\neg E$)}
\BinaryInfC{$\neg(P \lor \neg P), P \vdash \mathtt{FALSCH}$}
\RightLabel{($\to I$)}
\UnaryInfC{$\neg(P \lor \neg P) \vdash P \to \mathtt{FALSCH}$}
\RightLabel{($\neg I$)}
\UnaryInfC{$\neg(P \lor \neg P) \vdash \neg P$}
\RightLabel{($\lor I_r$)}
\UnaryInfC{$\neg(P \lor \neg P) \vdash P \lor \neg P$}
\RightLabel{($\neg E$)}
\BinaryInfC{$\neg(P \lor \neg P) \vdash \mathtt{FALSCH}$}
\RightLabel{($\to I$)}
\UnaryInfC{$\neg(P \lor \neg P) \to \mathtt{FALSCH}$}
\RightLabel{(RAA)}
\UnaryInfC{$P \lor \neg P$}
\end{prooftree}
$$

Wo sind wir?

Informelles

Syntax aussagenlogischer Formeln

Semantik aussagenlogischer Formeln

Boolesche Funktionen

Beweisbarkeit

Beweisen auf der Metaebene

Wozu denn dann?

- Nicht so gut für Beweissuche
- Wofür ist der Kalkül denn dann gut
- „Natürliches“ Schließen ausnutzen

!!! Beweisen auf der informellen / semiformellen / äußeren Metaebene

Beweisen auf der Metaebene

$$\frac{A \quad B}{A \land B} \; (\land I)$$

Zu zeigen ist $A \land B$. Dies zeigen wir getrennt:

1. *zu zeigen ist A.*

   $\ldots$

2. *zu zeigen ist B.*

   $\ldots$

Beweisen auf der Metaebene

$$\frac{A \quad B}{A \wedge B}\ (\wedge I)$$

Zu zeigen ist $A \wedge B$. Dies zeigen wir getrennt:

1. *zu zeigen ist A.*

   $\ldots$

2. *zu zeigen ist B.*

   $\ldots$

$$\frac{A \to B \qquad \neg A \to B}{B}$$

Zu zeigen ist B. Dazu eine Fallunterscheidung nach A:

- *1. Fall: A gelte.*

  $\ldots$ *‹Daraus folgt, dass B gilt. ›*

- *2. Fall: A gelte nicht.*

  $\ldots$ *‹Daraus folgt, dass B gilt.›*

Insgesamt ist damit B gezeigt.

Beweisen auf der Metaebene (II)

$$\frac{\neg A \rightarrow \texttt{FALSCH}}{A}\ (\text{RAA})$$

Zu zeigen ist A. Angenommen A sei nicht wahr, dann …

…

Daraus ergibt sich ein Widerspruch. Also gilt die Aussage A.

Beweisen auf der Metaebene (II)

$$\frac{\neg A \rightarrow \texttt{FALSCH}}{A}\ (\text{RAA})$$

Zu zeigen ist A. Angenommen A sei nicht wahr, dann …
…
Daraus ergibt sich ein Widerspruch. Also gilt die Aussage A.

Euklids Beweis für den Satz von Euklid

Zu zeigen ist, dass es unendlich viele Primzahlen gibt. Angenommen, die Menge $P \subseteq \mathbb{N}_+$ aller Primzahlen sei endlich. Dann gibt es auch eine größte Primzahl $p_{\max} \in P$, so dass für alle Primzahlen $p \in P$ gilt, dass $p \leq p_{\max}$. Definieren wir nun die Zahl $N := \left(\prod_{p \in P} p\right) + 1$, also das Produkt aller (endlich vielen) Primzahlen plus 1. Welche Primfaktoren hat N? Tatsächlich teilen nur 1 und N diese Zahl. Jede andere Primzahl kann kein Teiler von N sein, weil p ja schon $N - 1$ teilt. Also ist N eine Primzahl. N ist aber auch größer als $p_{\max}$. Dies ist ein Widerspruch zur Annahme, dass es nur endlich viele Primzahlen gebe. Deswegen muss es unendlich viele Primzahlen geben.

Abschlussbemerkung ...

Karlsruher Institut für Technologie

- Der Kalkül ist theoretisch sehr wertvoll.
- In der Praxis Aussagenlogik häufig verwendet,
  z. B. Konfigurationsmanagement:
  - PKW-Konfigurationen,
  - Software-Paketmanager
  - ...
- mittels automatischen Beweisern entschieden
- Diese verwenden fundamental andere Techniken!

Was ist wichtig

- Das sollten Sie mitnehmen:
  - *aussagenlogische Formeln* haben
    - Syntax
    - Semantik
  - *boolesche Funktionen*
  - Formalisierung von *Beweisbarkeit* in Kalkülen
    - Zusammenhang mit Allgemeingültigkeit

Das sollten Sie üben:

- Rechnen mit booleschen Funktionen
- Überprüfen von Formeln auf Erfüllbarkeit und Allgemeingültigkeit
- präzises Argumentieren wie bei Beweisen in Kalkülen