

Zusammenfassung Logik für Informatiker

© Tim Baumann, <http://timbaumann.info/uni-spicker>

Prädikatenlogik erster Stufe

Notation. Die Symbole x_0, x_1, \dots seien reserviert für die Verwendung als Variablennamen.

Def. Eine **Signatur** ist ein Paar $(\mathcal{F}, \mathcal{P})$, wobei \mathcal{F} und \mathcal{P} disjunkte, höchstens abzählbare Zeichenmengen sind. Dabei gibt es Folgen $(\mathcal{F}^n)_{n \in \mathbb{N}_0}$ und $(\mathcal{P}^n)_{n \in \mathbb{N}_0}$, sodass gilt:

$$\mathcal{F} = \bigsqcup_{n \in \mathbb{N}_0} \mathcal{F}^n, \quad \mathcal{P} = \bigsqcup_{n \in \mathbb{N}_0} \mathcal{P}^n.$$

Wir interpretieren \mathcal{F}^n als Menge der n -stelligen Funktionssymbole, \mathcal{F}^0 als Menge von Konstanten und \mathcal{P}^n als Menge der n -stelligen Prädikaten Symbole.

Def. Die Menge **Term** $_{\mathcal{F}, \mathcal{P}}$ ist die kleinste Menge mit

- $\{x_0, x_1, \dots\} \subset \text{Term}$
- $\forall n \in \mathbb{N}_0 : \forall f \in \mathcal{F}^n : \forall t_1, \dots, t_n \in \text{Term} : f(t_1, \dots, t_n) \in \text{Term}$

Def. Die Menge der **atomaren** $(\mathcal{F}, \mathcal{P})$ -**Formeln** ist induktiv definiert als die kleinste Menge $\text{At}_{\mathcal{F}, \mathcal{P}}$ mit

- $\forall t_1, t_2 \in \text{Term}_{\mathcal{F}, \mathcal{P}} : (t_1 = t_2) \in \text{At}_{\mathcal{F}, \mathcal{P}}$ (Logik mit Gleichheit)
- $\forall n \in \mathbb{N}_0 : \forall P \in \mathcal{P}^n : \forall t_1, \dots, t_n \in \text{Term}_{\mathcal{F}, \mathcal{P}} : P(t_1, \dots, t_n) \in \text{At}_{\mathcal{F}, \mathcal{P}}$

Notation. $\text{true} := p_0 \vee \neg p_0, \quad \text{false} := \neg \text{true} \quad \text{für } p_0 \in \mathcal{P}^0 \text{ fest.}$

Def. Die Menge der $(\mathcal{F}, \mathcal{P})$ -**Formeln** ist induktiv definiert als kleinste Menge $\text{For}_{\mathcal{F}, \mathcal{P}}$ mit

- $\text{At}_{\mathcal{F}, \mathcal{P}} \subset \text{For}_{\mathcal{F}, \mathcal{P}}$
- $\forall A \in \text{For}_{\mathcal{F}, \mathcal{P}} : \{\neg A, \forall x : A, \exists x : A\} \subset \text{For}_{\mathcal{F}, \mathcal{P}}$
- $\forall A, B \in \text{For}_{\mathcal{F}, \mathcal{P}} : \{A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B\} \subset \text{For}_{\mathcal{F}, \mathcal{P}}$

Def. Eine Interpretation I einer Signatur $(\mathcal{F}, \mathcal{P})$ besteht aus einer Menge $D = D_I$ und Zuordnungen

$$\overset{I}{-} : \prod_{n \in \mathbb{N}_0} \prod_{f \in \mathcal{F}^n} (D_I)^n \rightarrow D_I, \quad \overset{I}{-} : \prod_{n \in \mathbb{N}_0} \prod_{P \in \mathcal{P}^n} (D_I)^n \rightarrow \{F, T\}$$

Def. Eine Belegung β zu einer Interpretation I ist eine Funktion

$$\beta : \{x_0, x_1, \dots\} \rightarrow D_I.$$

Notation. Sei $\beta : \{x_0, x_1, \dots\} \rightarrow D_I$ eine Belegung zu einer Interpretation I , x eine Variable und $d \in D_I$. Dann setze

$$\beta_x^d : \{x_0, x_1, \dots\} \rightarrow D_I, \quad y \mapsto \begin{cases} d, & \text{falls } x = y \\ \beta(y), & \text{sonst} \end{cases}$$

Def. Die **Auswertung** eines Terms t unter I und β (geschrieben $t_{I, \beta}$) ist induktiv definiert als

- $x_{I, \beta} := \beta(x)$
- $f(t_1, \dots, t_n) := f^I((t_1)_{I, \beta}, \dots, (t_n)_{I, \beta})$

Def. Eine Interpretation I und eine Belegung β **erfüllen** eine Formel F , geschrieben $I, \beta \models F$, falls

$$\begin{aligned} I, \beta \models (t_1 = t_2) & \iff (t_1)_{I, \beta} = (t_2)_{I, \beta} \\ I, \beta \models P(t_1, \dots, t_n) & \iff P^I((t_1)_{I, \beta}, \dots, (t_n)_{I, \beta}) \\ I, \beta \models \neg A & \iff I, \beta \not\models A \\ I, \beta \models A \wedge B & \iff (I, \beta \models A) \wedge (I, \beta \models B) \\ I, \beta \models A \vee B & \iff (I, \beta \models A) \vee (I, \beta \models B) \\ I, \beta \models A \rightarrow B & \iff (I, \beta \not\models A) \vee (I, \beta \models B) \\ I, \beta \models A \leftrightarrow B & \iff ((I, \beta \not\models A) \wedge (I, \beta \not\models B)) \\ & \quad \vee ((I, \beta \models A) \wedge (I, \beta \models B)) \\ I, \beta \models \forall x : A & \iff \forall d \in D_I : I, \beta_x^d \models A \\ I, \beta \models \exists x : A & \iff \exists d \in D_I : I, \beta_x^d \models A \end{aligned}$$

Proposition. Es gilt für alle Interpretationen I , Belegungen β und Formeln A, B :

$$\begin{aligned} I, \beta \models A & \iff I, \beta \not\models \neg A \iff I, \beta \models \neg \neg A \\ I, \beta \models A \wedge B & \iff I, \beta \models \neg(A \rightarrow \neg B) \\ I, \beta \models A \vee B & \iff I, \beta \models \neg A \rightarrow B \\ I, \beta \models A \leftrightarrow B & \iff I, \beta \models (A \rightarrow B) \wedge (B \rightarrow A) \\ I, \beta \models \exists x : A & \iff I, \beta \models \neg \forall x : \neg A \end{aligned}$$

Def. Seien $A \in \text{For}$, $M \subset \text{For}$ und I eine Interpretation. Dann heißt I ein **Modell** von A bzw. M , falls

$$\begin{aligned} I \models A & \iff \text{für alle Belegungen } \beta \text{ gilt } I, \beta \models A, \\ I \models M & \iff \forall F \in M : I \models F. \end{aligned}$$

Notation. Für $M \subset \text{For}$, eine Interpretation I und eine Belegung β schreiben wir:

$$I, \beta \models M \iff \forall F \in M : I, \beta \models F$$

Def. Seien $A, B \in \text{For}$. Man sagt, B **folgt** aus A (geschrieben $A \models B$), falls für alle Interpretationen I und Belegungen β gilt:

$$I, \beta \models A \implies I, \beta \models B.$$

Falls $A \models B$ und $B \models A$ gilt, so heißen A und B **logisch äquivalent**, geschrieben $A \models B$.

Notation. $A_1, \dots, A_n \models A \iff \{A_1, \dots, A_n\} \models A$

Satz. Für alle Interpretationen I und $n \in \mathbb{N}$ gilt:

$$I \models \{A_1, \dots, A_n\} \iff I \models A_1 \wedge \dots \wedge A_n$$

Satz. Für alle $A, B \in \text{For}$ und $M \subset \text{For}$ gilt:

$$M \models A \rightarrow B \iff M \cup \{A\} \models B$$

Def. Eine Formel $A \in \text{For}$ heißt **Tautologie** oder **(allgemein-) gültig** (geschrieben $\models A$), falls $I \models A$ für alle Interpretationen I gilt.

Def. Eine Formel $A \in \text{For}$ heißt **erfüllbar**, wenn es eine Interpretation I und eine Belegung β mit $I, \beta \models A$ gibt. Falls es dies nicht gibt, so heißt A **unerfüllbar**.

Satz. Für $A \in \text{For}$ gilt:

$$\bullet \models A \implies A \text{ ist erfüllbar} \quad \bullet \models A \iff \emptyset \models A$$

Satz. Sei $A \in \text{For}$ und $M \subset \text{For}$. Dann gilt $M \models A$ genau dann, wenn $M \cup \{\neg A\}$ unerfüllbar ist. Insbesondere ist A genau dann gültig, wenn $\{\neg A\}$ unerfüllbar ist.

Def. **Universelle Formeln** sind Formeln, die sich nach den folgenden Regeln herleiten lassen:

$$\frac{A \text{ ist quantorenfrei}}{A} \quad \frac{A \quad B}{A \wedge B} \quad \frac{A \quad B}{A \vee B} \quad \frac{A}{\forall x : A}$$

Proposition. Sei I eine Teil-Interpretation zu J , β eine Belegung zu I und A eine universelle Formel. Dann gilt:

$$J, \beta \models A \implies I, \beta \models A.$$

Aussagenlogik

Def. Für $p \in \mathcal{P}^0$ heißen die Ausdrücke p und $\neg p$ **Literale**. Eine Disjunktion von Literalen heißt **Klausel**. Eine Formel ist in **konjunktiver Normalform (KNF)**, wenn sie eine Konjunktion von Klauseln ist.

Problem (SAT). Gegeben sei eine Formel in konjunktiver Normalform. Frage: Ist diese Formel erfüllbar?

Def. Eine Formel ist in **Negationsnormalform (NNF)**, wenn Negationen nur unmittelbar vor Atomen stehen.

Def. Der **Hilbert-Kalkül** besteht aus den Axiomen

$$\text{Ax}_1 := \{A \rightarrow (B \rightarrow A) \mid A, B \in \text{For}\}$$

$$\text{Ax}_2 := \{(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) \mid A, B, C \in \text{For}\}$$

$$\text{Ax}_3 := \{(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A) \mid A, B \in \text{For}\}$$

und der Schlussregel **Modus Ponens (MP)**

$$\frac{A \quad A \rightarrow B}{B}$$

Def. Eine Formel $F \in \text{For}$ ist aus $M \subset \text{For}$ **H-herleitbar**, notiert $M \vdash_H A$, wenn es eine Folge A_1, \dots, A_n in For gibt mit $A_n = A$, sodass für alle $i \in \{1, \dots, n\}$ gilt:

$$A_i \in \text{Ax}_1 \cup \text{Ax}_2 \cup \text{Ax}_3 \cup M \quad \text{oder} \quad \exists j, k < i : A_j = A_k \rightarrow A_i.$$

Def. $A \in \text{For}$ heißt **herleitbar**, notiert $\vdash A$, falls $\emptyset \vdash A$ gilt.

Beobachtung. Präfixe und Verkettungen von Herleitungen sind ebenfalls Herleitungen.

Proposition. • Aus $M \vdash A$ und $M \vdash A \rightarrow B$ folgt $M \vdash B$.

• Aus $M \vdash \neg A \rightarrow \neg B$ folgt $M \vdash B \rightarrow A$.

Satz (Deduktionstheorem). $M \vdash A \rightarrow B \iff M \cup \{A\} \vdash B$

Satz. Für alle $A, B, C \in \text{For}$ gilt:

$$\begin{aligned} \bullet \vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)) & \quad \bullet \vdash \neg A \rightarrow (A \rightarrow B) \\ \bullet \vdash \neg \neg A \rightarrow A & \quad \bullet \vdash A \rightarrow \neg \neg A & \quad \bullet \vdash (\neg A \rightarrow A) \rightarrow A \end{aligned}$$

Proposition. Es gilt:

$$\frac{A \rightarrow B \quad B \rightarrow C}{A \rightarrow C} \quad \frac{\neg \neg A}{A}$$

Satz (Korrektheitssatz). Sei $A \in \text{For}$ und $M \subset \text{For}$. Dann gilt

$$M \vdash A \implies M \models A.$$

Def. $M \subset \text{For}$ heißt **konsistent**, wenn für kein $A \in \text{For}$ zugleich $M \vdash A$ und $M \vdash \neg A$ gilt.

Lemma. • Ist M inkonsistent, so gilt $M \vdash B$ für alle $B \in \text{For}$.
• Für $A \in \text{For}$ gilt: $M \not\vdash A \implies M \cup \{A\}$ ist konsistent.

Lemma (Modell-Lemma). Jede konsistente Menge ist erfüllbar, d. h. sie besitzt ein Modell.

Satz (Vollständigkeitssatz). Sei $A \in \text{For}$ und $M \subset \text{For}$. Dann gilt

$$M \models A \implies M \vdash A.$$

Proposition. Sei $M \subset \text{For}$. Dann ist M genau dann erfüllbar, wenn M konsistent ist.

Satz (Endlichkeits- bzw. Kompaktheitssatz). Sei $A \in \text{For}$, $M \subset \text{For}$.

- Dann gilt $M \models A$ genau dann, wenn es eine endliche Teilmenge $M' \subset M$ mit $M' \models A$ gibt.
- Dann ist M genau dann erfüllbar, wenn jede endliche Teilmenge von M erfüllbar ist.

Hilbert-Kalkül für Prädikatenlogik

Proposition. Es gilt für alle $A \in \text{For}$, $M \subset \text{For}$:

$$M \models A \implies (\forall \text{ Interpretationen } I : I \models M \implies I \models A)$$

Achtung. Die Umkehrung gilt nicht!

Proposition. Sei $A \in \text{For}$. Dann gilt:

- $\forall x : A \models A$ • $A \models \forall x : A$ nicht (i. A.)

Def. Sei $A \in \text{For}$. Dann bezeichnet $\text{FV}(A)$ die Menge der **freien** Variablen und $\text{BV}(A)$ die Menge der **gebundenen** Variablen in A .

Def. Eine Formel $A \in \text{For}$ heißt **geschlossen**, falls $\text{FV}(A) = \emptyset$.

Def. • $\forall x : A$ heißt **Generalisierung** von $A \in \text{For}$.

- Ist $\text{FV}(A) = \{y_1, \dots, y_n\}$, so heißt jede der $n!$ Formeln $\forall y_1 : \forall y_2 : \dots \forall y_n : A$ ein **universeller Abschluss** von A .

Satz (Koinzidenzlemma). Seien $A, B \in \text{For}$, I eine Interpretation und β_1, β_2 Belegungen mit $\beta_1|_{\text{FV}(A)} = \beta_2|_{\text{FV}(A)}$. Dann gilt

$$I, \beta_1 \models A \iff I, \beta_2 \models A.$$

Korollar. Seien A, M geschlossen und β_1, β_2 Belegungen. Dann gilt

- $I, \beta_1 \models M \iff I, \beta_2 \models M$ • $I, \beta_1 \models M \iff I \models M$
- M ist erfüllbar $\iff M$ hat ein Modell
- $M \models A \iff (\forall \text{ Interpretationen } I : I \models M \iff I \models A)$

Proposition. • $I \models A \iff I \models \forall x : A$ • $\models A \iff \models \forall x : A$

Def. Sei x eine Variable und $t \in \text{Term}$ ein Term. Dann ist die Substitution $[t/x]$ für Terme und Formeln folgendermaßen definiert:

$$y[t/x] := \begin{cases} t, & \text{falls } y = x \\ y, & \text{sonst} \end{cases}$$

$$f(t_1, \dots, t_n)[t/x] := f(t_1[t/x], \dots, t_n[t/x]) \quad \text{für } f \in \mathcal{F}^n$$

$$P(t_1, \dots, t_n)[t/x] := P(t_1[t/x], \dots, t_n[t/x]) \quad \text{für } P \in \mathcal{P}^n$$

$$(t_1 = t_2)[t/x] := (t_1[t/x] = t_2[t/x])$$

$$(\neg A)[t/x] := \neg(A[t/x])$$

$$(A \rightarrow B)[t/x] := A[t/x] \rightarrow B[t/x]$$

$$(\forall y : A)[t/x] := \begin{cases} \forall y : A, & \text{falls } x = y \\ \forall y : (A[t/x]), & \text{sonst und falls } y \notin \text{FV}(t) \\ \forall z : (A[z/y][t/x]), & \text{sonst} \end{cases}$$

Im letzten Fall ist z eine frische Variable, d. h. $z \notin \text{FV}(t) \cup \text{FV}(A)$.

Def. Der **Hilbert-Kalkül** für Prädikatenlogik hat als Axiome für alle $A, B, C \in \text{For}$ und $t \in \text{Term}$ alle Generalisierungen von

$\text{Ax}_1, \text{Ax}_2, \text{Ax}_3$: wie zuvor

$\text{Ax}_4 : (\forall x : A) \rightarrow A[t/x]$ (**SP**ezialisierung)

$\text{Ax}_5 : A \rightarrow \forall x : A$, falls $x \notin \text{FV}(A)$ (**GE**neralisierung)

$\text{Ax}_6 : (\forall x : A \rightarrow B) \rightarrow ((\forall x : A) \rightarrow (\forall x : B))$ (**Distr. All**quantor)

$\text{Ax}_7 : x = x$ (**RE**flexivität)

$\text{Ax}_8 : (x = y) \rightarrow (A \rightarrow A')$ (**GL**eichheit),

wobei bei der letzten Regel A quantorenfrei ist und A' aus A durch Ersetzen eines oder mehrerer Vorkommen von x durch y entsteht. Außerdem gilt die Schlussregel **Modus Ponens**.

Satz (Deduktionstheorem). Wir beim Hilbert-Kalkül der Aussagenlogik gilt für $M \subset \text{For}$ und $A, B \in \text{For}$:

$$M \vdash A \rightarrow B \iff M \cup \{A\} \vdash B$$

Satz (Generalisierungstheorem). Sei $M \subset \text{For}$ und $A \in \text{For}$. Angenommen, es gilt $\forall B \in M : x \notin \text{FV}(B)$. Dann gilt $M \vdash \forall x : A$.

Korollar. $\vdash A \implies \vdash \forall x : A$

Proposition (α -Konversion). Sei $y \in \text{FV}(\forall x : A)$. Dann gilt

$$\vdash (\forall x : A) \rightarrow (\forall y : A[y/x]).$$

Satz (Korrektheit). Es gilt für alle $M \subset \text{For}$ und $A \in \text{For}$:

$$M \vdash A \implies M \models A.$$

Lemma. Für $M \subset \text{For}$ und $A \in \text{For}$ gilt:

- $M \not\vdash A \implies M \cup \{A\}$ ist konsistent.
- $M \not\vdash \forall x : A \implies M \cup \{\neg \forall x : A, \neg A[c/x]\}$ ist konsistent für jede Variable c , die nicht in M und A vorkommt.

Lemma (Modell-Lemma). konsistent \iff erfüllbar

Satz (Löwenheim-Skolem). Jede erfüllbare Menge M geschlossener Formeln hat ein höchstens abzählbares Modell bzw. im Falle von Logik ohne Gleichheit ein abzählbar unendliches Modell.

Satz (Vollständigkeit). Es gilt für alle $M \subset \text{For}$ und $A \in \text{For}$:

$$M \models A \implies M \vdash A.$$

Satz (Endlichkeits- bzw. Kompaktheitssatz der Prädikatenlogik). Sei $A \in \text{For}$, $M \subset \text{For}$.

- Dann gilt $M \models A$ genau dann, wenn es eine endliche Teilmenge $M' \subset M$ mit $M' \models A$ gibt.
- Dann ist M genau dann erfüllbar, wenn jede endliche Teilmenge von M erfüllbar ist.

Bemerkung. Die Menge der gültigen Formeln ist aufzählbar bzw. semi-entscheidbar.

Satz (Church). Das Gültigkeitsproblem der Prädikatenlogik erster Stufe ist unentscheidbar.

Korollar. Es gibt kein $A \in \text{For}$ mit

- $I \models A \iff D_I$ ist endlich.
- Bei Logik ohne Gleichheit: $I \models A \iff |D_I| = n$ für ein festes $n \in \mathbb{N}$.

Weitere Beweisverfahren

Def. Im **Gentzen-Kalkül** (\vdash_G) gelten die folgenden Schlussregeln:

	rechts		links
	$\frac{M \cup \{A\} \vdash_G B}{M \vdash_A \rightarrow B}$	Imp	$\frac{M \cup \{\neg C\} \vdash_G A \quad M \cup \{B\} \vdash_G C}{M \cup \{A \rightarrow B\} \vdash_G C}$
	$\frac{M \cup \{A\} \vdash_G \neg B}{M \cup \{B\} \vdash_G \neg A}$	Neg	$\frac{M \cup \{\neg B\} \vdash_G A}{M \cup \{\neg A\} \vdash_G B}$
	$\frac{M \vdash_G A \quad M \vdash_G B}{M \vdash_G A \wedge B}$	Kon	$\frac{M \cup \{A, B\} \vdash_G C}{M \cup \{A \wedge B\} \vdash_G C}$
	$\frac{M \cup \{\neg B\} \vdash_G A}{M \vdash_G A \vee B}$	Dis	$\frac{M \cup \{A\} \vdash_G C \quad M \cup \{B\} \vdash_G C}{M \cup \{A \vee B\} \vdash_G C}$

$$\frac{}{M \cup \{A\} \vdash_G A} \text{ (Axiom)}$$

Satz (Korrektheit, Vollständigkeit). Es gilt für alle $A \in \text{For}$ und $M \subset \text{For}$: $M \vdash_G A \iff M \models A$.

Notation. Für ein Literal l bezeichnet \bar{l} das **negierte Literal**, also

$$\bar{p} := \neg p, \quad \overline{\neg p} := p.$$

Def. Sei A eine Formel in KNF mit Klauseln K und K' , sodass ein Literal l existiert mit $l \in K$ und $\bar{l} \in K'$. Dann heißt

$$R = (K \setminus \{l\}) \cup (K' \setminus \{\bar{l}\}) \quad \text{Resolvente von } K \text{ und } K'.$$

Def. Ein **Resolutionsschritt** fügt eine Resolvente einer Formel in KNF der Formel hinzu. Die Formel, die aus einer Formel A durch mehrere Resolutionsschritte entsteht, sodass keine weiteren Resolutionsschritte möglich sind, wird mit $\text{Res}^*(A)$ bezeichnet.

Lemma. Sei A eine Formel in KNF mit Klauseln K und K' und einer Resolvente $R = (K \setminus \{l\}) \cup (K' \setminus \{\bar{l}\})$. Dann ist A genau dann erfüllbar, wenn $A \cup R$ es ist.

Satz (Resolutionssatz). Eine KNF-Formel A ist genau dann unerfüllbar, wenn $\emptyset \in \text{Res}^*(A)$.

Zusicherungskalkül

Def. Ein **Hoare-Tripel** hat die Form

$$\{A\} \ S \ \{B\},$$

wobei A und B prädikatenlogische Formeln, sogenannte **Zusicherungen**, und S eine Programmanweisung ist.

Def. • Ein Hoare-Tripel $\{A\} \ S \ \{B\}$ **gilt schwach**, wenn B nach Ausführung von S unter der Vorbedingung A gilt, falls S ohne Fehlerabbruch terminiert.
• Gilt das Hoare-Tripel schwach und sichert die Vorbedingung A die Terminierung ohne Fehler von S , so gilt das Tripel **streng**.

Def. Im **Zusicherungskalkül** (Hoare-Kalkül) gelten folgende Schlussregeln:

$$\begin{array}{c} \frac{\overline{\{B[E/x]\} \ x=E; \ \{B\}} \quad (=P)}{A \Rightarrow B \quad \{B\} \ S \ \{C\} \quad C \Rightarrow D} \quad (K) \quad \frac{\overline{\{D_E \wedge B[E/x]\} \ x=E; \ \{B\}} \quad (=T)}{\{A\} \ S \ \{B\} \quad \{B\} \ T \ \{C\}} \quad (sK) \\ \frac{\{A\} \ S \ \{D\}}{\{A\} \ S \ \{C\}} \quad \frac{\{A \wedge B\} \ S \ \{C\} \quad \{A \wedge \neg B\} \ T \ \{C\}}{\{A\} \text{ if } (B) \text{ then } S \text{ else } T \ \{C\}} \quad (\text{if}) \\ \frac{\{A \wedge B\} \ S \ \{A\}}{\{A\} \text{ while } (B) \text{ do } S \ \{A \wedge \neg B\}} \quad (\text{Wp}) \\ \frac{\forall z \in \mathbb{Z} : \{A \wedge B \wedge t = z\} \ S \ \{A \wedge t < z\} \quad A \wedge B \implies t \geq 0}{\{A\} \text{ while } (B) \text{ do } S \ \{A \wedge \neg B\}} \quad (\text{Wt}) \end{array}$$

Temporale Logik

Def. Ein **Ablauf** $\pi = s_0, s_1, \dots$ ist eine unendliche Folge von Zuständen aus einer Menge S mit einer Bewertung $L : S \rightarrow \mathfrak{P}(\mathcal{P})$.

Notation. $\pi^j := s_j, s_{j+1}, \dots$ heißt **j-tes Suffix** von π .

Def. Sei \mathcal{P} eine Menge von atomaren Formeln. Dann sind Formeln in (P)LTl (Propositional Linear Time Logic) über \mathcal{P} definiert als kleinste Menge TFor \mathcal{P} mit

- $\mathcal{P} \subset \text{TFor}_{\mathcal{P}}$ • $\forall A \in \text{TFor}_{\mathcal{P}} : \{\mathbf{GA}, \mathbf{FA}, \mathbf{XA}\} \subset \text{TFor}_{\mathcal{P}}$
- $\forall A, B \in \text{TFor}_{\mathcal{P}} : \{\neg A, A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B\} \subset \text{TFor}_{\mathcal{P}}$
- $\forall A, B \in \text{TFor}_{\mathcal{P}} : (A \mathbf{U} B) \in \text{TFor}_{\mathcal{P}}$

Def. Sei $\pi = s_0, s_1, \dots$ ein Ablauf. Eine Formel $A \in \text{TFor}$ gilt für π (π erfüllt A , $\pi \models A$), falls gilt:

$$\begin{array}{ll} \pi \models p & :\iff p \in L(s_0) \\ \pi \models \neg A & :\iff \pi \not\models A \\ \pi \models A \vee B & :\iff (\pi \models A) \vee (\pi \models B) \\ \pi \models \mathbf{XA} & :\iff \pi^1 \models A \\ \pi \models \mathbf{GA} & :\iff \forall j \in \mathbb{N}_0 : \pi^j \models A \\ \pi \models \mathbf{FA} & :\iff \exists j \in \mathbb{N}_0 : \pi^j \models A \\ \pi \models A \mathbf{U} B & :\iff \exists j \in \mathbb{N}_0 : \pi^j \models B \wedge (\forall i < j : \pi^i \models A) \end{array}$$

Def. Eine Formel $A \in \text{TFor}$ heißt **gültig** / **erfüllbar**, falls alle Abläufe / ein Ablauf A erfüllt.

Proposition. Für alle $A \in \text{TFor}$ gilt:

- $\mathbf{GA} \models \neg \mathbf{F} \neg A$ • $\mathbf{FA} \models \text{true} \mathbf{U} A$
- $A \mathbf{U} B \models \neg((\neg B) \mathbf{U} (\neg A \wedge \neg B)) \wedge \mathbf{FB}$

Satz. Für alle $A, B \in \text{TFor}$ gilt:

- $\models \mathbf{G}(A \rightarrow B) \rightarrow (\mathbf{GA} \rightarrow \mathbf{GB})$ • $\models \mathbf{XGA} \leftrightarrow \mathbf{GXA}$
- $\models (A \wedge \mathbf{G}(A \rightarrow \mathbf{XA})) \rightarrow \mathbf{GA}$ • $\models \mathbf{XFA} \rightarrow \mathbf{FA}$

Def. Eine **Kripke-Struktur** $K = (S, \rightarrow, L, s_0)$ besteht aus einer Menge S von Zuständen mit Startzustand s_0 , einer Bewertung $L : S \rightarrow \mathfrak{P}(\mathcal{P})$ und einer Transitionsrelation $\rightarrow \subset S \times S$, sodass $\forall s \in S : \exists s' \in S : s \rightarrow s'$ gilt.

Def. Ein **Ablauf** π von K ist eine unendliche Folge von Zuständen beginnend mit s_0 , also $\pi = s_0, s_1, s_2, \dots$ mit $\forall i \in \mathbb{N}_0 : s_i \rightarrow s_{i+1}$. Die Zustände eines solchen Ablaufs heißen **erreichbar**.

Def. Eine Kripke-Struktur K **erfüllt** $A \in \text{TFor}$, falls für alle Abläufe π von K gilt $\pi \models A$.

Def. Sei \mathcal{P} eine Menge von atomaren Formeln. Dann sind Formeln in CTL (Computation Tree Logic) über \mathcal{P} definiert als kleinste Menge CTFor \mathcal{P} mit

- $\forall A, B \in \text{TFor}_{\mathcal{P}} : \{\neg A, A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B\} \subset \text{CTFor}_{\mathcal{P}}$
- $\mathcal{P} \subset \text{CTFor}_{\mathcal{P}}$ • $\forall A, B \in \text{TFor}_{\mathcal{P}} : \{\mathbf{A}(A \mathbf{U} B), \mathbf{E}(A \mathbf{U} B)\} \subset \text{TFor}_{\mathcal{P}}$
- $\forall A \in \text{TFor}_{\mathcal{P}} : \{\mathbf{AGA}, \mathbf{AFA}, \mathbf{AXA}, \mathbf{EGA}, \mathbf{EFA}, \mathbf{EXA}\} \subset \text{TFor}_{\mathcal{P}}$

Def. Sei K eine Kripke-Struktur, s ein Zustand. Eine Formel $A \in \text{CTFor}$ **gilt** für (K, s) , falls (koinduktive Definition)

$$\begin{array}{ll} K, s \models p & :\iff p \in L(s) \\ K, s \models \neg A & :\iff K, s \not\models A \\ K, s \models A \vee & :\iff (K, s \models A) \vee (K, s \models B) \\ K, s \models \mathbf{AXB} & :\iff \forall s' \in S : (s \rightarrow s') \Rightarrow K, s' \models B \\ K, s \models \mathbf{EXB} & :\iff \exists s' \in S : (s \rightarrow s') \wedge (K, s' \models B) \\ K, s \models \mathbf{AGB} & :\iff K, s \models B \wedge \forall s' \in S : (s \rightarrow s') \Rightarrow K, s' \models \mathbf{AGB} \\ K, s \models \mathbf{EGB} & :\iff K, s \models B \wedge \exists s' \in S : (s \rightarrow s') \wedge (K, s' \models \mathbf{EGB}) \\ K, s \models \mathbf{AFB} & :\iff \forall \text{Abläufe } \pi = s_0, s_1, s_2, \dots \text{ von } K \text{ mit } s_0 = s : \\ & \quad \exists j \in \mathbb{N}_0 : K, s_j \models B \end{array}$$

$$\begin{array}{ll} K, s \models \mathbf{EFB} & :\iff \exists \text{Ablauf } \pi = s_0, s_1, s_2, \dots \text{ von } K \text{ mit } s_0 = s : \\ & \quad \exists j \in \mathbb{N}_0 : K, s_j \models B \\ K, s \models \mathbf{A}(B \mathbf{U} C) & :\iff \forall \text{Abläufe } \pi = s_0, s_1, s_2, \dots \text{ von } K \text{ mit } s_0 = s : \\ & \quad \exists j \in \mathbb{N}_0 : (K, s_j \models C) \wedge (\forall i < j : K, s_i \models B) \\ K, s \models \mathbf{E}(B \mathbf{U} C) & :\iff \exists \text{Ablauf } \pi = s_0, s_1, s_2, \dots \text{ von } K \text{ mit } s_0 = s : \\ & \quad \exists j \in \mathbb{N}_0 : (K, s_j \models C) \wedge (\forall i < j : K, s_i \models B) \end{array}$$

Notation. $K \models A :\iff K, s_0 \models A$, wobei s_0 Startzustand von K .

Def. Eine Formel $A \in \text{CTFor}$ heißt **gültig** / **erfüllbar**, wenn alle Kripke-Strukturen / eine Kripke-Struktur A erfüllen / erfüllt.

Satz. Für alle $B, C \in \text{CTFor}$ gilt:

- $\models (B \wedge \mathbf{AG}(B \rightarrow \mathbf{AXB})) \rightarrow \mathbf{AGB}$
- $\models \mathbf{AX}(B \rightarrow C) \wedge \mathbf{AXB} \rightarrow \mathbf{AXC}$

Satz. Für alle $A, B \in \text{CTFor}$ gilt:

- $\mathbf{AGB} \models \neg \mathbf{EF} \neg B$ • $\mathbf{EGB} \models \neg \mathbf{AF} \neg B$
- $\mathbf{EFB} \models \mathbf{E}(\text{true} \mathbf{U} B)$ • $\mathbf{AFB} \models \mathbf{A}(\text{true} \mathbf{U} B)$
- $\mathbf{AXB} \models \neg \mathbf{EX} \neg B$ • $\mathbf{A}(B \mathbf{U} C) \models \neg \mathbf{E}(\neg C \mathbf{U} (\neg C \wedge \neg B)) \wedge \mathbf{AFC}$

Modale Logik

Def. Sei \mathcal{P} eine Menge von atomaren Formeln. Dann ist die Menge der Formeln in der modalen Logik definiert als kleinste Menge MFor \mathcal{P} mit

- $\forall A, B \in \text{MFor}_{\mathcal{P}} : \{\neg A, A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B\} \subset \text{MFor}_{\mathcal{P}}$
- $\mathcal{P} \subset \text{MFor}_{\mathcal{P}}$ • $\forall A \in \text{MFor}_{\mathcal{P}} : \{\Box A, \Diamond A\} \subset \text{MFor}_{\mathcal{P}}$

Def. Zustände in Kripke-Strukturen dürfen in diesem Kapitel auch keine Übergänge zu nächsten Zuständen besitzen, d. h. es muss *nicht* unbedingt gelten:

$$\forall s \in S : \exists s' \in S : s \rightarrow s'.$$

Def. Für eine Kripke-Struktur mit Zustand s und $A \in \text{MFor}$ wird $K, s \models A$ analog zur CTL definiert, wobei \Box als **AX** und \Diamond wie **EX** behandelt wird.

Def. Für eine Kripke-Struktur K und $A \in \text{MFor}_{\mathcal{P}}$ setzen wir

$$K \models A :\iff \forall s : K, s \models A.$$

Achtung. Obige Definition weicht ab von der Definition in CTL!

Bemerkung. Es gilt immer: • $\models \Box(A \rightarrow B) \wedge \Box A \rightarrow \Box B$

- $\models \Box(A \wedge B) \leftrightarrow (\Box A \wedge \Box B)$ • $\models \Diamond(A \vee B) \leftrightarrow (\Diamond A \vee \Diamond B)$
- $K, s \models \Diamond \text{true} \iff \forall A \in \text{MFor}_{\mathcal{P}} : K, s \models \Box A \rightarrow \Diamond A$

Def. Ein **Rahmen** $F = (S, \rightarrow)$ besteht aus einer Menge von Welten S und einer Transitionsrelation $\rightarrow \subset S \times S$. Er **erfüllt** eine modale Formel $A \in \text{MFor}_{\mathcal{P}}$ genau dann, wenn jede Kripke-Struktur $K = (S, \rightarrow, L, s_0)$ mit $L : S \rightarrow \mathfrak{P}(\mathcal{P})$ beliebig A erfüllt.

Def. Eine Relation $\rightarrow \subset S \times S$ heißt **euklidisch**, falls gilt:

$$\forall s, s', s'' : (s \rightarrow s') \wedge (s \rightarrow s'') \implies (s' \rightarrow s'')$$

Satz. Für jeden Rahmen $F = (S, \rightarrow)$ und jedes Atom p gilt:

- \rightarrow reflexiv $\iff \forall A : F$ erfüllt $\Box A \rightarrow A \iff F$ erfüllt $\Box p \rightarrow p$
- \rightarrow transitiv $\iff \forall A : F$ erfüllt $\Box A \rightarrow \Box \Box A \iff F$ erfüllt $\Box p \rightarrow \Box \Box p$
- \rightarrow euklidisch $\iff \forall A : F$ erfüllt $\Diamond A \rightarrow \Box \Diamond A \iff F$ erfüllt $\Diamond p \rightarrow \Box \Diamond p$.

Der Allquantor bezieht sich dabei auf alle $A \in \text{MFor}_{\mathcal{P}}$.