Grundbegriffe der Informatik

Kapitel 5: Aussagenlogik

Thomas Worsch

KIT, Institut für Theoretische Informatik

Wintersemester 2015/2016

Wo sind wir?

Informelles

Syntax aussagenlogischer Formeln

Boolesche Funktionen

Semantik aussagenlogischer Formeln

Beweisbarkeit

Aussagen — „objektiv“ wahr oder falsch

Beispielaussagen

- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist injektiv.“
- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist surjektiv.“

Aussagen — „objektiv“ wahr oder falsch

Beispielaussagen

- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist injektiv.“ **wahr**
- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist surjektiv.“

Aussagen — „objektiv“ wahr oder falsch

Beispielaussagen

- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist injektiv.“ **wahr**
- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist surjektiv.“ **falsch**

Aussagen — „objektiv“ wahr oder falsch

Beispielaussagen

- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist injektiv.“ **wahr**
- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist surjektiv.“ **falsch**

Manches ist keine Aussage, sondern sinnlos

- „Ein Barbier ist ein Mann,
  der genau alle diejenigen Männer rasiert,
  die sich nicht selbst rasieren.“

Aussagen — „objektiv“ wahr oder falsch

Beispielaussagen

- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist injektiv.“ **wahr**
- „Die Abbildung $U : A_U \to \mathbb{N}_0$ ist surjektiv.“ **falsch**

Manches ist keine Aussage, sondern sinnlos

- „Ein Barbier ist ein Mann,
  der genau alle diejenigen Männer rasiert,
  die sich nicht selbst rasieren.“
- Rasiert er sich selbst?

Komplizierte Aussagen —
aus einfacheren zusammengesetzt

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.

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.

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 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.

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 es in Deutschland etwa 11.2 Mio. Internet-Nutzer“*
- „Wenn P, dann Q“
  - tatsächlich eine Aussage
  - und zwar *wahr*
  - Kausalität irrelavant

Wo sind wir?

Informelles

Syntax aussagenlogischer Formeln

Boolesche Funktionen

Semantik aussagenlogischer Formeln

Beweisbarkeit

Alphabet der Aussagenlogik

Aussagevariable: $\mathtt{P}_0, \mathtt{P}_1, \mathtt{P}_2, \mathtt{P}_3 \ldots$
$Var_{AL} \subseteq \{\mathtt{P}_i \mid i \in \mathbb{N}_0\}$

- kurz $\mathtt{P}, \mathtt{Q}, \mathtt{R}, \mathtt{S}$

aussagenlogische Konnektive: $\neg, \wedge, \vee, \rightarrow$

Alphabet

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

Konstruktionsabbildungen

$$
\begin{aligned}
f_{\neg} &: && A_{AL}^* \to A_{AL}^* : && G \mapsto (\neg G) \\
f_{\wedge} &: A_{AL}^* \times{} && A_{AL}^* \to A_{AL}^* : && (G,H) \mapsto (G \wedge H) \\
f_{\vee} &: A_{AL}^* \times{} && A_{AL}^* \to A_{AL}^* : && (G,H) \mapsto (G \vee H) \\
f_{\to} &: A_{AL}^* \times{} && A_{AL}^* \to A_{AL}^* : && (G,H) \mapsto (G \to H)
\end{aligned}
$$

sinnvolles Beispiel:

$f_{\wedge}(\,(\mathtt{P} \to \mathtt{Q})\,,\ \mathtt{R}\,) = ((\mathtt{P} \to \mathtt{Q}) \wedge \mathtt{R})$

auch ein Beispiel:

$f_{\wedge}(\neg \to\ ), \mathtt{R}\vee) = (\,\neg \to\ ) \wedge \mathtt{R} \vee\ )$

jede Abbildung vergrößert die Anzahl Konnektive

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")

Syntax — Konstruktion immer größerer Formeln

induktiv

$$
\begin{aligned}
M_0 &= Var_{AL} \\
\text{für jedes } n \in \mathbb{N}_0 : M_{n+1} &= M_n \cup f_{\neg}(M_n) \\
&\quad \cup f_{\wedge}(M_n \times M_n) \\
&\quad \cup f_{\vee}(M_n \times M_n) \\
&\quad \cup f_{\rightarrow}(M_n \times M_n)
\end{aligned}
$$

die Formeln: alle zusammen

$$For_{AL} = \bigcup_{i \in \mathbb{N}_0} M_i$$

Konstruktion — ein Beispiel

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

$M_0 = \{\mathtt{P}, \mathtt{Q}\}$

Konstruktion — ein Beispiel

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

$M_0 = \{\mathtt{P}, \mathtt{Q}\}$

$$
\begin{aligned}
f_{\neg}(M_0) &= \{\mathtt{(\neg P)}, \mathtt{(\neg Q)}\} \\
f_{\wedge}(M_0 \times M_0) &= \{\mathtt{(P \wedge P)}, \mathtt{(P \wedge Q)}, \mathtt{(Q \wedge P)}, \mathtt{(Q \wedge Q)}\} \\
f_{\vee}(M_0 \times M_0) &= \{\mathtt{(P \vee P)}, \mathtt{(P \vee Q)}, \mathtt{(Q \vee P)}, \mathtt{(Q \vee Q)}\} \\
f_{\rightarrow}(M_0 \times M_0) &= \{\mathtt{(P \rightarrow P)}, \mathtt{(P \rightarrow Q)}, \mathtt{(Q \rightarrow P)}, \mathtt{(Q \rightarrow Q)}\}
\end{aligned}
$$

Konstruktion — ein Beispiel

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

$$M_0 = \{\mathtt{P}, \mathtt{Q}\}$$

$$\begin{aligned}
f_\neg(M_0) &= \{(\neg\mathtt{P}), (\neg\mathtt{Q})\}\\
f_\wedge(M_0 \times M_0) &= \{(\mathtt{P}\wedge\mathtt{P}), (\mathtt{P}\wedge\mathtt{Q}), (\mathtt{Q}\wedge\mathtt{P}), (\mathtt{Q}\wedge\mathtt{Q})\}\\
f_\vee(M_0 \times M_0) &= \{(\mathtt{P}\vee\mathtt{P}), (\mathtt{P}\vee\mathtt{Q}), (\mathtt{Q}\vee\mathtt{P}), (\mathtt{Q}\vee\mathtt{Q})\}\\
f_\rightarrow(M_0 \times M_0) &= \{(\mathtt{P}\rightarrow\mathtt{P}), (\mathtt{P}\rightarrow\mathtt{Q}), (\mathtt{Q}\rightarrow\mathtt{P}), (\mathtt{Q}\rightarrow\mathtt{Q})\}
\end{aligned}$$

also $M_1 = \{\mathtt{P}, \mathtt{Q},$

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

Konstruktion aussagenlogischer Formeln

M_2 enthält zum Beispiel

- $(\neg(\neg P))$
- $((P \to Q) \land (Q \lor P))$

aber zum Beispiel auch

- $(Q \lor (\neg Q))$
- $((P \lor Q) \land P)$
- $(P \to (Q \to P))$

Konstruktion aussagenlogischer Formeln

M_2 enthält zum Beispiel

- $(\neg(\neg P))$
- $((P \to Q) \wedge (Q \vee P))$

aber zum Beispiel auch

- $(Q \vee (\neg Q))$
- $((P \vee Q) \wedge P)$
- $(P \to (Q \to P))$

für jede Formel G und H noch eine Abkürzung

- $(G \leftrightarrow H)$ statt $((G \to H) \wedge (H \to G))$

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 von $((P \lor R) \to ((\neg Q) \land R))$

Wo sind wir?

Informelles

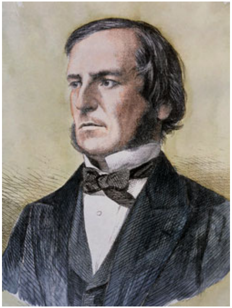
Syntax aussagenlogischer Formeln

Boolesche Funktionen

Semantik aussagenlogischer Formeln

Beweisbarkeit

George Boole



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

„Wahrheitswerte“: $\mathbb{B} = \{\mathbf{w}, \mathbf{f}\}$

boolesche Funktionen $f : \mathbb{B}^k \to \mathbb{B}$

Beispiele, die gleich verwendet werden:

x_1	x_2	$b_\neg(x_1)$	$b_\wedge(x_1, x_2)$	$b_\vee(x_1, x_2)$	$b_\rightarrow(x_1, x_2)$
f	**f**	**w**	**f**	**f**	**w**
f	**w**	**w**	**f**	**w**	**w**
w	**f**	**f**	**f**	**w**	**f**
w	**w**	**f**	**w**	**w**	**w**

Übliche Notation für boolesche Funktionen

$b_{\neg}(x)$	$\neg x$	$\bar{x}$	Negation bzw. Nicht
$b_{\wedge}(x, y)$	$x \wedge y$	$x \cdot y$	Und
$b_{\vee}(x, y)$	$x \vee y$	$x + y$	Oder
$b_{\rightarrow}(x, y)$			Implikation

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

Man kann die meisten booleschen Funktionen aus wenigen „zusammensetzen“

Beispiel

- $\mathbb{B}^2 \to \mathbb{B} : (x, y) \mapsto (\neg x) \vee x$
- Abbildung, die konstant **w** ist

für jedes $x \in \mathbb{B}$ und $y \in \mathbb{B}$
$b_{\rightarrow}(x, y) = (\neg x) \vee y$

x	y	$\neg x$	$(\neg x) \vee y$	$b_{\rightarrow}(x, y)$
f	**f**	**w**	**w**	**w**
f	**w**	**w**	**w**	**w**
w	**f**	**f**	**f**	**f**
w	**w**	**f**	**w**	**w**

Wo sind wir?

Ziel: Bedeutung einer aussagenlogischen Formel — eine boolesche Funktion

Es sei V eine Menge von Aussagevariablen

Interpretation $I : V \to \mathbb{B}$

- $\mathbb{B}^V$ Menge aller Intepretationen

als Tabelle z. B.

P_1	P_2	P_3
f	**f**	**f**
f	**f**	**w**
f	**w**	**f**
f	**w**	**w**
w	**f**	**f**
w	**f**	**w**
w	**w**	**f**
w	**w**	**w**

Auswertung von Formeln

Es sei $I : V \to \mathbb{B}$ eine Interpretation.

für jede aussagenlogische Formel F definiere $val_I(F)$ so:

für jedes $X \in V$ und jede $G, H \in For_{AL}$ sei

$$\begin{aligned}
val_I(X) &= I(X) \\
val_I(\neg G) &= b_\neg(val_I(G)) \\
val_I(G \wedge H) &= b_\wedge(val_I(G), val_I(H)) \\
val_I(G \vee H) &= b_\vee(val_I(G) val_I(H)) \\
val_I(G \to H) &= b_\to(val_I(G), val_I(H))
\end{aligned}$$

Auswertung von Formeln — ein Beispiel

Interpretation I mit $I(\mathtt{P}) = \mathbf{w}$ und $I(\mathtt{Q}) = \mathbf{f}$

Formel $\neg(\mathtt{P} \wedge \mathtt{Q})$

berechne $val_I(G)$ durch schrittweise Anwendung der Definition:

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

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**

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

- $\neg P \vee \neg Q$ und $\neg(P \wedge Q)$
- $\neg\neg P$ und P
- $P \rightarrow Q$ und $(\neg P) \vee Q$

informelle Überlegung zum letzten Fall

- „Gegenteil“ von $P \rightarrow Q$: $(P \wedge \neg Q)$
- also $P \rightarrow Q$ äquivalent zu $\neg(P \wedge \neg Q)$
- äquivalent zu $(\neg P) \vee (\neg\neg Q)$
- äquivalent zu $(\neg P) \vee Q$

Kleine Randbemerkung —
Auffassung einer Formel als Abbildung

$val_I(G)$ definiert für jedes I und jedes G

wir haben

$$\mathbb{B}^V \to \mathbb{B} : I \mapsto val_I(G)\ .$$

Konsequenz: $G = \mathtt{P}_0 \wedge \mathtt{P}_0$ und $H = \mathtt{P}_2 \wedge \mathtt{P}_2$ *nicht* äquivalent

- betrachte Interpretation I mit $I(\mathtt{P}_0) = \mathbf{w}$ und $I(\mathtt{P}_2) = \mathbf{f}$
- $val_I(G) = \mathbf{w}$, aber $val_I(H) = \mathbf{f}$.

Kleine Randbemerkung — Auffassung einer Formel als Abbildung

$val_I(G)$ definiert für jedes I und jedes G

wir haben

$$\mathbb{B}^V \to \mathbb{B} : I \mapsto val_I(G) \ .$$

Konsequenz: $G = \mathtt{P}_0 \land \mathtt{P}_0$ und $H = \mathtt{P}_2 \land \mathtt{P}_2$ *nicht* äquivalent

- betrachte Interpretation I mit $I(\mathtt{P}_0) = \mathbf{w}$ und $I(\mathtt{P}_2) = \mathbf{f}$
- $val_I(G) = \mathbf{w}$, aber $val_I(H) = \mathbf{f}$.

wollen die „Namen" der Aussagevariablen „vergessen"

$$\mathbb{B}^k \to \mathbb{B} : x \mapsto val_{I_x}(G) \ .$$

Kleine Randbemerkung — Auffassung einer Formel als Abbildung

$val_I(G)$ definiert für jedes I und jedes G

wir haben

$$\mathbb{B}^V \to \mathbb{B} : I \mapsto val_I(G) \ .$$

Konsequenz: $G = \mathtt{P}_0 \land \mathtt{P}_0$ und $H = \mathtt{P}_2 \land \mathtt{P}_2$ *nicht* äquivalent

- betrachte Interpretation I mit $I(\mathtt{P}_0) = \mathbf{w}$ und $I(\mathtt{P}_2) = \mathbf{f}$
- $val_I(G) = \mathbf{w}$, aber $val_I(H) = \mathbf{f}$.

sei $V = \{\mathtt{P}_{i_1}, \ldots, \mathtt{P}_{i_k}\}$ mit $i_1 < i_2 < \cdots < x_k$

definiere für jedes $x = (x_1, \ldots, x_k) \in \mathbb{B}^k$

$$I_x : \mathtt{P}_{i_j} \mapsto x_j \ .$$

Kleine Randbemerkung —
Auffassung einer Formel als Abbildung

$val_I(G)$ definiert für jedes I und jedes G

wir haben

$$\mathbb{B}^V \to \mathbb{B} : I \mapsto val_I(G) \ .$$

Konsequenz: $G = \mathtt{P}_0 \wedge \mathtt{P}_0$ und $H = \mathtt{P}_2 \wedge \mathtt{P}_2$ *nicht* äquivalent

- betrachte Interpretation I mit $I(\mathtt{P}_0) = \mathbf{w}$ und $I(\mathtt{P}_2) = \mathbf{f}$
- $val_I(G) = \mathbf{w}$, aber $val_I(H) = \mathbf{f}$.

sei $V = \{\mathtt{P}_{i_1}, \dots, \mathtt{P}_{i_k}\}$ mit $i_1 < i_2 < \cdots < x_k$

definiere für jedes $x = (x_1, \dots, x_m) \in \mathbb{B}^m$ mit $m \geq k$

$$I_x : \mathtt{P}_{i_j} \mapsto x_j \ .$$

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. `P ∨ ¬P`
- z. B. `P → (Q → P)`

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

- in einigen Anwendungen wichtig
- für manche Formeln einfach, für andere anscheinend nicht
  - `(P ∧ ¬Q) ∨ (¬P ∧ R)`
  - `(P ∨ ¬Q) ∧ (¬P ∨ R)`
- mehr in „Theoretische Grundlagen der Informatik“

Tautologien — viele Beispiele auf ein Mal

betrachte $G \leftrightarrow H$

- Abkürzung für $G \rightarrow H \wedge H \rightarrow G$

für jedes I ist

$$\begin{aligned} val_I(G \rightarrow H \wedge H \rightarrow G) &= b_\wedge(val_I(G \rightarrow H), val_I(H \rightarrow G)) \\ &= b_\wedge(b_\rightarrow(val_I(G), val_I(H)), \\ &\qquad b_\rightarrow(val_I(H), val_I(G))) \end{aligned}$$

wenn $G \equiv H$, also $val_I(G) = val_I(H)$ für jedes I

$$\begin{aligned} \text{dann } val_I(G \leftrightarrow H) &= b_\wedge(b_\rightarrow(val_I(G), val_I(G)), \\ &\qquad b_\rightarrow(val_I(G), val_I(G))) \\ &= b_\wedge(\mathbf{w}, \mathbf{w}) = \mathbf{w} \end{aligned}$$

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

$\neg\neg G \leftrightarrow G$

$(G \rightarrow H) \leftrightarrow (\neg G \vee H)$

$(G \rightarrow H) \leftrightarrow (\neg H \rightarrow \neg G)$

$(G \wedge H) \leftrightarrow \neg(\neg G \vee \neg H)$ 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 anderer Bauart

für $G, H, K \in For_{AL}$ sind z. B. auch

- $G \to G$
- $\neg G \vee G$
- $G \to (H \to G)$
- $(G \to (H \to K)) \to ((G \to H) \to (G \to K))$
- $(\neg H \to \neg G) \to ((\neg H \to G) \to H)$

alles Tautologien

Wo sind wir?

Kalkül — ein System für Beweise

allgemein

- Alphabet A
- syntaktisch korrekte Formeln $For \subseteq A^*$
- *Axiome* $Ax \subseteq For$,
- *Schlussregeln* $R \subseteq For_{AL}^k$

Aussagenkalkül für Aussagenlogik

- Alphabet A_{AL}
- syntaktisch korrekte Formeln $For_{AL} \subseteq A_{AL}^*$
- *Axiome* $Ax_{AL} \subseteq A_{AL}$,
- Schlussregel *Modus Ponens* $MP \subseteq For_{AL}^3$

Aussagenkalkül

Axiome

$$
\begin{aligned}
Ax_{AL} = &\left\{(G \to (H \to G)) \;\middle|\; G, H \in For_{AL}\right\} \\
&\cup \left\{(G \to (H \to K)) \to ((G \to H) \to (G \to K)) \;\middle|\; G, H, K \in For_{AL}\right\} \\
&\cup \left\{(\neg H \to \neg G) \to ((\neg H \to G) \to H) \;\middle|\; G, H \in For_{AL}\right\}
\end{aligned}
$$

- kurz Ax_{AL1}, Ax_{AL2} und Ax_{AL3} für die drei Teilmengen

Modus Ponens $MP \subseteq For_{AL}^3$

- $MP = \{(G \to H, G, H) \mid G, H \in For_{AL}\}$
- $MP: \quad \dfrac{G \to H \qquad G}{H}$

Ableitungen — formal gefasst

Ableitungen nutzen Prämissen, Axiome und Schlussregeln

$\Gamma \subseteq For_{AL}$ *Hypothesen* oder *Prämissen* und
G eine Formel

Ableitung von G aus Γ

- endliche Folge $(G_1, \ldots, G_n)$ von Formeln mit
- $G_n = G$ (oder weiter vorne) und
- für jedes G_i trifft einer der folgenden Fälle zu:
  - Axiom $G_i \in Ax_{AL}$,
  - Prämisse $G_i \in \Gamma$
  - oder es gibt Indizes i_1 und i_2 echt kleiner i, für die gilt: $(Gi_1, G_{i_2}, G_i) \in MP$.

geschrieben $\Gamma \vdash G$

Beweis — formal gefasst

Beweis von G: Ableitung aus $\Gamma = \{\}$

- geschrieben $\vdash G$
- G heißt *Theorem* des Kalküls

Beweis — erstes Beispiel $\mathtt{P} \to \mathtt{P}$

1.	$(\mathtt{P} \to ((\mathtt{P} \to \mathtt{P}) \to \mathtt{P})) \to ((\mathtt{P} \to (\mathtt{P} \to \mathtt{P})) \to (\mathtt{P} \to \mathtt{P}))$	Ax_{AL2}
2.	$\mathtt{P} \to ((\mathtt{P} \to \mathtt{P}) \to \mathtt{P})$	Ax_{AL1}
3.	$(\mathtt{P} \to (\mathtt{P} \to \mathtt{P})) \to (\mathtt{P} \to \mathtt{P})$	$MP(1, 2)$
4.	$\mathtt{P} \to (\mathtt{P} \to \mathtt{P})$	Ax_{AL1}
5.	$\mathtt{P} \to \mathtt{P}$	$MP(3, 4)$

analog für jede Formel G

- ein Beweis„schema“

Beweis — zweites Beispiel $(\neg P \rightarrow P) \rightarrow P$

1.	$(\neg P \rightarrow \neg P) \rightarrow ((\neg P \rightarrow P) \rightarrow P)$	Ax_{AL3}
2.	$(\neg P \rightarrow \neg P)$	Beispiel von eben
3.	$(\neg P \rightarrow P) \rightarrow P$	$MP(1,2)$

genaugenommen statt Zeile 2 die fünf Zeilen von eben

Auch Beweise strukturiert man!

Modus Ponens „erhält Allgemeingültigkeit“

Lemma

Wenn sowohl $G \rightarrow H$ als auch G Tautologien sind, dann ist auch H eine Tautologie.

Beweis

- wenn $G \rightarrow H$ Tautologie, dann gilt für jedes I:

$$\mathbf{w} = val_I(G \rightarrow H) = b_{\rightarrow}(val_I(G), val_I(H)) \ .$$

- da G Tautologie, ist $val_I(G) = \mathbf{w}$ und folglich

$$b_{\rightarrow}(val_I(G), val_I(H)) = b_{\rightarrow}(\mathbf{w}, val_I(H)) = val_I(H)$$

- also für jede Bewertung I: $\mathbf{w} = val_I(H)$
- also ist H Tautologie

Alle Theorem des Aussagenkalküls sind Tautologien

alle Axiome sind Tautologien

Modus Ponens erhält Allgemeingültigkeit

die umgekehrte Richtung gilt auch

schwieriger zu beweisen:

Lemma
Jede Tautologie ist im Aussagenkalkül beweisbar.

insgesamt

Theorem
Für jede Formel $G \in For_{AL}$
gilt $\models G$ *genau dann, wenn* $\vdash G$ *gilt.*

Ein Beispiel für die Nützlichkeit des Kalküls

Theorem

Für jedes $G \in For_{AL}$ und jedes $H \in For_{AL}$ gilt $G \vdash H$ genau dann, wenn $\vdash (G \to H)$.

einfache Richtung:
wenn $\vdash (G \to H)$, dann $G \vdash H$

- es sei $(G_1, \ldots, G_n)$ ein Beweis für $\vdash (G \to H)$ mit $G_n = (G \to H)$
- Ableitung für $G \vdash H$?
  verlängere die Folge um zwei Formeln
  - $G_{n+1} = G$ Prämisse
  - $G_{n+2} = H$ *MP* aus G_n und G_{n+1}

umgekehrte Richtung: auf der nächsten Folie

Fortsetzung des Beweises

Zeige: Wenn $G \vdash H$ dann $\vdash (G \to H)$.

- es sei $(G_1, \ldots, G_n)$ ein Ableitung für $G \vdash H$
- konstruieren Beweis $(H_1, \ldots, H_m)$ für $\vdash (G \to H)$

Ziel: für jedes G_i ist ein $H_{i'} = (G \to G_i)$

- wenn G_i Axiom, drei Formeln
  - $(G_i \to (G \to G_i))$ $\quad Ax_{AL1}$
  - G_i $\quad$ Axiom
  - MP aus diesen beiden Formeln
- wenn $G_i = G$, Formeln für Beweis der Tautologie
  - $(G_i \to G_i)$
- dritter Fall …

Fortsetzung des Beweises

Zeige: Wenn $G \vdash H$ dann $\vdash (G \to H)$.

- es sei $(G_1, \ldots, G_n)$ ein Ableitung für $G \vdash H$
- konstruieren Beweis $(H_1, \ldots, H_m)$ für $\vdash (G \to H)$

Ziel: für jedes G_i ist ein $H_{i'} = (G \to G_i)$

- wenn $G_i = K_2$ durch *MP* aus $G_{i_1} = K_1 \to K_2$ und $G_{i_2} = K_1$
  - dann schon abgeleitet
  - $G \to G_{i_1}$
  - $G \to G_{i_2}$
  - $(G \to (K_1 \to K_2)) \to ((G \to K_1) \to (G \to K_2)) \quad Ax_{AL3}$
    $= (G \to G_{i_1}) \to ((G \to G_{i_2}) \to (G \to G_i))$
  - zweimal *MP* liefert $G \to G_i$

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