1 Aussagenlogik

Aussage

Eine Aussage ist ein Satz, der entweder wahr oder falsch ist, also nie beides zugleich. Wahre Aussagen haben den Wahrheitswert w und falsche Aussagen den Wahrheitswert f.

OSI-Schicht	TCP-IP	Prot.	Einheit
Anwendungsschicht	Anwendungs-schicht	FTP, HTTP, SMPT	Daten
Darstellungsschicht			
Kommunikations-steuerungsschicht			
Transportschicht	Transport-schicht	TCP, UDP	Segmente
Vermittlungsschicht	Internet-schicht	IP	Pakete
Sicherungsschicht	Netzwerk-schicht	Ethernet, Token Ring	Frames
Bitübertragungsschicht			Bits

Belegung von Variablen

Sei $\mathscr{A}_B(F) = f$. Dann ist stets $\mathscr{A}_B(F \Rightarrow G) = w$

Formelbeweis über Belegung

Wenn $F \wedge G$ eine Tautologie ist, dann (und nur dann) ist F eine Tautologie und G auch. Hinweis: In dem Lemma stecken zwei Teilaussagen, die beide zu beweisen sind: 1. Wenn $F \wedge G$ eine Tautologie ist, dann ist F eine Tautologie und G auch. 2. Umgekehrt: Sind F und G Tautologien, dann ist auch $F \wedge G$ eine. *Beweis.* 1. Annahme: $F \wedge G$ sei eine Tautologie. Dann: Für jede Belegung B wertet $F \wedge G$ zu wahr aus. Dann: Das ist nur der Fall, wenn sowohl F als auch G (für jedes B) zu wahr auswerten. Dann: Für jede Belegung B wertet F zu wahr aus. Und: Für jede Belegung B wertet G zu wahr aus. Dann: F ist Tautologie und G ist Tautologie. 2. Annahme: F ist Tautologie und G ist Tautologie. Dann: Für jede Belegung B_1 wertet F zu wahr aus. Und: Für jede Belegung B_2 wertet G zu wahr aus. Dann: Für jede Belegung B wertet $F \wedge G$ zu wahr aus. Dann: $F \wedge G$ ist eine Tautologie.

Äquivalenz und Folgerung

$p \equiv q$ gilt genau dann, wenn sowohl $p \models q$ als auch $q \models p$ gelten. *Beweis.* $p \equiv q$ GDW $p \Leftrightarrow q$ ist Tautologie nach Def. von $\equiv$ GDW $(p \Rightarrow q) \wedge (q \Rightarrow p)$ ist Tautologie GDW $(p \Rightarrow q)$ ist Tautologie und $(q \Rightarrow p)$ ist Tautologie GDW $(p \models q)$ gilt und $q \models p$ gilt.

Substitution

Ersetzt man in einer Formel eine beliebige Teilformel F durch eine logisch äquivalente Teilformel F', so verändert sich der Wahrheitswerteverlauf der Gesamtformel nicht. Man kann Formeln also vereinfachen, indem man Teilformeln durch äquivalente (einfachere) Teilformeln ersetzt.

Universum

Die freien Variablen in einer Aussagenform können durch Objekte aus einer als Universum bezeichneten Gesamtheit wie $\mathbb{N}, \mathbb{R}, \mathbb{Z}, \mathbb{Q}$ ersetzt werden.

Tautologien

$(p \wedge q) \Rightarrow p$ bzw. $p \Rightarrow (p \vee q)$
$(q \Rightarrow p) \vee (\neg q \Rightarrow p)$
$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$
$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ (Kontraposition)
$(p \wedge (p \Rightarrow q)) \Rightarrow q$ (Modus Ponens)
$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
$((p \Rightarrow q) \wedge (p \Rightarrow r)) \Rightarrow (p \Rightarrow (q \wedge r))$
$((p \Rightarrow q) \wedge (q \Rightarrow p)) \Leftrightarrow (p \Leftrightarrow q)$

Nützliche Äquivalenzen

Kommutativität:
$(p \wedge q) \equiv (q \wedge p)$
$(p \vee q) \equiv (q \vee p)$
Assoziativität:
$(p \wedge (q \wedge r)) \equiv ((p \wedge q) \wedge r)$
$(p \vee (q \vee r)) \equiv ((p \vee q) \vee r)$
Distributivität:
$(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$
$(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$
Idempotenz:
$(p \wedge p) \equiv p$
$(p \vee p) \equiv p$
Doppelnegation:
$\neg(\neg p) \equiv p$
de Morgans Regeln:
$\neg(p \wedge q) \equiv ((\neg p) \vee (\neg q))$
$\neg(p \vee q) \equiv ((\neg p) \wedge (\neg q))$
Definition Implikation:
$(p \Rightarrow q) \equiv (\neg p \vee q)$
Tautologieregeln:
$(p \wedge q) \equiv p$ (falls q eine Tautologie ist)
$(p \vee q) \equiv q$
Kontradiktionsregeln:
$(p \wedge q) \equiv q$ (falls q eine Kontradiktion ist)
$(p \vee q) \equiv p$
Absorptionsregeln:
$(p \wedge (p \vee q)) \equiv p$
$(p \vee (p \wedge q)) \equiv p$
Prinzip vom ausgeschlossenen Dritten:
$p \vee (\neg p) \equiv w$
Prinzip vom ausgeschlossenen Widerspruch:
$p \wedge (\neg p) \equiv f$

Äquivalenzen von quant. Aussagen

Negationsregeln:
$\neg \forall x : p(x) \equiv \exists x : (\neg p(x))$
$\neg \exists x : p(x) \equiv \forall x : (\neg p(x))$
Ausklammerregeln:
$(\forall x : p(x) \wedge \forall y : q(y)) \equiv \forall z : (p(z) \wedge q(z))$
$(\exists x : p(x) \wedge \exists y : q(y)) \equiv \exists z : (p(z) \wedge q(z))$
Vertauschungsregeln
$\forall x \forall y : p(x,y) \equiv \forall y \forall x : p(x,y)$
$\exists x \exists y : p(x,y) \equiv \forall y \exists x : p(x,y)$

Äquivalenzumformung

Wir demonstrieren an der Formel $\neg(\neg p \wedge q) \wedge (p \vee q)$, wie man mit Hilfe der aufgelisteten logischen Äquivalenzen tatsächlich zu Vereinfachungen kommen kann:

$\neg(\neg p \wedge q) \wedge (p \vee q)$
$\equiv (\neg(\neg p) \vee (\neg q)) \wedge (p \vee q)$ de Morgan
$\equiv (p \vee (\neg q)) \wedge (p \vee q)$ Doppelnegation
$\equiv p \vee ((\neg q) \wedge q)$ Distributivität v.r.n.l.
$\equiv p \vee (q \wedge (\neg q))$ Kommutativität
$\equiv p \vee f$ Prinzip v. ausgeschl. Widerspruch
$\equiv p$ Kontradiktionsregel

Quantifizierte Aussagen

Sei $p(x)$ eine Aussageform über dem Universum U. $\exists x : p(x)$ ist wahr genau dann, wenn ein u in U existiert, so dass $p(u)$ wahr ist. $\forall x : p(x)$ ist wahr genau dann, wenn $p(u)$ für jedes u aus U wahr ist.

2 Beweistechniken

Direkter Beweis

Beim direkten Beweis wird Schritt für Schritt mittels *Wenn, Dann* bewiesen.

Kontraposition

Da $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ kann man die Aussage auch mittels Kontraposition beweisen.

Widerspruch

Beim Widerspruchsbeweis wird Gegenteil angenommen und in einen Widerspruch geführt. Also muss die ursprüngliche Aussage wahr sein.

Äquivalenzbeweis

Beweis über zeigen der Hin- und Rückrichtung.

Fallunterscheidung

Beweis aller möglichen Fälle.

Induktionsbeweis

Induktionsanfang (n kleinste Zahl):
Induktionsbehauptung: Aussage gelte für beliebiges aber festes $n \in \mathbb{N}$ mit $n \geq$ kleinste Zahl.
Induktionsschluss ($n \Longrightarrow n+1$): Zu zeigen ist also $n+1$ einsetzen $\Rightarrow$ Aussage gilt auch, *mit Benutzung von Induktionsbehauptung*.

3 Relationen

Binäre Relation

Eine binäre Relation R ist eine Menge von Paaren $(a,b) \in A \times B$.
$aRb \Leftrightarrow (a,b) \in R$ bzw. $a(\neg R)b \Leftrightarrow (a,b) \notin R$
Beispiele:
Teilerrelation (nTm): $P_3 := \{(n, m+3) \mid n, m \in \mathbb{N}\} = \{(1,4),(2,5),(3,6),...\}$
Relation $\subset$ über $\mathscr{P}(M)$ für $M = \{1,2\}$:
$\{(\emptyset,\{1\}),(\emptyset,\{2\}),(\emptyset,\{1,2\}),(\{1\},\{1,2\}),$
$(\{2\},\{1,2\})\}$

Inverse Relation

Sei $R \subseteq A \times B$. Die inverse Relation zu R ist $R^{-1} = \{(y,x) \in B \times A \mid (x,y) \in R\}$. Also ist $R^{-1} \subseteq B \times A$.
Beispiel: Sei $R = \{(1,a),(1,c),(3,b)\}$ dann ist $R^{-1} = \{(a,1),(c,1),(b,3)\}$

Komposition

Seien $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$ zweistellige Relationen. Die Verknüpfung $(R \circ S) \subseteq (M_1 \times M_3)$ heißt Komposition der Relationen R, S.
$R \circ S := \{(x,z) \mid \exists y \in M_2 : (x,y) \in R \wedge (y,z) \in S\}$
Beispiel: Sei $R = \{(1,2),(2,5),(5,1)\}$, dann ist $R^2 = R \circ R = \{(1,5),(2,1),(5,2)\}$
Sei $R \subseteq \mathbb{N} \times \mathbb{N}$ mit $(n,m) \in R \Leftrightarrow m = 3n$ und $S \subseteq \mathbb{N} \times \mathbb{Z}$ mit $(n,z) \in S \Leftrightarrow z = -n$. Dann ist $R \circ S = \{(n,z) \mid z = -3n\} \subseteq \mathbb{N} \times \mathbb{Z}$

Eigenschaften von Operationen

$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
$(R \circ S)^{-1} = S^{-1} \circ R^{-1}$
$(R \cap S) \circ T \subseteq (R \circ T) \cap (S \circ T)$
$T \circ (R \cap S) \subseteq (T \circ R) \cap (T \circ S)$
$(R \cup S) \circ T = (R \circ T) \cup (S \circ T)$
$T \circ (R \cup S) = (T \circ R) \cup (T \circ S)$

Eigenschaften von Relationen

Reflexiv: $\forall a \in A : (a,a) \in R$
Symmetrisch: $\forall a,b \in A : (a,b) \in R \Rightarrow (b,a) \in R$
Antisymm.: $\forall a,b \in A : (a,b) \in R \wedge (b,a) \in R \Rightarrow a = b$
Transitiv: $\forall a,b,c \in A : (a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$
Total: $\forall a,b \in A : (a,b) \in R \vee (b,a) \in R$
Irreflexiv: $\forall a \in A : (a,a) \notin R$
Asymm.: $\forall a,b \in A : (a,b) \in R \Rightarrow (b,a) \notin R$
Alternativ: $\forall a,b \in A : (a,b) \in R \oplus (b,a) \in R$
Rechtseind.: $\forall a \in A : (a,b) \in R \wedge (a,c) \in R \Rightarrow b = c$
Linkseind.: $\forall a \in A : (b,a) \in R \wedge (c,a) \in R \Rightarrow b = c$
Eindeutig: R ist recht- und linkseindeutig.
Linkstotal: $\forall a \in A \exists b \in B : (a,b) \in R$
Rechtstotal: $\forall b \in B \exists a \in A : (a,b) \in R$

Äquivalenzrelation

Ist eine Relation $\sim$ reflexiv, symmetrisch und transitiv, heißt sie Äquivalenzrelation.

Äquivalenzklassen

Gegeben eine Äquivalenzrelation R über der Menge A. Dann ist für $a \in A$: $[a]_R = \{x \mid (a,x) \in R\}$ die Äquivalenzklasse von a.
(Äquivalente Elemente kommen in die gleiche Menge)
Beispiel (Restklassen):
$[4] = \{n \mid n \mod 3 = 4 \mod 3\} = [1]$
$[5] = \{n \mid n \mod 3 = 5 \mod 3\} = [2]$
$[6] = \{n \mid n \mod 3 = 6 \mod 3\} = [3]$

Zerlegungen, Partition

Eine Zerlegung (Partition) $\mathscr{Z}$ ist eine Einteilung von A in nicht leere, paarweise elementfremde Teilmengen, deren Vereinigung mit A übereinstimmt.
Beispiel: Sei $A = \{1,2,3,...,10\}$. Dann ist $\mathscr{Z}_\infty = \{\{1,3\},\{2,5,9\},\{4,10\},\{6,7,8\}\}$

Abschluss einer Relation

R^*_ϕ bildet die fehlenden Relationen mit der Eigenschaft ϕ, also alle Kombinationen aus A, die noch nicht in R sind.
Beispiel:
Sei $A = \{1,2,3\}$ und $R = \{(1,2),(2,3),(3,3)\}$. Dann ist $R^*_{refl} = R \cup \{(1,1),(2,2)\}$,
$R^*_{sym} = R \cup \{(2,1),(3,2)\}$, $R^*_{tra} = R \cup \{(1,3)\}$

Halbordunung

Eine Relation R, die reflexiv, antisymmetrisch und transitiv ist.