Zusammenfassung Logik für Informatiker

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

Prädikatenlogik erster Stufe

Notation. Die Symbole $x_0, x_1, ...$ 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 Prädikatensymbole.

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

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

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

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

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

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

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

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

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

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

$$\beta : \{x_0, x_1, ...\} \to D_I.$$

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

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

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

- $x_{I,\beta} \coloneqq \beta(x)$
- $f(t_1, ..., t_n) \coloneqq f^I((t_1)_{I,\beta}, ..., (t_n)_{I,\beta})$

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

$$\begin{aligned}
I,\beta \vDash (t_1 = t_2) &\quad :\iff (t_1)_{I,\beta} = (t_2)_{I,\beta} \\
I,\beta \vDash P(t_1, ..., t_n) &\quad :\iff P^I((t_1)_{I,\beta}, ..., (t_n)_{I,\beta}) \\
I,\beta \vDash \neg A &\quad :\iff I,\beta \nvDash A \\
I,\beta \vDash A \wedge B &\quad :\iff (I,\beta \vDash A) \wedge (I,\beta \vDash B) \\
I,\beta \vDash A \vee B &\quad :\iff (I,\beta \vDash A) \vee (I,\beta \vDash B) \\
I,\beta \vDash A \to B &\quad :\iff (I,\beta \nvDash A) \vee (I,\beta \vDash B) \\
I,\beta \vDash A \leftrightarrow B &\quad :\iff ((I,\beta \nvDash A) \wedge (I,\beta \nvDash B)) \\
&\qquad\qquad \vee ((I,\beta \vDash A) \wedge (I,\beta \vDash B)) \\
I,\beta \vDash \forall\, x : A &\quad :\iff \forall\, d \in D_I : I, \beta^d_x \vDash A \\
I,\beta \vDash \exists\, x : A &\quad :\iff \exists\, d \in D_I : I, \beta^d_x \vDash A
\end{aligned}$$

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

$$\begin{aligned}
I,\beta \vDash A &\iff I,\beta \nvDash \neg A \iff I,\beta \vDash \neg\neg A \\
I,\beta \vDash A \wedge B &\iff I,\beta \vDash \neg(A \to \neg B) \\
I,\beta \vDash A \vee B &\iff I,\beta \vDash \neg A \to B \\
I,\beta \vDash A \leftrightarrow B &\iff I,\beta \vDash (A \to B) \wedge (B \to A) \\
I,\beta \vDash \exists\, x : A &\iff I,\beta \vDash \neg\forall\, x : \neg A
\end{aligned}$$

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

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

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

$$I,\beta \vDash M \quad :\iff \forall\, F \in M : I,\beta \vDash F$$

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

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

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

Notation. $A_1, ..., A_n \vDash A \quad :\iff \{A_1, ..., A_n\} \vDash A$

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

$$I \vDash \{A_1, ..., A_n\} \iff I \vDash A_1 \wedge ... \wedge A_n$$

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

$$M \vDash A \to B \iff M \cup \{A\} \vDash B$$

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

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

Satz. Für $A \in \mathrm{For}$ gilt:

- $\vDash A \implies A$ ist erfüllbar
- $\vDash A \iff \varnothing \vDash A$

Satz. Sei $A \in \mathrm{For}$ und $M \subset \mathrm{For}$. Dann gilt $M \vDash A$ 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:

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

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

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

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

$$\begin{aligned}
\mathrm{Ax}_1 &\coloneqq \{A \to (B \to A) \mid A, B \in \mathrm{For}\} \\
\mathrm{Ax}_2 &\coloneqq \{(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \mid A, B, C \in \mathrm{For}\} \\
\mathrm{Ax}_3 &\coloneqq \{(\neg A \to \neg B) \to (B \to A) \mid A, B \in \mathrm{For}\}
\end{aligned}$$

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

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

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

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

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

Beob. Präfixe und Verkettungen von Herleitungen sind ebenfalls Herleitungen.

Prop.

- Aus $M \vdash A$ und $M \vdash A \to B$ folgt $M \vdash B$.
- Aus $M \vdash \neg A \to \neg B$ folgt $M \vdash B \to A$.

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

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

- $\vdash (A \to B) \to ((B \to C) \to (A \to C))$
- $\vdash \neg A \to (A \to B)$
- $\vdash \neg\neg A \to A$
- $\vdash A \to \neg\neg A$
- $\vdash (\neg A \to A) \to A$

Prop. Es gilt:

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

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

$$M \vdash A \implies M \vDash A.$$

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

Lem.
- Ist M inkonsistent, so gilt $M \vdash B$ für alle $B \in \mathrm{For}$.
- Für $A \in \mathrm{For}$ gilt: $M \nvdash A \implies M \cup \{A\}$ ist konsistent.

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

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

$$M \vDash A \implies M \vdash A.$$

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

Satz (Endlichkeits- bzw. Kompaktheitssatz). Sei $A \in \mathrm{For}$, $M \subset \mathrm{For}$.
- Dann gilt $M \vDash A$ genau dann, wenn es eine endliche Teilmenge $M' \subset M$ mit $M' \vDash A$ gibt.
- Dann ist M genau dann erfüllbar, wenn jede endliche Teilmenge von M erfüllbar ist.

Hilbert-Kalkül für Prädikatenlogik

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

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

Achtung. Die Umkehrung gilt nicht!

Prop. Sei $A \in \mathrm{For}$. Dann gilt:
- $\forall x : A \vDash A$
- $A \vDash \forall x : A$ nicht (i. A.)

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

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

Def.
- $\forall x : A$ heißt **Generalisierung** von $A \in \mathrm{For}$.
- Ist $\mathrm{FV}(A) = \{y_1, ..., y_n\}$, so heißt jede der $n!$ Formeln $\forall y_1 : \forall y_2 : ... \forall y_n : A$ ein **universeller Abschluss** von A.

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

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

Kor. Seien A, M geschlossen und β_1, β_2 Belegungen. Dann gilt
- $I, \beta_1 \vDash M \iff I, \beta_2 \vDash M$
- $I, \beta_1 \vDash M \iff I \vDash M$
- M ist erfüllbar $\iff M$ hat ein Modell
- $M \vDash A \iff (\forall \text{ Interpretationen } I : I \vDash M \iff I \vDash A)$

Prop.
- $I \vDash A \iff I \vDash \forall x : A$
- $\vDash A \iff \vDash \forall x : A$

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

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

$$f(t_1, ..., t_n)[t/x] \coloneqq f(t_1[t/x], ..., t_n[t/x]) \quad \text{für } f \in \mathcal{F}^n$$
$$P(t_1, ..., t_n)[t/x] \coloneqq P(t_1[t/x], ..., t_n[t/x]) \quad \text{für } P \in \mathcal{P}^n$$
$$(t_1 = t_2)[t/x] \coloneqq (t_1[t/x] = t_2[t/x])$$
$$(\neg A)[t/x] \coloneqq \neg(A[t/x])$$
$$(A \to B)[t/x] \coloneqq A[t/x] \to A[t/x]$$

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

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

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

$\mathrm{Ax}_1, \mathrm{Ax}_2, \mathrm{Ax}_3$: wie zuvor	
$\mathrm{Ax}_4 : (\forall x : A) \to A[t/x]$	(**SP**ezialisierung)
$\mathrm{Ax}_5 : A \to \forall x : A, \quad$ falls $x \notin \mathrm{FV}(A)$	(**GE**neralisierung)
$\mathrm{Ax}_6 : (\forall x : A \to B) \to ((\forall x : A) \to (\forall x : B))$	(**D**istr. **A**llquantor)
$\mathrm{Ax}_7 : x = x$	(**RE**flexivität)
$\mathrm{Ax}_8 : (x = y) \to (A \to A')$	(**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 $M \subset \mathrm{For}$ und $A, B \in \mathrm{For}$:

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

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

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

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

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

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

$$M \vdash A \implies M \vDash A.$$

Lem. Für $M \subset \mathrm{For}$ und $A \in \mathrm{For}$ gilt:
- $M \nvdash A \implies M \cup \{A\}$ ist konsistent.
- $M \nvdash \forall x : A \implies M \cup \{\neg \forall x : A, \neg A[c/x]\}$ ist konsisten für jede Variable c, die nicht in M und A vorkommt.

Lem (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 $M \subset \mathrm{For}$ und $A \in \mathrm{For}$:

$$M \vDash A \implies M \vdash A.$$

Satz (Endlichkeits- bzw. Kompaktheitssatz der Prädikatenlogik). Sei $A \in \mathrm{For}$, $M \subset \mathrm{For}$.
- Dann gilt $M \vDash A$ genau dann, wenn es eine endliche Teilmenge $M' \subset M$ mit $M' \vDash A$ gibt.
- Dann ist M genau dann erfüllbar, wenn jede endliche Teilmenge von M erfüllbar ist.

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

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

Kor. Es gibt kein $A \in \mathrm{For}$ mit
- $I \vDash A \iff D_I$ ist endlich.
- Bei Logik ohne Gleichheit: $I \vDash A \iff |D_I| = n$ für ein festes $n \in \mathbb{N}$.

Weitere Beweisverfahren

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

	rechts		links
Imp	$\dfrac{M \cup \{A\} \vdash_G B}{M \vdash A \to B}$		$\dfrac{M \cup \{\neg C\} \vdash_G A \quad M \cup \{B\} \vdash_G C}{M \cup \{A \to B\} \vdash_G C}$
Neg	$\dfrac{M \cup \{A\} \vdash_G \neg B}{M \cup \{B\} \vdash_G \neg A}$		$\dfrac{M \cup \{\neg B\} \vdash_G A}{M \cup \{\neg A\} \vdash_G B}$
Kon	$\dfrac{M \vdash_G A \quad M \vdash_G B}{M \vdash_G A \wedge B}$		$\dfrac{M \cup \{A, B\} \vdash_G C}{M \cup \{A \wedge B\} \vdash_G C}$
Dis	$\dfrac{M \cup \{\neg B\} \vdash_G A}{M \vdash_G A \vee B}$		$\dfrac{M \cup \{A\} \vdash_G C \quad M \cup \{B\} \vdash_G C}{M \cup \{A \vee B\} \vdash_G C}$

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

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

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

$$\overline{p} \coloneqq \neg p, \quad \overline{\neg p} \coloneqq p.$$

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

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

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 $\mathrm{Res}^*(A)$ bezeichnet.

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

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

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:

$$\frac{}{\{B[^E/_x]\}\ x = E;\ \{B\}}\ (=\mathrm{p}) \qquad \frac{}{\{D_E \wedge B[^E/_x]\}\ x = E;\ \{B\}}\ (=\mathrm{t})$$

$$\frac{A \Rightarrow B \quad \{B\}\ S\ \{C\} \quad C \Rightarrow D}{\{A\}\ S\ \{D\}}\ (\mathrm{K}) \qquad \frac{\{A\}\ S\ \{B\} \quad \{B\}\ T\ \{C\}}{\{A\}\ S;T\ \{C\}}\ (\mathrm{sK})$$

$$\frac{\{A \wedge B\}\ S\ \{C\} \quad \{A \wedge \neg B\}\ T\ \{C\}}{\{A\}\ \text{if } (B) \text{ then } S \text{ else } T\ \{C\}}\ (\mathrm{if})$$

$$\frac{\{A \wedge B\}\ S\ \{A\}}{\{A\}\ \text{while } (B) \text{ do } S\ \{A \wedge \neg B\}}\ (\mathrm{Wp})$$

$$\frac{\forall z \in \mathbb{Z} : \{A \wedge B \wedge t = z\}\ S\ \{A \wedge t < z\} \quad A \wedge B \implies t \geq 0}{\{A\}\ \text{while } (B) \text{ do } S\ \{A \wedge \neg B\}}\ (\mathrm{Wt})$$

Temporale Logik

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

Notation. $\pi^j \coloneqq s_j, s_{j+1}, \ldots$ 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 $\mathrm{TFor}_\mathcal{P}$ mit
- $\mathcal{P} \subset \mathrm{TFor}_\mathcal{P}$
- $\forall A \in \mathrm{TFor}_\mathcal{P} : \{\mathbf{G}A, \mathbf{F}A, \mathbf{X}A\} \subset \mathrm{TFor}_\mathcal{P}$
- $\forall A, B \in \mathrm{TFor}_\mathcal{P} : \{\neg A, A \wedge B, A \vee B, A \to B, A \leftrightarrow B\} \subset \mathrm{TFor}_\mathcal{P}$
- $\forall A, B \in \mathrm{TFor}_\mathcal{P} : (A\,\mathbf{U}\,B) \in \mathrm{TFor}_\mathcal{P}$

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

$$\begin{aligned}
\pi &\vDash p && :\iff p \in L(s_0)\\
\pi &\vDash \neg A && :\iff \pi \nvDash A\\
\pi &\vDash A \vee B && :\iff (\pi \vDash A) \vee (\pi \vDash B)\\
\pi &\vDash \mathbf{X}A && :\iff \pi^1 \vDash A\\
\pi &\vDash \mathbf{G}A && :\iff \forall\, j \in \mathbb{N}_0 : \pi^j \vDash A\\
\pi &\vDash \mathbf{F}A && :\iff \exists\, j \in \mathbb{N}_0 : \pi^j \vDash A\\
\pi &\vDash A\,\mathbf{U}\,B && :\iff \exists\, j \in \mathbb{N}_0 : \pi^j \vDash B \wedge (\forall\, i < j : \pi^i \vDash A)
\end{aligned}$$

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

Prop. Für alle $A \in \mathrm{TFor}$ gilt:
- $\mathbf{G}A \dashv\vDash \neg\mathbf{F}\neg A$
- $\mathbf{F}A \dashv\vDash true\,\mathbf{U}\,A$
- $A\,\mathbf{U}\,B \dashv\vDash \neg((\neg B)\,\mathbf{U}\,(\neg A \wedge \neg B)) \wedge \mathbf{F}B$

Satz. Für alle $A, B \in \mathrm{TFor}$ gilt:
- $\vDash \mathbf{G}(A \to B) \to (\mathbf{G}A \to \mathbf{G}B)$
- $\vDash \mathbf{XG}A \leftrightarrow \mathbf{GX}A$
- $\vDash (A \wedge \mathbf{G}(A \to \mathbf{X}A)) \to \mathbf{G}A$
- $\vDash \mathbf{XF}A \to \mathbf{F}A$

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

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

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

Def. Sei $\mathcal{P}$ eine Menge von atomaren Formeln. Dann sind Formeln in CTL (Computation Tree Logic) über $\mathcal{P}$ definiert als kleinste Menge $\mathrm{CTFor}_\mathcal{P}$ mit
- $\forall A, B \in \mathrm{TFor}_\mathcal{P} : \{\neg A, A \wedge B, A \vee B, A \to B, A \leftrightarrow B\} \subset \mathrm{CTFor}_\mathcal{P}$
- $\mathcal{P} \subset \mathrm{CTFor}_\mathcal{P}$
- $\forall A, B \in \mathrm{TFor}_\mathcal{P} : \{\mathbf{A}(A\,\mathbf{U}\,B), \mathbf{E}(A\,\mathbf{U}\,B)\} \subset \mathrm{TFor}_\mathcal{P}$
- $\forall A \in \mathrm{TFor}_\mathcal{P} : \{\mathbf{AG}A, \mathbf{AF}A, \mathbf{AX}A, \mathbf{EG}A, \mathbf{EF}A, \mathbf{EX}A\} \subset \mathrm{TFor}_\mathcal{P}$

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

$$\begin{aligned}
K, s &\vDash p && :\iff p \in L(s)\\
K, s &\vDash \neg A && :\iff K, s \neg\vDash A\\
K, s &\vDash A \vee && :\iff (K, s \vDash A) \vee (K, s \vDash B)\\
K, s &\vDash \mathbf{AX}B && :\iff \forall\, s' \in S : (s \to s') \Rightarrow K, s' \vDash B\\
K, s &\vDash \mathbf{EX}B && :\iff \exists\, s' \in S : (s \to s') \wedge (K, s' \vDash B)\\
K, s &\vDash \mathbf{AG}B && :\iff K, s \vDash B \wedge \forall\, s' \in S : (s \to s') \Rightarrow K, s' \vDash \mathbf{AG}B\\
K, s &\vDash \mathbf{EG}B && :\iff K, s \vDash B \wedge \exists\, s' \in S : (s \to s') \wedge (K, s' \vDash \mathbf{EG}B)\\
K, s &\vDash \mathbf{AF}B && :\iff \forall \text{ Abläufe } \pi = s_0, s_1, s_2, \ldots \text{ von } K \text{ mit } s_0 = s :\\
&&& \quad \exists\, j \in \mathbb{N}_0 : K, s_j \vDash B\\
K, s &\vDash \mathbf{EF}B && :\iff \exists \text{ Ablauf } \pi = s_0, s_1, s_2, \ldots \text{ von } K \text{ mit } s_0 = s :\\
&&& \quad \exists\, j \in \mathbb{N}_0 : K, s_j \vDash B\\
K, s &\vDash \mathbf{A}(B\,\mathbf{U}\,C) && :\iff \forall \text{ Abläufe } \pi = s_0, s_1, s_2, \ldots \text{ von } K \text{ mit } s_0 = s :\\
&&& \quad \exists\, j \in \mathbb{N}_0 : (K, s_j \vDash C) \wedge (\forall\, i < j : K, s_i \vDash B)\\
K, s &\vDash \mathbf{E}(B\,\mathbf{U}\,C) && :\iff \exists \text{ Ablauf } \pi = s_0, s_1, s_2, \ldots \text{ von } K \text{ mit } s_0 = s :\\
&&& \quad \exists\, j \in \mathbb{N}_0 : (K, s_j \vDash C) \wedge (\forall\, i < j : K, s_i \vDash B)
\end{aligned}$$

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

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

Satz. Für alle $B, C \in \mathrm{CTFor}$ gilt:
- $\vDash (B \wedge \mathbf{AG}(B \to \mathbf{AX}B)) \to \mathbf{AG}B$
- $\vDash \mathbf{AX}(B \to C) \wedge \mathbf{AX}B \to \mathbf{AX}C$

Satz. Für alle $A, B \in \mathrm{CTFor}$ gilt:
- $\mathbf{AG}B \dashv\vDash \neg\mathbf{EF}\neg B$
- $\mathbf{EG}B \dashv\vDash \neg\mathbf{AF}\neg B$
- $\mathbf{EF}B \dashv\vDash \mathbf{E}(true\,\mathbf{U}\,B)$
- $\mathbf{AF}B \dashv\vDash \mathbf{A}(true\,\mathbf{U}\,B)$
- $\mathbf{AX}B \dashv\vDash \neg\mathbf{EX}\neg B$
- $\mathbf{A}(B\,\mathbf{U}\,C) \dashv\vDash \neg\mathbf{E}(\neg C\,\mathbf{U}\,(\neg C \wedge \neg B)) \wedge \mathbf{AF}C$

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 $\mathrm{MFor}_\mathcal{P}$ mit
- $\forall A, B \in \mathrm{MFor}_\mathcal{P} : \{\neg A, A \wedge B, A \vee B, A \to B, A \leftrightarrow B\} \subset \mathrm{MFor}_\mathcal{P}$
- $\mathcal{P} \subset \mathrm{MFor}_\mathcal{P}$
- $\forall A \in \mathrm{MFor}_\mathcal{P} : \{\Box A, \Diamond A\} \subset \mathrm{MFor}_\mathcal{P}$

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

$$\forall\, s \in S : \exists\, s' \in S : s \to s'.$$

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

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

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

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

Bem. Es gilt immer:
- $\vDash \Box(A \to B) \wedge \Box A \to \Box B$
- $\vDash \Box(A \wedge B) \leftrightarrow (\Box A \wedge \Box B)$
- $\vDash \Diamond(A \vee B) \leftrightarrow (\Diamond A \vee \Diamond B)$
- $K, s \vDash \Diamond true \iff \forall\, A \in \mathrm{MFor}_\mathcal{P} : K, s \vDash \Box A \to \Diamond A$

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

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

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

Satz. Für jeden Rahmen $F = (S, \to)$ und jedes Atom p gilt:
- $\to$ reflexiv $\Leftrightarrow \forall\, A : F$ erfüllt $\Box A \to A \Leftrightarrow F$ erfüllt $\Box p \to p$
- $\to$ transitiv $\Leftrightarrow \forall\, A : F$ erfüllt $\Box A \to \Box\Box A \Leftrightarrow F$ erfüllt $\Box p \to \Box\Box p$
- $\to$ euklidisch $\Leftrightarrow \forall\, A : F$ erfüllt $\Diamond A \to \Box\Diamond A \Leftrightarrow F$ erfüllt $\Diamond p \to \Box\Diamond p$.

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