# Mathematische Logik - Merkzettel

Philipp Fischer

# Aussagenlogik

## Verschiedenes

- Aussagenlogisches *Interpolationstheorem*: Sei $\psi \to \varphi$ eine aussagenlogische Tautologie. Dann existiert eine aussagenlogische Formel $\vartheta$ mit $\tau(\vartheta) \subseteq \tau(\psi) \cap \tau(\varphi)$, sodass $\psi \to \vartheta$ und $\vartheta \to \varphi$ Tautologien sind
- Das *Erfüllbarkeit*sproblem für Formeln in *DNF* kann in linearer Laufzeit gelöst werden
- Eine Formelmenge ist *endlich axiomatisierbar*, wenn eine endliche Formelmenge existiert, welche die gleichen Modelle hat
- Sei $\Phi \subseteq \mathrm{AL}$ eine Formelmenge und $X \in \tau(\Phi)$ eine Aussagenvariable. $X$ heißt *explizit definierbar* in $\Phi$, wenn eine Formel $\varphi \in \mathrm{AL}$ existiert, welche $X$ nicht enthält, sodass $\Phi \models X \leftrightarrow \varphi$

## Eigenschaften der Folgerungsbeziehung

- $\{\psi, \varphi\} \models \psi \wedge \varphi$
- $\Phi \cup \{\psi\} \models \varphi$ und $\Phi \cup \{\neg\psi\} \models \varphi$ dann gilt $\Phi \models \varphi$
- $\varnothing \models \psi$ genau dann wenn $\psi$ Tautologie
- $\Phi \models \psi$ genau dann wenn $\Phi \cup \{\neg\psi\}$ unerfüllbar
- $\Phi \models \psi$ und $\Phi \models \neg\psi$ dann ist $\Phi$ unerfüllbar. Unerfüllbare Formelmenge folgern jede beliebige Formel.

## Horn-Formeln und Erfüllbarkeitstest

- Konjunktion von Disjunktionen (*Klauseln*)
- Jede Klausel von der Form

$$\begin{array}{lll} (1) & \neg X_1 \vee \ldots \vee \neg X_k \vee X \equiv X_1 \wedge \ldots \wedge X_k \to X & \text{(oder } 1 \to X\text{)} \\ (2) & \neg X_1 \vee \ldots \vee \neg X_k \equiv X_1 \wedge \ldots \wedge X_k \to 0 & \end{array}$$

- Algorithmus zum Test der Erfüllbarkeit:
  - Markiere zu Beginn alle $X$ der Form $1 \to X$
  - Solange sich aus bereits markierten Variablen eine neue folgern lässt, markiere diese. Lässt sich 0 folgern, so ist die Formel unerfüllbar.
- Der Algorithmus findet das *kleinste Modell* von $\psi$

## Kompaktheitssatz und Derivate

- $\Phi$ ist erfüllbar $\Leftrightarrow$ jede endliche Teilmenge von $\Phi$ ist erfüllbar.
- $\Phi \models \varphi \Leftrightarrow$ es existiert eine endliche Teilmenge $\Phi_0 \subseteq \Phi$ mit $\Phi_0 \models \varphi$
- Ist $\Phi$ äquivalent zu einer endlichen Formelmenge $\Psi$, so existiert auch eine endliche Teilmenge $\Phi_0 \subseteq \Phi$ die äquivalent zu $\Phi$ ist.

## Resolution

Zum Nachweis der Unerfüllbarkeit von Formeln in KNF. Formel muss in Klauselform betrachtet werden.

- $C$ ist *Resolvente* von $C_1$ und $C_2$ wenn $Y \in C_1$ und $\overline{Y} \in C_2$ und $C = (C_1 - \{Y\}) \cup (C_2 - \{\overline{Y}\})$
- $\mathrm{Res}(K) = K \cup \{C \mid C \text{ ist Resolvente}\}$
- $\mathrm{Res}^*(K) = \bigcup_{n \in \mathbb{N}} \mathrm{Res}^n(K)$

Eine spezielle Form der Resolution, die *Einheitsresolution* ist nur für Horn-Formeln vollständig. Sie verwendet pro Resolutionsschritt immer mindestens eine Klausel mit nur einem Literal.

Eine weitere Form, die *P-Resolution* bildet nur Resolventen aus Klauseln, wenn eine der beiden Klauseln nur positive Literale enthält. Sie ist korrekt und vollständig.

## Sequenzenkalkül

- Eine *Sequenz*: *Antezedens* $\Rightarrow$ *Sukzedens*
- Eine *Schlussregel* besteht aus *Prämisse* und *Konklusion*. Eine Interpretation falsifiziert die Konklusion genau dann wenn sie eine Prämisse der Regel falsifiziert. Es folgt, dass die Konklusion genau dann gültig ist, wenn die Prämissen gültig sind
- $\Gamma \Rightarrow \Delta$ ist gültig, genau dann wenn $\bigwedge \Gamma \models \bigvee \Delta$ genau dann wenn $\bigwedge \Gamma \wedge \neg \bigvee \Delta$ unerfüllbar.

$$(\neg \Rightarrow)\ \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma, \neg\psi \Rightarrow \Delta} \qquad (\Rightarrow \neg)\ \frac{\Gamma, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\psi} \qquad (\vee \Rightarrow)\ \frac{\Gamma, \psi \Rightarrow \Delta \quad \Gamma, \vartheta \Rightarrow \Delta}{\Gamma, \psi \vee \vartheta \Rightarrow \Delta} \qquad (\Rightarrow \vee)\ \frac{\Gamma \Rightarrow \Delta, \psi, \vartheta}{\Gamma \Rightarrow \Delta, \psi \vee \vartheta}$$

$$(\wedge \Rightarrow)\ \frac{\Gamma, \psi, \vartheta \Rightarrow \Delta}{\Gamma, \psi \wedge \vartheta \Rightarrow \Delta} \qquad (\Rightarrow \wedge)\ \frac{\Gamma \Rightarrow \Delta, \psi \quad \Gamma \Rightarrow \Delta, \vartheta}{\Gamma \Rightarrow \Delta, \psi \wedge \vartheta} \qquad (\to\Rightarrow)\ \frac{\Gamma \Rightarrow \Delta, \psi \quad \Gamma, \vartheta \Rightarrow \Delta}{\Gamma, \psi \to \vartheta \Rightarrow \Delta} \qquad (\Rightarrow\to)\ \frac{\Gamma, \psi \Rightarrow \Delta, \vartheta}{\Gamma \Rightarrow \Delta, \psi \to \vartheta}$$

$$(\oplus \Rightarrow)\ \frac{\Gamma, \varphi, \neg\psi \Rightarrow \Delta \quad \Gamma, \neg\varphi, \psi \Rightarrow \Delta}{\Gamma, \varphi \oplus \psi \Rightarrow \Delta} \qquad (\Rightarrow \oplus)\ \frac{\Gamma \Rightarrow \Delta, \varphi, \psi \quad \Gamma \Rightarrow \Delta, \neg\varphi, \neg\psi}{\Gamma \Rightarrow \Delta, \varphi \oplus \psi}$$

$$(| \Rightarrow)\ \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma, \varphi|\psi \Rightarrow \Delta} \qquad (\Rightarrow |)\ \frac{\Gamma, \varphi, \psi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi|\psi}$$

# Prädikatenlogik

## Struktur

- $\mathfrak{A}$ ist *Substruktur* von $\mathfrak{B}$, wenn $A \subseteq B$ und alle Funktionen und Relationen von $\mathfrak{B}$ auf $A$ eingeschränkt sind. Umgekehrt ist dann $\mathfrak{B}$ *Erweiterung* von $\mathfrak{A}$.

$$(2\mathbb{N}, +) \xrightarrow{\mathbb{N}\text{-Substruktur}} (\mathbb{N}, +)$$

- $\mathfrak{A}$ ist *$\sigma$-Redukt* von $\mathfrak{B}$, wenn wir alle Funktionen und Relationen außer die in $\sigma$ aus der Signatur $\tau$ von $\mathfrak{B}$ streichen. Umgekehrt heißt $\mathfrak{B}$ dann *$\tau$-Expansion*

$$(\mathbb{R}, +, \cdot, 0, 1) \xrightarrow{(+,0)\text{-Redukt}} (\mathbb{R}, +, 0)$$

## Beispiele

- *Graphen*: $(V, E^G)$. Das Universum ist die Punktmenge, die zweistellige Relation $E^G$ definiert Kanten. Es darf keine Schlingen geben und es herrscht Kantensymmetrie (ungerichteter Graph)
- *Partielle Ordnung*: $(A, <)$. Es gelten Irreflexivität und Transitivität
- *Lineare Ordnung*: (Zusätzlich) Für alle $a, b$ gilt $a < b$, $a = b$ oder $b < a$.
- *Wohlordnung*: (Noch zusätzlich) Keine unendlichen *absteigenden* Ketten
- *Transitionssystem*: $(S, P_b, E_a)$. Es ist $A$ die Menge von Aktionen und $B$ die Menge von Eigenschaften der Zustände. $P_b$ ist eine einstellige Relation, die dann wahr ist, wenn das Argument (Zustand) Eigenschaft $b$ hat. $E_a$ ist eine zweistellige Relation und ist dann wahr, wenn es eine Transition zwischen den beiden Argumenten (Zustände) gibt, die die Aktion $a$ ausführt.

## Modellklasse

Sei $\Phi$ eine Menge von Sätzen. Die *Modellklasse* $\mathrm{Mod}(\Phi)$ enthält alle Strukturen, mit $\mathfrak{A} \models \Phi$. Eine Klasse $\mathcal{K}$ von Strukturen ist *axiomatisiert* durch $\Phi$, wenn $\mathcal{K} = \mathrm{Mod}(\Phi)$. $\Phi$ ist dann das *Axiomensystem* dieser Klasse.

Axiomatisierungen:

- Klasse aller Gruppen $(G, \circ, e, ^{-1})$:

$$\Phi_{\text{Gruppe}} = \{\forall x \forall y \forall z (x \circ (y \circ z) = (x \circ y) \circ z), \forall x (x \circ e = x), \forall x (x \circ x^{-1} = e)\}$$

- Klasse aller linearen Ordnungen:

$$\Phi_< = \{\forall x \neg x < x, \forall x \forall y \forall z (x < y \wedge y < z \to x < z), \forall x \forall y (x < y \vee x = y \vee y < x)\}$$

- Klasse aller unendlichen Strukturen:

$$\varphi_{\geq n} = \exists x_1 \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$$

$$\Phi_\infty = \{\varphi_{\geq n} \mid n \in \mathbb{N}\}$$



## Normalformen

- Eine FO-Formel heißt *reduziert*, wenn sie nur die Junktoren $\vee$, $\neg$ und den Quantor $\exists$ verwendet. Normalisierung durch De-Morgan und Quantorenregel.
- Eine FO-Formel ist in *Negationsnormalform*, wenn sie nur aus Literalen $(X, \neg X)$ und den Junktoren $\vee$, $\wedge$ und den Quantoren $\exists$, $\forall$ aufgebaut ist. (Keine Negation außer bei Literalen). Normalisierung von außen nach innen.
- Eine FO-Formel heißt *termreduziert*, wenn sie nur Atome der Form $Rx$, $fx = y$ und $x = y$ enthält. (Keine Terme mit Tiefe größer 1). Normalisierung durch Einführen neuer Variablen. Beispiel: $Rxyz$ hat Tiefe 1, aber $Rfx$ hat Tiefe 2
- Eine FO-Formel ist in *Pränex-Normalform*, wenn sie bereinigt ist und die Quantoren alle am Anfang stehen. *Bereinigt* heißt, dass jede Variable nur entweder frei oder gebunden ist, außerdem darf sie nicht mehrfach gebunden sein. Transformation über die Quantorenregeln.
- Nur *erfüllbarkeitsäquivalent*: Ein FO-Satz $\psi$ lässt sich in *Skolem-Normalform* transformieren, sodass $\varphi = \forall y_1 \ldots \forall y_s\, \varphi'$ und $\varphi \models \psi$ und sodass zu jedem $\psi$-Modell ein $\varphi$-Modell existiert (als Expansion). Transformation durch Eliminieren der Existenzquantoren und Ersetzen der Variable durch neue Funktionen, die abhängig von den vorangehenden Allquantoren sind.
- Zu jeder Formel $\psi$ existiert ein Formel $\varphi$ in *relationaler Skolem-Normalform* die *relational* ist und die Gestalt $\forall x_1 \ldots \forall x_r \exists y_1 \ldots \exists y_s\, \eta$ hat, sodass $\psi$ und $\varphi$ über denselben Universen erfüllbar sind. (Die Signatur ist dann eventuell anders, da neue Relationen eingeführt und Funktionen entfernt werden) Transformation durch bringen auf Skolem-Normalform, dann Termreduktion, nach-außen-Wandern der Existenzquantoren und dann Einführen neuer Relationen, die die Funktionen „beinhalten“
- Simultane Substitution: $\varphi[x_1/l_1, \ldots, x_k/l_k]$. Gebundene Variablen werden nicht ersetzt. Kollisionen mit Bezeichnern werden durch Umbenennung der gebundenen Variablen gelöst

## Spieltheorie

- Ein Spiel ist *fundiert* wenn es endlich ist. Es heißt *determiniert*, wenn von jeder Position aus einer der beiden Spieler eine Gewinnstrategie hat. Alle fundierten Spiele sind determiniert
- Zu einem FO-Satz $\psi$ und einer passenden Struktur $\mathfrak{A}$ wird das Auswertungsspiel $\mathrm{MC}(\mathfrak{A}, \psi)$ definiert.
- Eine Position des Spiels: $(\varphi, \beta)$, wobei $\varphi$ Unterformel von $\psi$ und $\beta : \mathrm{frei}(\varphi) \to A$
- $\mathfrak{A} \models \psi$ genau dann, wenn die Verifiziererin eine Gewinnstrategie für das Spiel $\mathrm{MC}(\mathfrak{A}, \psi)$ von der Anfangsposition aus hat.

## Modallogik

- Ein *Transitionssystem* bzw. eine *Kripkestruktur*: $\mathcal{K} = (V, (E_a)_{a \in A}, (P_i)_{i \in I})$ wobei $E_a \subseteq V \times V$ $(a \in A)$ und $P_i \subseteq V$ $(i \in I)$
- $\mathcal{K}, v \models \psi$ heißt $\psi$ gilt im Zustand $v$ von $\mathcal{K}$
- $\mathcal{K}, v \models \langle a \rangle \psi$ wenn ein $w$ existiert, zu dem man mit Transition $a$ kommt und bei dem $\psi$ gilt.
- $\mathcal{K}, v \models [a]\psi$ wenn für alle Nachbarn $w$ zu denen man mit Transition $a$ kommt $\psi$ gilt. (Wenn keine dann wahr)
- Die *Extension* von $\psi$ in $\mathcal{K}$ wird definiert als $[\![\psi]\!]^{\mathcal{K}} = \{v \mid \mathcal{K}, v \models \psi\}$ (Also alle Zustände in denen $\psi$ gilt)
- $[\![P_i]\!] = P_i$
- $[\![\neg\psi]\!]^{\mathcal{K}} = V - [\![\psi]\!]^{\mathcal{K}}$
  $[\![\psi \wedge \varphi]\!]^{\mathcal{K}} = [\![\psi]\!]^{\mathcal{K}} \cap [\![\varphi]\!]^{\mathcal{K}}$
  $[\![\psi \vee \varphi]\!]^{\mathcal{K}} = [\![\psi]\!]^{\mathcal{K}} \cup [\![\varphi]\!]^{\mathcal{K}}$
  $[\![\psi \to \varphi]\!]^{\mathcal{K}} = (V - [\![\psi]\!]^{\mathcal{K}}) \cup [\![\varphi]\!]^{\mathcal{K}}$
- $[\![\langle a \rangle \psi]\!]^{\mathcal{K}} = \{v \mid vE_a \cap [\![\psi]\!]^{\mathcal{K}} \neq \varnothing\}$
- $[\![[a]\psi]\!]^{\mathcal{K}} = \{v \mid vE_a \subseteq [\![\psi]\!]^{\mathcal{K}}\}$
- Formel ist *erfüllbar*, wenn es ein entsprechendes Transitionssystem und einen Zustand gibt, der sie erfüllt. Formel ist *gültig*, wenn $\mathcal{K}, v \models \psi$ für alle $\mathcal{K}$, $v$
- Für alle Formeln $\psi, \varphi \in \mathrm{ML}$ und alle Aktionen gilt:
  - $\langle a \rangle \psi \to [a]\psi$ ist erfüllbar aber nicht gültig
  - $[a](\psi \to \varphi) \to ([a]\psi \to [a]\psi)$ ist gültig
  - $[a]\psi \equiv \neg\langle a \rangle \neg\psi$ (*Dualität* von $\langle a \rangle$ und $[a]$)
- $[a]\psi \equiv \neg\langle a \rangle \neg\psi$
- Bisimilarität zweier Kripkestrukturen: $\mathcal{K}, u \sim \mathcal{K}', u'$
- $\mathcal{K}, v \sim \mathcal{K}', v'$ dann $\mathcal{K}, v \sim_n \mathcal{K}', v'$ für alle $n$ aber umgekehrt nicht
- Modaltiefe: $\mathrm{md}(\langle a \rangle \psi) = \mathrm{md}([a]\psi) = md(\psi) + 1$ Bei Verzweigungen durch Junktoren zählt das Maximum.
- Aus $\mathcal{K}, u \sim_n \mathcal{K}', u'$ folgt $\mathcal{K}, u \equiv^n_{\mathrm{ML}} \mathcal{K}', u'$ (Für den unendlichen Fall auch ohne $n$; Umkehrung gilt allgemein nur in endlich verzweigten Transitionssystemen)
- Die Modallogik hat die *Baummodelleigenschaft*. Sie kann die abgewickelte Kripkestruktur nicht von der ursprünglichen unterscheiden, da diese bisimilar sind.

## Temporale Logiken

### LTL - Linear time Temporal Logic

- Auswertung auf endlichen oder unendlichen *Wörtern* $v_0 v_1 \ldots$ mit atomaren Aussagen $P_i$
- LTL-Formeln: Alle AL-Formeln über $\{P_i \mid i \in \mathbb{N}\}$ und die Ausdrücke $\mathrm{X}\psi$ und $(\psi \mathrm{U} \varphi)$
- Eine Formel $\psi$ gilt an einem Punkt $v_i$ geschrieben als $\mathcal{W}, v_i \models \psi$
- $\mathcal{W}, v_i \models \mathrm{X}\psi$ genau dann, wenn $v_i$ nicht das letzte Element von $\mathcal{W}$ ist und $\mathcal{W}, v_{i+1} \models \psi$
- $\mathcal{W}, v_i \models (\psi \mathrm{U} \varphi)$ genau dann, wenn ein $n \geq i$ existiert, sodass $\mathcal{W}, v_n \models \varphi$ und $\mathcal{W}, v_m \models \psi$ für alle $m$ mit $i \leq m < n$
- $\mathrm{F}\psi := (1 \mathrm{U} \psi)$ (irgendwann gilt $\psi$)
- $\mathrm{G}\psi := \neg \mathrm{F} \neg \psi$ (immer wird $\psi$ gelten)
- $\mathrm{GF}\varphi$ wenn $\varphi$ an unendlich vielen Positionen gilt
- $\mathrm{FG}\neg\varphi$ wenn $\varphi$ nur an endlich vielen Positionen gilt
- *Einbettbar in FO* in die Struktur $\mathcal{W} = (V, <, (P_i)_{i \in I})$. Dabei wird wie folgt übersetzt:

$$\begin{array}{rl} \psi = \mathrm{X}\varphi & \psi^*(x) := \exists y (x < y \wedge \neg \exists z (x < z \wedge z < y) \wedge \varphi^*(y)) \\ \psi = (\varphi \mathrm{U} \vartheta) & \psi^*(x) := \exists y (x < y \wedge \vartheta^*(y) \wedge \forall z ((x \leq z \wedge z < y) \to \varphi^*(y))) \end{array}$$

- Wird statt der Ordnungsrelation $<$ nur eine Nachfolgerrelation verwendet, ist LTL nicht einbettbar in FO
- Auf *Transitionssystemen* sagen wir, dass $\psi$ am Zustand $v$ von $\mathcal{K}$ gilt $(\mathcal{K}, v \models \psi)$ wenn $\psi$ auf *allen* unendlichen Pfaden durch $\mathcal{K}$, welche bei $v$ beginnen, gilt.

### CTL - Computation Tree Logic / Branching time Temporal Logic

- Auswertung auf einer *Kripkestruktur*. Syntax ähnlich zu LTL, aber anstatt *next*- und *until*-Relation führen wir ein:
- $\mathrm{EX}\psi := \Diamond\psi$
- $\mathrm{AX}\psi := \Box\psi$
- Es gilt $\mathcal{K}, v \models \mathrm{E}(\psi \mathrm{U} \varphi)$, wenn ein Pfad $v_0 v_1 \dots$ mit $v = v_0$ und ein $n \geq 0$ existiert, sodass $\mathcal{K}, v_n \models \varphi$ und $\mathcal{K}, v_m \models \psi$ für alle $m$ mit $0 \leq m < n$
- Es gilt $\mathcal{K}, v \models \mathrm{A}(\psi \mathrm{U} \varphi)$, wenn für alle unendlichen Pfade $v_0 v_1 \dots$ mit $v = v_0$ ein $n \geq 0$ existiert, sodass $\mathcal{K}, v_n \models \varphi$ und $\mathcal{K}, v_m \models \psi$ für alle $m$ mit $0 \leq m < n$
- $\mathrm{EF}\psi := E(1\mathrm{U}\psi)$ (ex. ein Pfad auf dem irgendwann $\psi$ gilt; *Erreichbarkeit* von $\psi$)
- $\mathrm{AF}\psi := A(1\mathrm{U}\psi)$ (auf allen Pfaden gilt irgendwann $\psi$)
- $\mathrm{EG}\psi := \neg\mathrm{AF}\neg\psi$ (ex. ein Pfad auf dem immer $\psi$ gilt)
- $\mathrm{AG}\psi := \neg\mathrm{EF}\neg\psi$ (auf allen Pfaden gilt immer $\psi$)
- $\mathrm{AG}\neg(P \wedge Q)$ bedeutet, dass sich $P$ und $Q$ in allen erreichbaren Zuständen ausschließen
- $\mathrm{AGAF}\psi$ bedeutet, dass $\psi$ unendlich oft auf allen Pfaden gilt
- Für alle $\psi \in$ CTL gilt: Wenn $\mathcal{K}, v \models \psi$ und $\mathcal{K}, v \sim \mathcal{K}', v'$ dann auch $\mathcal{K}', v' \models \psi$.
  Es folgt, dass CTL die *Baummodell-Eigenschaft* hat
- Das *Erfüllbarkeit*sproblem für CTL ist entscheidbar (in exponentieller Zeit)

### MSO - Monadische Logik (zweiter Stufe)

- Ist eine Erweiterung der Prädikatenlogik (FO)
- Es sind *Quantoren über einstelligen Relationssymbolen* erlaubt
- Durch folgendes Beispiel kann ausgedrückt werden, dass im Graphen $(V, E)$ ein Pfad von $s$ nach $t$ existiert:

$$\forall X(Xs \wedge \forall y \forall z(Xy \wedge Eyz \rightarrow Xz) \rightarrow Xt)$$

## Definierbarkeit in der Prädikatenlogik

- Eine Strukturklasse $\mathcal{K} \subseteq \mathrm{Str}(\tau)$ ist FO-*axiomatisierbar*, wenn eine Satzmenge $\Phi$ existiert, sodass $\mathcal{K} = \mathrm{Mod}(\Phi)$. Ist $\Phi$ endlich, so ist $\mathcal{K}$ *endlich* oder *elementar axiomatisierbar*
- Eine Relation $R \subseteq A^r$ heißt *(elementar) definierbar* wenn $R = \psi^{\mathfrak{A}}$ für eine Formel $\psi \in FO(\tau)$
- Eine Funktion $f : A^r \rightarrow A$ heißt *(elementar) definierbar* wenn ihr Graph $R_f$ elementar definierbar ist.
- Eine Konstante ist *termdefinierbar*, wenn ein Grundterm $t \in T(\tau)$ existiert, sodass $t^{\mathfrak{A}} = a$. Jede termdefinierbare Konstante ist elementar definierbar durch die Formel $x = t$.
- Beispiel: Ordnungsrelation $<$ auf $\mathbb{R}$ ist in $(\mathbb{R}, +, \cdot, 0, 1)$ elementar definierbar: $\varphi(x, y) = \exists z(z \neq 0 \wedge x + z \cdot z = y)$
- Schreibweise der relativierten Quantoren: $(\exists x.\alpha)\psi$ für $\exists x(\alpha \wedge \psi)$ und $(\forall x.\alpha)\psi$ für $\forall x(\alpha \rightarrow \psi)$
- Ein *Isomorphismus* ist eine bijektive Abbildung $\pi : A \rightarrow B$ zwischen $\mathfrak{A}$ und $\mathfrak{B}$ sodass:

$$(a_1, \dots, a_n) \in R^{\mathfrak{A}} \Leftrightarrow (\pi a_1, \dots, \pi a_n) \in R^{\mathfrak{B}}$$
$$\pi f^{\mathfrak{A}}(a_1, \dots, a_n) = f^{\mathfrak{B}}(\pi a_1, \dots, \pi a_n)$$

- Zwei Strukturen sind *isomorph* wenn ein Isomorphismus $\pi : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$ existiert. Man schreibt dann $\mathfrak{A} \cong \mathfrak{B}$
- *Isomorphielemma*: Ist $\pi$ ein Isomorphismus dann gilt für alle $\psi \in FO(\tau)$: $\quad \mathfrak{A} \models \psi(a_1, \dots, a_n) \Leftrightarrow \mathfrak{B} \models \psi(\pi a_1, \dots, \pi a_n)$
- Es folgt für jede Klasse $\mathcal{K} = \mathrm{Mod}(\psi)$ wenn $\mathfrak{A} \cong \mathfrak{B}$ dass $\mathfrak{A} \in \mathcal{K} \Leftrightarrow \mathfrak{B} \in \mathcal{K}$
- Ist $\pi$ ein *Automorphismus* einer $\tau$-Struktur $\mathfrak{A}$ und $\psi \in \mathrm{FO}(\tau)$ dann ist $\pi$ auch ein Automorphismus der expandierten Struktur $(\mathfrak{A}, \psi^{\mathfrak{A}})$. Wenn also bspw. in $\mathfrak{A}$ ein Automorphismus gilt und in $\mathfrak{B}$ nicht, dann kann $\mathfrak{B}$ keine Expansion durch elementar definierbare Relationen und Funktionen von $\mathfrak{A}$ sein

### Theorien und elementar äquivalente Strukturen

- Eine *Theorie* ist eine erfüllbare abgeschlossene Menge von $\tau$-*Sätzen*. Erfüllt die Theorie einen Satz $(T \models \psi)$ so ist $\psi \in T$
- Die Theorie ist *vollständig*, wenn für jeden Satz $\psi \in T$ oder $\neg\psi \in T$ gilt
- Die *Theorie einer Struktur* $\mathfrak{A}$ ist $\mathrm{Th}(\mathfrak{A}) = \{\psi \mid \mathfrak{A} \models \psi\}$. Sie ist immer vollständig
- Zwei Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ sind *elementar äquivalent*, wenn $\mathrm{Th}(\mathfrak{A}) = \mathrm{Th}(\mathfrak{B})$ d.h. wenn für alle $\tau$-Sätze gilt $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{B} \models \psi$. Man schreibt dann $\mathfrak{A} \equiv \mathfrak{B}$
- Eine Theorie ist genau dann vollständig, wenn alle ihre Modelle elementar äquivalent sind
- Isomorphe Strukturen sind elementar äquivalent. Die Umkehrung gilt im Allgemeinen nicht (jedoch bei endlichen Strukturen)
- Der *Quantorenrang* $\mathrm{qr}(\psi)$ einer Formel gibt die maximale Schachtelungstiefe von Quantoren an
- Zwei Strukturen sind *m-äquivalent* $(\mathfrak{A} \equiv_m \mathfrak{B})$, wenn für alle Sätze $\psi$ mit $\mathrm{qr}(\psi) \leq m$ gilt: $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{B} \models \psi$

## Ehrenfeucht-Fraïssé-Spiele

Zum Nachweis der elementaren Äquivalenz und der m-Äquivalenz von Strukturen und damit zum Nachweis der nicht-axiomatisierbarkeit von Strukturklassen.

- Ein *lokaler* oder *partieller Isomorphismus* ist eine injektive Funktion $p : \mathrm{dom}(p) \rightarrow B$ mit $\mathrm{dom}(p) \subseteq A$ sodass $(a_1, \dots, a_n) \in R^{\mathfrak{A}} \Leftrightarrow (pa_1, \dots, pa_n) \in R^{\mathfrak{B}}$. Die *Menge der lokalen Isomorphismen* ist $\mathrm{Loc}(\mathfrak{A}, \mathfrak{B})$
- Das Ehrenfeucht-Fraïssé-Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ wird von Herausforderer und Duplikatorin in $m$ Zügen gespielt
- In Zug $i$: Der Herausforderer wählt entweder ein Element $a_i$ aus $A$ oder $b_i$ aus $B$, die Duplikatorin antwortet mit Wahl von Element aus der jeweils anderen Struktur. Duplikatorin gewinnt, wenn nach $m$ Zügen $\{(a_1, b_1), \dots, (a_n, b_n)\}$ ein lokaler Isomorphismus ist
- $\mathfrak{A} \equiv_m \mathfrak{B}$ genau dann, wenn die Duplikatorin das Spiel $G_m(\mathfrak{A}, \mathfrak{B})$ gewinnt. (Gilt auch ohne $m$)
- Wenn $\mathfrak{A} \in \mathcal{K}$ und $\mathfrak{B} \notin \mathcal{K}$ und die Duplikatorin das Spiel $G(\mathfrak{A}, \mathfrak{B})$ gewinnt, dann folgt, dass kein FO-Satz $\mathfrak{A}$ und $\mathfrak{B}$ unterscheiden kann, also auch kein FO-Satz $\mathcal{K}$ axiomatisiert
- Wenn man Folgen $(\mathfrak{A}_m)_{m \in \mathbb{N}}$ und $(\mathfrak{B}_m)_{m \in \mathbb{N}}$ angeben kann sodass $\mathfrak{A}_m \in \mathcal{K}$ und $\mathfrak{B}_m \notin \mathcal{K}$ für alle $m$ und die Duplikatorin alle Spiele $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$ gewinnt, dann ist $\mathcal{K}$ wieder nicht elementar axiomatisierbar.
  **Beispiel:** Für alle $m \in \mathbb{N}$ setze $\mathfrak{A}_m = \mathbb{N}$ und $\mathfrak{B}_m = \{1, \dots, m\}$. Offensichtlich gewinnt die Duplikatorin das Spiel $G_m(\mathfrak{A}_m, \mathfrak{B}_m)$ und somit trennt kein Satz $\psi \in \mathrm{FO}(\varnothing)$ die endlichen von den unendlichen Mengen
- Es existiert kein FO-Formel, welche in $\mathfrak{A} = (A, E)$ die transitive Hülle von E definiert



# Prädikatenlogik: Vollständigkeits-, Kompaktheitssatz, Unentscheidbarkeit

## Erweiterung des Sequenzenkalküls um Prädikatenlogik

Gleichheits- und Substitutionsregel:

$$(=)\ \frac{\Gamma, t = t \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \qquad (S \Rightarrow)\ \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, t \doteq t', \psi(t') \Rightarrow \Delta} \qquad (S \Rightarrow)\ \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma, t \doteq t' \Rightarrow \Delta, \psi(t')}$$

Regeln für die Quantoren:

$$(\exists \Rightarrow)\ \frac{\Gamma, \psi(c) \Rightarrow \Delta}{\Gamma, \exists x\psi(x) \Rightarrow \Delta} \qquad (\Rightarrow \exists)\ \frac{\Gamma \Rightarrow \Delta, \psi(t)}{\Gamma \Rightarrow \Delta, \exists x\psi(x)} \qquad (\forall \Rightarrow)\ \frac{\Gamma, \psi(t) \Rightarrow \Delta}{\Gamma, \forall x\psi(x) \Rightarrow \Delta} \qquad (\Rightarrow \forall)\ \frac{\Gamma \Rightarrow \Delta, \psi(c)}{\Gamma \Rightarrow \Delta, \forall x\psi(x)}$$

*$c$ darf dabei nicht in $\Gamma, \Delta$ und $\psi$ vorkommen*

- Ein Satz $\psi$ ist aus $\Phi$ *ableitbar* $(\Phi \vdash \psi)$, wenn eine endliche Teilmenge $\Gamma \subseteq \Phi$ existiert, sodass die Sequenz $\Gamma \Rightarrow \psi$ im Sequenzenkalkül ableitbar ist
- Eine Sequenz $\Gamma \Rightarrow \Delta$ ist aus $\Phi$ *ableitbar*, wenn es eine ableitbare Sequenz $\Gamma, \Gamma' \Rightarrow \Delta$ gibt mit $\Gamma' \subseteq \Phi$
- Wenn nicht jeder Satz aus $\Phi$ ableitbar ist, dann nennen wir $\Phi$ *konsistent*
- *$\Phi$ ist genau dann konsistent, wenn $\Phi$ erfüllbar ist*
- $\Phi \models \psi \Leftrightarrow \Phi \vdash \psi$
- Löwenheim,Skolem: Jede erfüllbare *abzählbare Satzmenge* hat ein *abzählbares Modell*
- Sei $\Phi \subseteq \mathrm{FO}(\tau)$ eine Satzmenge mit beliebig großen endlichen Modellen (d.h für jedes $n \in \mathbb{N}$ gibt es ein endliches Modell $\mathfrak{A} \models \Phi$ mit $|\mathfrak{A}| > n$). Dann hat $\Phi$ auch ein unendliches Modell (Satz 5.21)
- Die *Klasse aller endlichen $\tau$-Strukturen* ist nicht FO-axiomatisierbar (Folgerung 5.22)
- Keine Menge ist gleich mächtig zu ihrer Potenzmenge
- Sei $\mathfrak{A}$ eine unendliche Struktur. Dann gibt es eine Struktur $\mathfrak{B}$ mit $\mathfrak{B} \equiv \mathfrak{A}$ aber $\mathfrak{B} \ncong \mathfrak{A}$. Insbesondere ist die Isomorphieklasse $\{\mathfrak{B} \mid \mathfrak{B} \cong \mathfrak{A}\}$ *nicht FO-axiomatisierbar* (Satz 5.27)
- $\{\mathfrak{B} \mid \mathfrak{A} \equiv \mathfrak{B}\}$ ist die *kleinste axiomatisierbare* Modellklasse die $\mathfrak{A}$ enthält (Lemma 5.26)
- Das *Gültigkeit*sproblem und damit auch das *Erfüllbarkeit*sproblem der *Prädikatenlogik* ist *unentscheidbar* (Church,Turing)
- Das *Erfüllbarkeit*sproblem für Formeln der Form $\exists x_1 \dots \exists x_r \forall y_1 \dots \forall y_s \varphi$ ist *entscheidbar*
- Das *Erfüllbarkeit*sproblem für Formeln unter Signaturen nur mit *monadischen* Relationen ist *erfüllbar*
- ML und CTL sind (sogar effizient) *entscheidbar*. AL ist zwar entscheidbar, aber das Problem ist NP-vollständig
- Aufsteigender Satz von Löwenheim-Skolem: $\Phi$ besitze eine unendliches Modell. Dann gibt es zu jeder Menge $M$ ein Modell $\mathfrak{D} \models \Phi$ über einem Universum D, welches mindestens so mächtig ist wie $M$
- Ist $\mathfrak{A}$ eine *endliche* Struktur mit endlicher Signatur, dann ist $\{\mathfrak{B} \mid \mathfrak{B} \cong \mathfrak{A}\}$ *endlich axiomatisierbar*

# Anhang

**Lemma von König:** Sei $T$ ein endlich verzweigter Baum mit Wurzel $w$, in dem es beliebig lange endliche Wege gibt. Dann gibt es auch einen unendlichen Weg in $T$ (der bei der Wurzel $w$ beginnt)

**Lemma von Zorn:** Sei $(A, <)$ eine nicht-leere partielle Ordnung, in der jede Kette nach oben beschränkt ist. Dann besitzt $(A, <)$ ein maximales Element.
(Also zum Beispiel ein Formelmengensystem, dass durch $\subseteq$ geordnet ist)

## Beweis Kompaktheitssatz (nur nicht-triviale Richtungen)

**Teil 2 als Folgerung aus 1:** $\Phi \models \psi$ genau dann wenn $\Phi \cup \{\neg\psi\}$ unerfüllbar. Das ist nach Teil 1 des Kompaktheitssatzes genau dann der Fall, wenn nicht jede endliche Teilmenge von $\Phi \cup \{\neg\psi\}$ erfüllbar ist. Es gibt also eine endliche Teilmenge $\Phi_0$ von $\Phi \cup \{\neg\psi\}$ die nicht erfüllbar ist. Offensichtlich ist $\Phi_0 \cup \{\neg\psi\}$ dann auch nicht erfüllbar was gleichbedeutend ist mit $\Phi_0 \models \psi$

**Teil 1:** Sei jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar und

$$A = \{\Psi \mid \Psi \supseteq \Phi \text{ und jede endliche Teilmenge von } \Psi \text{ ist erfüllbar}\}$$

Es sind die Voraussetzungen für Zorns Lemma gegeben: Sei $K \subseteq A$ eine Kette, also $\Theta \subseteq \Psi$ oder $\Psi \subseteq \Theta$ für alle $\Psi, \Theta \in K$. Es ist $\Gamma = \bigcup K$ eine obere Schranke für K. Es ist noch zu zeigen, dass $\Gamma$ in $A$ enthalten ist, und so jede endliche Teilmenge $\Gamma_0 \subseteq \Gamma$ erfüllbar ist.
Jede Formel $\gamma \in \Gamma_0$ ist in einer Formelmenge $\Psi(\gamma) \in K$ und da $K$ eine Kette ist, gibt es unter den endlich vielen Mengen $\Psi(\gamma)$ eine maximale, welche $\Gamma_0$ enthält Jede endliche Teilmenge dieser Menge ist also erfüllbar, insbesondere $\Gamma_0$. Nach dem Lemma von Zorn hat $A$ also ein maximales Element $\Phi_{max}$
Für jede Formel gilt entweder $\psi \in \Phi_{max}$ oder $\neg\psi \in \Phi_{max}$. Andernfalls betrachten wir die Erweiterungen $\Phi_{max} \cup \{\psi\}$ und $\Phi_{max} \cup \{\neg\psi\}$. Aufgrund der Maximalität von $\Phi_{max}$ gehört keine dieser Mengen zu $A$. Also gibt es endliche Teilmengen $\Psi_0, \Psi_1 \subseteq \Phi_{max}$, sodass $\Psi_0 \cup \{\psi\}$ und $\Psi_1 \cup \{\neg\psi\}$ unerfüllbar sind. Aber dann ist $\Psi_0 \cup \Psi_1$ eine endliche unerfüllbare Teilmenge von $\Phi_{max}$, im Widerspruch zu $\Phi_{max} \in A$.

$$\mathfrak{I}(X) = 1 \Leftrightarrow X \in \Phi_{max}$$

Per Induktion über den Formelaufbau kann man zeigen, dass $\mathfrak{I} \models \psi$ genau dann, wenn $\psi \in \Phi_{max}$:

- Für atomare $\psi$ folgt dies aus der Definition
- Sei $\psi = \neg\varphi$. Dann ist nach Induktionsvoraussetzung der eben gezeigten Eigenschaft von $\Phi_{max}$

$$\mathfrak{I} \models \psi \Leftrightarrow \mathfrak{I} \not\models \varphi \Leftrightarrow \varphi \notin \Phi_{max} \Leftrightarrow \psi \in \Phi_{max}$$

- Sei $\psi = \varphi \wedge \vartheta$. Nach Induktionsvoraussetzung folgt, dass genau dann $\mathfrak{I} \models \psi$ gilt, wenn $\varphi, \vartheta \in \Phi_{max}$. Aber das ist genau dann der Fall wenn auch $\psi \in \Phi_{max}$. Wenn nämlich $\psi \notin \Phi_{max}$, dann $\neg\psi \in \Phi_{max}$ was unmöglich ist, da $\Phi_{max}$ dann mit $\{\varphi, \vartheta, \neg(\varphi \wedge \vartheta)\}$ eine unerfüllbare endliche Teilmenge enthalten würde. Wenn aber $\psi \in \Phi_{max}$, dann müssen auch $\varphi$ und $\vartheta$ in $\Phi_{max}$ liegen, da sonst $\Phi_{max}$ mit $\{\varphi \wedge \vartheta, \neg\varphi\}$ oder $\{\varphi \wedge \vartheta, \neg\vartheta\}$ wieder eine endliche unerfüllbare Teilmenge enthalten würde
- Andere Fälle analog

Also ist $\mathfrak{I}$ ein Modell von $\Phi_{max}$ und damit auch von $\Phi$

## Beweis zu nicht FO-Axiomatisierbarkeit der Graphen mit Knoten endlichen Grades

Angenommen die Klasse wäre FO-axiomatisierbar. Sei $\Gamma$ das Axiomensystem für diese Klasse. Sei weiter

$$\Phi = \Gamma \cup \{\forall x \exists y_1 \exists y_2 \dots \exists y_n (\bigwedge_{1 \leq i < j \leq n} (y_i \neq y_j) \wedge \bigwedge_{i=1}^{n} Exy_i) \mid n \in \mathbb{N}\} \quad (\Gamma \text{ und Knoten hat unendlich viele Nachbarn})$$

Mit dem Kompaktheitssatz kann man nun zeigen, dass $\Phi$ erfüllbar ist und so ein Modell hat, welche nicht in der Klasse liegt, da es ein Knoten mit unendlich vielen Nachbarn gibt.

Dazu weist man die Erfüllbarkeit jeder Teilmenge von $\Phi$ nach: Sei $\Phi_0 \subseteq \Phi$ endlich, also kann $\Phi_0$ auch nur die Existenz von endlich vielen $k$ Nachbarknoten fordern. Sei $G_k$ der vollständige Graph mit $k + 1$ Knoten. Jeder Knoten hat genau $k$ Nachbarn. Also $G_k$ erfüllt $\Gamma$ und auch die Forderung das jeder Knoten mindestens $k$ Nachbarn hat. Also lässt sich zu jeder Teilmenge $\Phi_0 \subseteq \Phi$ ein Modell konstruieren, das diese erfüllt.

Nach dem Kompaktheitssatz ist nun aber auch $\Phi$ erfüllbar und hat somit ein Modell was im Widerspruch zur Definition der Klasse steht.

## Multiple Choice Fragen

Es gelte $\Phi \models \varphi$

- Für alle $\Psi \subseteq \Phi$ gilt $\Psi \models \varphi$ (*N*)
- Für alle $\Psi \supseteq \Phi$ gilt $\Psi \models \varphi$ (*J*)
- Es gibt endliche Teilmenge $\Phi_0 \subseteq \Phi$, sodass $\Phi_0 \cup \{\neg\varphi\}$ unerfüllbar (*J*)

Sei $\Phi$ abzählbare und erfüllbare Satzmenge

- $\Phi$ hat ein endliches Modell (*N*)
- $\Phi$ hat ein abzählbares Modell (*J*)
- $\Phi$ hat ein überabzählbares Modell (*N*)
- Alle Modell von $\Phi$ sind elementar äquivalent (*N*)