

Logik und Diskrete Strukturen

Kapitel 8: Weitere Logiken

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für Theoretische Informatik und Theorembeweisen

Sommersemester 2026

Basierend auf Folien von PD Dr. Jan Johannsen

Übersicht

Quantifizierte Aussagenlogik
Modallogik
Temporale Logik
Prädikatenlogik zweiter Stufe
Intuitionistische Logik

Quantifizierte Aussagenlogik

Erweiterung der Aussagenlogik um Quantoren.

Syntax der Aussagenlogik erweitert um:

- ▶ Ist F eine Formel und $x \in X$ eine Variable, dann sind $\forall x F$ und $\exists x F$ Formeln.

Semantik:

- ▶ $\llbracket \forall x F \rrbracket_{\alpha} = 1$
gdw. $\forall \varepsilon \in \mathbb{B} \llbracket F \rrbracket_{\alpha[x:=\varepsilon]} = 1$
gdw. $\llbracket F \rrbracket_{\alpha[x:=0]} = 1$ und $\llbracket F \rrbracket_{\alpha[x:=1]} = 1$
- ▶ $\llbracket \exists x F \rrbracket_{\alpha} = 1$
gdw. $\exists \varepsilon \in \mathbb{B} \llbracket F \rrbracket_{\alpha[x:=\varepsilon]} = 1$
gdw. $\llbracket F \rrbracket_{\alpha[x:=0]} = 1$ oder $\llbracket F \rrbracket_{\alpha[x:=1]} = 1$

QBF Solving

Eine geschlossene Formel F ist in **Pränex-KNF** (PKNF), wenn sie von der Form

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n G$$

ist, wobei $Q_i \in \{\forall, \exists\}$ ist, und G in KNF ist und keine Quantoren enthält.

Ein **QBF-Löser** ist ein Programm mit:

- ▶ Input: Formel F in PKNF
- ▶ Output: $\llbracket F \rrbracket$

Q-Resolution

Beweissystem zur Widerlegung falscher Formeln in PKNF,
Erweiterung der Resolution auf QBF.

Schlussregeln sind

Resolution

$$\frac{C \vee x \quad D \vee \bar{x}}{C \vee D}$$

wobei gilt: x ist $\exists$ -quantifiziert und $C \vee D$ ist keine Tautologie.

Reduktion

$$\frac{C \vee y}{C} \quad \frac{C \vee \bar{y}}{C}$$

wobei gilt: y ist $\forall$ -quantifiziert nach allen anderen Variablen in C .

Q-Resolution

Eine Q-Resolutions-Widerlegung einer Formel F in PKNF ist eine Folge $C_1, \dots, C_k$ von Klauseln mit:

- ▶ $C_k = 0$
- ▶ für jedes $i \leq k$ gilt eines der Folgenden:
 - ▶ C_i ist eine Klausel $C_i \in F$
 - ▶ es gibt $j_1, j_2 < i$ sodass C_i Resolvente von C_{j_1} und C_{j_2} ist
 - ▶ es gibt $j < i$ sodass C_i aus C_j durch Reduktion entsteht

Theorem

Es gibt eine Q-Resolutions-Widerlegung für F gdw. $\llbracket F \rrbracket = 0$.

Modallogik

Erweiterung der Aussagenlogik um Modal-Operatoren $\Box$ und $\Diamond$.

Syntax:

- Ist F eine Formel, dann sind $\Box F$ und $\Diamond F$ Formeln.

$\Box F$ bedeutet: F ist notwendig

$\Diamond F$ bedeutet: F ist möglich

Modallogik: Semantik

Interpretation $\mathcal{W}$ besteht aus

- ▶ Menge W mit ausgezeichnetem Element $w_0 \in W$
- ▶ Relation $R \subseteq W \times W$ auf W
- ▶ Bewertung $\alpha_w : X \rightarrow \mathbb{B}$ für jedes $w \in W$

Definition der Erfüllungtheit:

- ▶ $w \models x$ gdw. $\alpha_w(x) = 1$
- ▶ $w \models \Box F$ gdw. für alle $w' \in W$ mit $w R w'$ gilt $w' \models F$
- ▶ $w \models \Diamond F$ gdw. es ein $w' \in W$ gibt mit $w R w'$ und $w' \models F$

$\mathcal{W} \models F$ gdw. $w_0 \models F$.

Modallogik: Gesetze

Folgende Gesetze gelten:

- ▶ $\neg \Box F \equiv \Diamond \neg F$
- ▶ $\neg \Diamond F \equiv \Box \neg F$
- ▶ $\Box(F \wedge G) \equiv \Box F \wedge \Box G$
- ▶ $\Diamond(F \vee G) \equiv \Diamond F \vee \Diamond G$
- ▶ $\Diamond(F \wedge G)$ impliziert $\Diamond F \wedge \Diamond G$, aber nicht umgekehrt
- ▶ $\Box F \vee \Box G$ impliziert $\Box(F \vee G)$, aber nicht umgekehrt

Folgende Gesetze gelten nur für gewisse Relationen:

- ▶ $\Box F \rightarrow F$ wenn R reflexiv ist
- ▶ $\Box F \rightarrow \Box \Box F$ wenn R transitiv ist
- ▶ $\Box F \rightarrow \Diamond F$ wenn R links-total ist

Modallogik: Interpretationen

Andere Interpretationen der Modaloperatoren:

- ▶ Deontische Logik

 - $\Box F$: F ist geboten

 - $\Diamond F$: F ist erlaubt

- ▶ Epistemische Logik

 - $\Box F$: F ist bekannt

 - $\Diamond F$: F wird für möglich gehalten

- ▶ Beweisbarkeits-Logik

 - $\Box F$: F ist beweisbar

 - $\Diamond F$: F ist konsistent (widerspruchsfrei)

Temporale Logik

Beschreibung zeitlicher Abläufe eines Systems.

Syntax der Modallogik erweitert um:

- ▶ Ist F eine Formel, dann ist $\bigcirc F$ eine Formel.

$\Box F$ bedeutet: F gilt immer

$\Diamond F$ bedeutet: F gilt irgendwann

$\bigcirc F$ bedeutet: F gilt zum nächsten Zeitpunkt

Auffassung einer Interpretation $\mathcal{W}$:

- ▶ $w \in W$ sind Zustände eines Systems
- ▶ $w R w'$, wenn System von w in w' übergehen kann
- ▶ α_w ist der Wert der Komponenten im Zustand w

Temporale Logik: Semantik

Ein Ablauf $\vec{v} = v_0, v_1, v_2, \dots$ ist eine unendliche Folge von Zuständen mit $v_i R v_{i+1}$ für alle i .

$$\vec{v}_i := v_i, v_{i+1}, v_{i+2}, \dots$$

Definition der Erfüllungtheit:

- ▶ $\vec{v} \models x$ gdw. $\alpha_{v_0}(x) = 1$
- ▶ $\vec{v} \models \bigcirc F$ gdw. $\vec{v}_1 \models F$
- ▶ $\vec{v} \models \Box F$ gdw. für alle $j \geq 0$ gilt $\vec{v}_j \models F$
- ▶ $\vec{v} \models \Diamond F$ gdw. es ein $j \geq 0$ gibt mit $\vec{v}_j \models F$

$\mathcal{W} \models F$ gdw. es einen Lauf $\vec{v}$ in $\mathcal{W}$ gibt mit $v_0 = w_0$ und $\vec{v} \models F$.

Temporale Logik: Gesetze

Folgende Gesetze gelten:

$$\blacktriangleright \neg \bigcirc F \equiv \bigcirc \neg F$$

$$\blacktriangleright \bigcirc (F \wedge G) \equiv \bigcirc F \wedge \bigcirc G$$

$$\blacktriangleright \bigcirc (F \vee G) \equiv \bigcirc F \vee \bigcirc G$$

$$\blacktriangleright \Box F \equiv F \wedge \bigcirc \Box F$$

$$\blacktriangleright \Diamond F \equiv F \vee \bigcirc \Diamond F$$

$$\blacktriangleright \Box \Box F \equiv \Box F$$

$$\blacktriangleright \Diamond \Diamond F \equiv \Diamond F$$

$$\blacktriangleright \Diamond \Box \Diamond F \equiv \Box \Diamond F$$

$$\blacktriangleright \Box \Diamond \Box F \equiv \Diamond \Box F$$

Temporale Logik: Gesetze

Bisher: nur Aussagen über einen Ablauf

Lineare Temporale Logik (LTL)

Andere temporale Logik: CTL (Computation Tree Logic)

Explizite Pfadquantoren:

- ▶ $A\varphi$ heißt: φ gilt für alle Abläufe
- ▶ $E\varphi$ heißt: es gibt Ablauf, für den φ gilt

Bisher auch: nur Aussagen über die Zukunft.

Es gibt auch temporale Logiken mit Operatoren für die Vergangenheit.

Prädikatenlogik zweiter Stufe

Erweiterung der Prädikatenlogik um

- ▶ Variablen für k -stellige Prädikate
- ▶ Quantoren darüber

Für jedes $k \in \mathbb{N}$ bezeichnet $X^{(k)}$ eine Variable der Stelligkeit k .

Definition von Formeln der Sprache L erweitert um:

- ▶ Ist $X^{(k)}$ eine Variable der Stelligkeit k ,
und sind $t_1, \dots, t_k$ Terme,
dann ist $X^{(k)}(t_1, \dots, t_k)$ eine atomare Formel
- ▶ Ist F eine Formel und $X^{(k)}$ eine k -stellige Variable,
dann sind $\forall X^{(k)} F$ und $\exists X^{(k)} F$ Formeln.

Prädikatenlogik zweiter Stufe: Semantik

Eine Bewertung η weist jeder k -stelligen Variablen $X^{(k)}$ eine Relation $\eta(X^{(k)}) \subseteq M_A^k$ zu.

Definition des Wertes einer Formel erweitert um:

- Für Variable $X^{(k)}$ und Terme $t_1, \dots, t_k$ ist

$$\llbracket X^{(k)}(t_1, \dots, t_k) \rrbracket_{\eta}^A = \begin{cases} 1 & \text{falls } (\llbracket t_1 \rrbracket_{\eta}^A, \dots, \llbracket t_k \rrbracket_{\eta}^A) \in \eta(X^{(k)}) \\ 0 & \text{sonst} \end{cases}$$

- $\llbracket \forall X^{(k)} F \rrbracket_{\eta}^A = \begin{cases} 1 & \text{falls } \forall R \subseteq M_A^k \llbracket F \rrbracket_{(\eta[X^{(k)} := R])}^A = 1 \\ 0 & \text{sonst} \end{cases}$

- Analog für $\exists$

Prädikatenlogik zweiter Stufe: Eigenschaften

Betrachte folgende Formeln:

$$\blacktriangleright F_{irr} = \forall x \neg X^{(2)}(x, x)$$

$$\blacktriangleright F_{trans} = \forall x \forall y \forall z (X^{(2)}(x, y) \wedge X^{(2)}(y, z) \rightarrow X^{(2)}(x, z))$$

$$\blacktriangleright F_{max} = \forall x \exists y X^{(2)}(x, y)$$

$A \models \neg \exists X^{(2)} (F_{irr} \wedge F_{trans} \wedge F_{max})$ gdw. M_A endlich ist.

Theorem

Es gibt keine Formel G erster Stufe mit:

$$A \models G \text{ gdw. } M_A \text{ endlich ist}$$

Theorem

Es gibt keinen Beweiskalkül, in dem genau die allgemeingültigen Formeln zweiter Stufe herleitbar sind.

Intuitionistische Logik

Entstanden aus der mathematischen Grundlagenkrise im 19. Jahrhundert.

Nicht-konstruktive Beweisprinzipien werden abgelehnt:

- ▶ Beweis für $A \vee B$ soll entscheiden ob A oder B gilt.
- ▶ Daher nicht gültig: $F \vee \neg F$
- ▶ Beweis für $\exists x F$ nur durch Konstruktion eines t mit $F[x := t]$
- ▶ Daher nicht gültig: $\neg \forall x F \rightarrow \exists x \neg F$
- ▶ Auch nicht gültig: $\neg \neg F \rightarrow F$

Anwendungen in der Informatik:

- ▶ Extraktion von Programmen aus Beweisen
- ▶ Typsysteme und Semantik für funktionale Programmiersprachen

Intuitionistische Logik: Sequenzenkalkül

Sequenzen haben rechts höchstens eine Formel:

$$\Gamma \vdash A \quad \text{oder} \quad \Gamma \vdash$$

Regel ($\vee$ -R) wird ersetzt durch:

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} (\vee\text{-R1}) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} (\vee\text{-R2})$$

Damit sind folgende Sequenzen nicht herleitbar:

- ▶ $\vdash F \vee \neg F$
- ▶ $\neg\neg F \vdash F$
- ▶ $\neg\forall x F \vdash \exists x \neg F$

Ende der 13. Vorlesung