TECHNISCHE UNIVERSITÄT DRESDEN

# THEORETISCHE INFORMATIK UND LOGIK

## 15. Vorlesung: Logisches Schließen

**Markus Krötzsch**
**Lehrstuhl Wissensbasierte Systeme**

TU Dresden, 14. Juni 2017

## Ankündigung

Prüfungstermin im Sommersemester 2017:

**24. Juli 2017**

Lernräume werden organisiert und auf der Webseite angekündigt.



## Prädikatenlogik als Universalsprache

Die Entwicklung der Logik hat ein zentrales Motiv:
Logik als eine universelle, präzise Sprache

- Aristoteles (384–322 v.Chr.): Logik als Grundlage der (philosophischen) Argumentation zwischen vernünftig denkenden Menschen

- Leibniz (1646–1716): Vordenker des automatischen Schließens:

> „. . . falls es zu Unstimmigkeiten käme, dann gäbe es zwischen zwei Philosophen nicht mehr Anlass für Streitigkeiten als zwischen zwei Buchhaltern. Denn es würde genügen, dass beide die Stifte zur Hand nehmen, sich zum Rechenschieber setzen und sagen [· · ·]: Lasst uns rechnen!“

- Hilbert (1862–1942): Programm zur Formalisierung der Mathematik

- Russell (1872–1970): Entwicklung eines logischen Kalküls als Grundlage aller Mathematik



## Kernproblem logisches Schließen

Drückt man die Mathematik in logischen Formeln aus, dann wird logisches Schließen zur Kernaufgabe mathematischer Forschung

Das Problem des prädikatenlogischen Schließens besteht in der folgenden Frage:

**Gegeben:** Eine endliche Menge prädikatenlogischer Sätze (Theorie) $\mathcal{T}$ und ein Satz $F$
**Frage:** Gilt $\mathcal{T} \models F$, d.h. folgt $F$ aus $\mathcal{T}$?

Dieses Problem ist zu verschiedenen anderen äquivalent:

Satz: Für endliche Theorie $\mathcal{T}$ und einen Satz $F$ sind die folgenden Fragen äquivalent:

- Gilt $\mathcal{T} \models F$?
- Ist $\mathcal{T} \cup \{\neg F\}$ unerfüllbar?
- Ist $\bigwedge_{G \in \mathcal{T}} G \rightarrow F$ eine Tautologie?

## Die Bedeutung von Erfüllbarkeit

Satz: Für endliche Theorie $\mathcal{T}$ und einen Satz $F$ sind die folgenden Fragen äquivalent:

- Gilt $\mathcal{T} \models F$?
- Ist $\mathcal{T} \cup \{\neg F\}$ unerfüllbar?
- Ist $\bigwedge_{G \in \mathcal{T}} G \to F$ eine Tautologie?

**Daraus folgt:** Logisches Schließen kann auf das Überprüfen der Erfüllbarkeit einer Formel

$$\bigwedge_{G \in \mathcal{T}} G \wedge \neg F$$

zurückgeführt werden

$\rightsquigarrow$ Erfüllbarkeit als zentrale Frage des Schließens



# Gleichheit



## Gleichheit in Prädikatenlogik

Gleichheit spielt in vielen Anwendungen eine große Rolle:

Manchmal wird Prädikatenlogik so definiert, dass es ein spezielles Gleichheitsprädikat $\approx$ gibt, welches man in der Regel infix schreibt

**Semantik:** In allen Interpretationen $\mathcal{I}$ ist $\approx^{\mathcal{I}} = \{\langle \delta, \delta \rangle \mid \delta \in \Delta^{\mathcal{I}}\}$.

Wir haben bereits ein Beispiel dafür gesehen:

Beispiel: Partielle Ordnungen $\preceq$ sind antisymmetrisch:

$$\forall x, y.((x \preceq y \wedge y \preceq x) \to x \approx y)$$

Auch erlaubt uns Gleichheit, in Logik zu zählen:

Beispiel: „Es gibt nur einen Rudi Völler“ (erster Suchvorschlag von Google bei Eingabe „Es gibt nur einen “, Stand Mai 2017)

$$\forall x, y.(\text{rudiVöller}(x) \wedge \text{rudiVöller}(y) \to x \approx y)$$



## Gleichheit der Interpretation von Konstanten

Die übliche Semantik von Prädikatenlogik erlaubt, dass verschiedene Konstanten gleich interpretiert werden.

Mit Gleichheit kann man das erzwingen oder verbieten:

Beispiel: Seien nun rudiVöller, tanteKäthe, rudi $\in$ **C** Konstanten. Wir können ausdrücken:

$$\text{rudiVöller} \approx \text{tanteKäthe}$$
$$\neg\ \text{rudiVöller} \approx \text{rudi}$$

Manchmal wird auch $\not\approx$ als spezielles Prädikat eingeführt. Wir können das aber auch leicht definieren:

$$\forall x, y.(x \not\approx y \leftrightarrow \neg x \approx y)$$

## Ist Ungleichheit wirklich nötig?

Ungleichheit von Konstanten kann man auch leicht ohne $\approx$ ausdrücken:

Beispiel: Wir betrachten zwei neue, einstellige Prädikate $O_{\text{rudiVöller}}$ und $O_{\text{rudi}}$. Die folgende Theorie impliziert ¬rudiVöller $\approx$ rudi:

$$O_{\text{rudiVöller}}(\text{rudiVöller}) \quad O_{\text{rudi}}(\text{rudi}) \quad \forall x.\neg(O_{\text{rudiVöller}}(x) \wedge O_{\text{rudi}}(x))$$

**Idee:**

- Die Prädikate $O_{\text{rudiVöller}}$ und $O_{\text{rudi}}$ beschreiben zwei Mengen
- Die Mengen enthalten jeweils mindestens die Elemente, welche durch rudiVöller bzw. rudi bezeichnet werden
- Die Mengen sind disjunkt (d.h. enthalten keine gemeinsamen Elemente)

$\rightsquigarrow$ Erzwingung von Ungleichheit durch Zuweisung unvereinbarer Eigenschaften



## Ist Gleichheit wirklich nötig?

Es stellt sich heraus, dass man die wesentlichen Eigenschaften von $\approx$ logisch beschreiben kann:

Für eine gegebene endliche Menge **R** von relevanten Prädikatensymbolen und ein neues zweistelliges Prädikatensymbol eq definieren wir die folgende Gleichheitstheorie $\mathcal{EQ}_{\mathbf{R}}$:

$$\forall x.\text{eq}(x,x) \qquad \text{Reflexivität}$$

$$\forall x,y.\text{eq}(x,y) \rightarrow \text{eq}(y,x) \qquad \text{Symmetrie}$$

$$\forall x,y,z.\text{eq}(x,y) \wedge \text{eq}(y,z) \rightarrow \text{eq}(x,z) \qquad \text{Transitivität}$$

$$\forall x_1,\ldots,x_n,y.((p(x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n) \wedge \text{eq}(x_i,y)) \rightarrow p(x_1,\ldots,x_{i-1},y,x_{i+1},\ldots,x_n)) \qquad \text{Kongruenz}$$

wobei der letzte Satz für alle $n$-stelligen $p \in \mathbf{R}$ und alle $i \in \{1,\ldots,n\}$ instanziiert wird ($\rightsquigarrow$ endlich viele Sätze).



## Gleichheit ist nicht nötig

Für eine beliebige Theorie $\mathcal{T}$ der Prädikatenlogik mit Gleichheit definieren wir $\mathcal{T}_{\text{eq}}$ als die Theorie, die man erhält, indem man $\approx$ in allen Sätzen von $\mathcal{T}$ durch eq ersetzt.

Satz: Sei $\mathcal{T}$ eine Theorie der Prädikatenlogik mit $\approx$ und weiteren Prädikatensymbolen aus der endlichen Menge **R**.

Dann ist $\mathcal{T}$ genau dann in der Prädikatenlogik mit Gleichheit erfüllbar wenn $\mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$ in der Prädikatenlogik ohne Gleichheit erfüllbar ist.

**Warum ist das nützlich?**

- Logisches Schließen kann auf den Test von Erfüllbarkeit zurückgeführt werden
- Erfüllbarkeit bleibt erhalten, wenn man „eingebaute“ Gleicheit durch eine logische Beschreibung von Gleichheit ersetzt

$\rightsquigarrow$ Schließen wird durch Gleichheit nicht wesentlich komplizierter



## Beweis (1)

Satz: Sei $\mathcal{T}$ eine Theorie der Prädikatenlogik mit $\approx$ und weiteren Prädikatensymbolen aus der endlichen Menge **R**.

Dann ist $\mathcal{T}$ genau dann in der Prädikatenlogik mit Gleichheit erfüllbar wenn $\mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$ in der Prädikatenlogik ohne Gleichheit erfüllbar ist.

**Beweis:** „⇒“ Nehmen wir an, $\mathcal{T}$ ist in der Prädikatenlogik mit Gleichheit erfüllbar.

- Dann hat $\mathcal{T}$ ein Modell $\mathcal{I} \models \mathcal{T}$, wobei $\approx^{\mathcal{I}} = \{\langle\delta,\delta\rangle \mid \delta \in \Delta^{\mathcal{I}}\}$
- Wir definieren eine Interpretation $\mathcal{J}$ mit $\Delta^{\mathcal{J}} := \Delta^{\mathcal{I}}$:
  - $c^{\mathcal{J}} := c^{\mathcal{I}}$ für alle Konstanten $c \in \mathbf{C}$
  - $p^{\mathcal{J}} := p^{\mathcal{I}}$ für alle Prädikate $p \in \mathbf{P}$ mit $p \neq \approx$
  - $\text{eq}^{\mathcal{J}} := \approx^{\mathcal{I}}$
- Dann gilt $\mathcal{J} \models \mathcal{T}_{\text{eq}}$ per Definition
- Zudem gilt $\mathcal{J} \models \mathcal{EQ}_{\mathbf{R}}$, da $\text{eq}^{\mathcal{J}} = \{\langle\delta,\delta\rangle \mid \delta \in \Delta^{\mathcal{J}}\}$

$\rightsquigarrow \mathcal{J} \models \mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$, das heißt $\mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$ ist erfüllbar

## Beweis (2)

Satz: Sei $\mathcal{T}$ eine Theorie der Prädikatenlogik mit $\approx$ und weiteren Prädikatensymbolen aus der endlichen Menge **R**.

Dann ist $\mathcal{T}$ genau dann in der Prädikatenlogik mit Gleichheit erfüllbar wenn $\mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$ in der Prädikatenlogik ohne Gleichheit erfüllbar ist.

**Beweis:** „⇐“ Nehmen wir an, $\mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$ ist erfüllbar.

- Dann gibt es ein Modell $\mathcal{J} \models \mathcal{T}_{\text{eq}} \cup \mathcal{EQ}_{\mathbf{R}}$
- Aus $\mathcal{J} \models \mathcal{EQ}_{\mathbf{R}}$ folgt, dass $\text{eq}^{\mathcal{J}}$ eine Äquivalenzrelation auf der Menge $\Delta^{\mathcal{J}}$ ist:
  Äquivalenzklassen schreiben wir als $[\delta] = \{\epsilon \mid \langle \delta, \epsilon \rangle \in \text{eq}^{\mathcal{J}}\}$
- Faktorisierung von $\mathcal{J}$ mit $\text{eq}^{\mathcal{J}}$ erzeugt eine Interpretation $\mathcal{I}$:
  - $\Delta^{\mathcal{I}} := \{[\delta] \mid \delta \in \Delta^{\mathcal{J}}\}$
  - $c^{\mathcal{I}} := [c^{\mathcal{J}}]$ für alle Konstanten $c \in \mathbf{C}$
  - $p^{\mathcal{I}} := \{\langle [\delta_1], \ldots, [\delta_n] \rangle \mid \langle \delta_1, \ldots, \delta_n \rangle \in p^{\mathcal{J}}\}$ für alle $p \in \mathbf{P}$ $(p \neq \approx)$



## Beweis (3)

**Beweis:** (Forts.) Wir haben $\mathcal{I}$ konstruiert, indem wir alle Domänenelemente von $\mathcal{J}$ gleichsetzen, welche in der Relation $\text{eq}^{\mathcal{J}}$ stehen

Wir wollen zeigen, dass $\mathcal{I} \models \mathcal{T}$ in der Prädikatenlogik mit Gleichheit gilt.[1]

Wir zeigen eine allgemeinere Behauptung:[2]

- Für eine Zuweisung $\mathcal{Z}$ für $\mathcal{J}$ definieren wir eine Zuweisung $\mathcal{Z}'$ für $\mathcal{I}$ wie folgt: $\mathcal{Z}'(x) := [\mathcal{Z}(x)]$ für alle $x \in \mathbf{V}$
- Wir behaupten: Für jede Formel $F$ der Prädikatenlogik mit Gleichheit und jede Zuweisung $\mathcal{Z}$ für $\mathcal{J}$ gilt

$$\mathcal{J}, \mathcal{Z} \models F_{\text{eq}} \text{ genau dann wenn } \mathcal{I}, \mathcal{Z}' \models F$$

- Daraus folgt wie gewünscht $\mathcal{I} \models \mathcal{T}$, weil $\mathcal{T}$ abgeschlossen ist (Zuweisung irrelevant) und $\mathcal{J} \models \mathcal{T}_{\text{eq}}$

[1] Verständnischeck: Klingt das plausibel? Sogar offensichtlich? Gut. Warum genau?

[2] Mathematische Taktik: Scheint ein Beweis zu schwer, dann beweise etwas stärkeres!



## Beweis (4)

**Beweis:** (Forts.) Wir behaupten: Für jede Formel $F$ der Prädikatenlogik mit Gleichheit und jede Zuweisung $\mathcal{Z}$ für $\mathcal{J}$ gilt

$$\mathcal{J}, \mathcal{Z} \models F_{\text{eq}} \text{ genau dann wenn } \mathcal{I}, \mathcal{Z}' \models F$$

Wie kann man so eine Behauptung zeigen?

$\rightsquigarrow$ Induktion über den Aufbau von Formeln

**Induktionsanfang:** Für atomare Formeln $F = p(t_1, \ldots, t_n)$ mit $p \neq \approx$ gilt die Behauptung, weil

$$\langle [\delta_1], \ldots, [\delta_n] \rangle \in p^{\mathcal{I}} \text{ genau dann wenn } \langle \delta_1, \ldots, \delta_n \rangle \in p^{\mathcal{J}}$$

$\Rightarrow$ folgt weil $\mathcal{J} \models \mathcal{EQ}_{\mathbf{R}}$, so dass $\text{eq}^{\mathcal{J}}$ eine Kongruenzrelation ist
$\Leftarrow$ folgt direkt aus der Definition von $p^{\mathcal{I}}$

Für atomare Formeln $F = (t_1 \approx t_2)$ gilt die Behauptung ebenfalls, da $[\delta] = [\epsilon]$ genau dann wenn $\langle \delta, \epsilon \rangle \in \text{eq}^{\mathcal{J}}$.



## Beweis (5)

**Beweis:** (Forts.) Wir behaupten: Für jede Formel $F$ der Prädikatenlogik mit Gleichheit und jede Zuweisung $\mathcal{Z}$ für $\mathcal{J}$ gilt

$$\mathcal{J}, \mathcal{Z} \models F_{\text{eq}} \text{ genau dann wenn } \mathcal{I}, \mathcal{Z}' \models F$$

**Induktionsannahme:** Die Behauptung gilt für Formeln $G$ und $H$ (IA)

**Induktionsschritte:**

- Falls $F = (G \wedge H)$, dann berechnen wir:
  $\mathcal{J}, \mathcal{Z} \models (G \wedge H)_{\text{eq}}$ gdw. $\mathcal{J}, \mathcal{Z} \models G_{\text{eq}}$ und $\mathcal{J}, \mathcal{Z} \models H_{\text{eq}}$ gdw.[IA]
  $\mathcal{I}, \mathcal{Z}' \models G$ und $\mathcal{I}, \mathcal{Z}' \models H$ gdw. $\mathcal{I}, \mathcal{Z}' \models (G \wedge H)$
- Die Fälle $F = \neg G$, $F = (G \vee H)$, $F = (G \rightarrow H)$ und $F = (G \leftrightarrow H)$ sind analog
- Falls $F = \exists x.G$, dann: $\mathcal{J}, \mathcal{Z} \models (\exists x.G)_{\text{eq}}$ gdw.
  $\mathcal{J}, \mathcal{Z}[x \mapsto \delta] \models G_{\text{eq}}$ für ein $\delta \in \Delta^{\mathcal{J}}$ gdw.[IA]
  $\mathcal{I}, \mathcal{Z}'[x \mapsto [\delta]] \models G$ für ein $\delta \in \Delta^{\mathcal{J}}$ gdw.
  $\mathcal{I}, \mathcal{Z}'[x \mapsto [\delta]] \models G$ für ein $[\delta] \in \Delta^{\mathcal{I}}$ gdw. $\mathcal{I}, \mathcal{Z}' \models \exists x.G$
- Der Fall $F = \forall x.G$ ist analog □

## Strukturelle Induktion

Die gezeigte Variante von Induktion heißt strukturelle Induktion

- Klassische Induktion: Ist $E$ eine Eigenschaft, so dass gilt: (1) die Zahl $0$ hat $E$ und (2) eine natürliche Zahl $n > 0$ hat $E$ falls ihr Vorgänger $n - 1$ $E$ hat; dann haben alle natürlichen Zahlen die Eigenschaft $E$.
- Strukturelle Induktion auf Formeln: Ist $E$ eine Eigenschaft, so dass gilt: (1) atomare Formeln haben $E$ und (2) eine nicht-atomare Formel $F$ hat $E$ falls ihre maximalen echten Teilformeln $E$ haben; dann haben alle Formeln die Eigenschaft $E$.

Allgemein kann man Induktion über jede induktiv definierte syntaktische Struktur durchführen (Formeln, Terme, Programme, ...)

Beispiel: Induktion auf der Insel der Wahrheitssager und Lügner. Ein Einwohner verkündet: „Was ich jetzt sage, das habe ich schon einmal gesagt.“ Welchen Typ hat er?



# Unentscheidbarkeit des logischen Schließens



## Schließen ist schwer

**Erinnerung:** $F$ ist logische Konsequenz von $G$, wenn alle Modelle von $F$ auch Modelle von $G$ sind.

- Es ist nicht offensichtlich, wie man das überprüfen sollte, denn es gibt unendliche viele Modelle
- Ebenso schwer erscheinen die gleichwertigen Probleme der Erfüllbarkeit und Allgemeingültigkeit

**Intuition:** prädikatenlogisches Schließen ist unentscheidbar

Wie kann man das beweisen?

Durch Reduktion eines bekannten unentscheidbaren Problems, z.B.

- Halteproblem
- Postsches Korrespondenzproblem
- Äquivalenz kontextfreier Sprachen
- ...



## Unentscheidbarkeit (1)

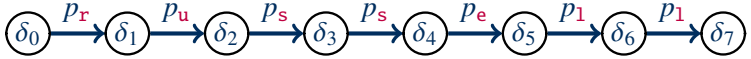
Satz: Logisches Schließen (Erfüllbarkeit, Allgemeingültigkeit, logische Konsequenz) in der Prädikatenlogik ist unentscheidbar.

**Beweis:** Durch Reduktion vom CFG-Schnittproblem:

**Gegeben:** Kontextfreie Grammatiken $G_1$ und $G_2$
**Frage:** Gibt es ein Wort $w \in \mathbf{L}(G_1) \cap \mathbf{L}(G_2)$?

**Idee:** Wir kodieren Wörter in der Prädikatenlogik als Ketten von binären Relationen.

Zum Beispiel würde das Wort `russell` in einer Modellstruktur $\mathcal{I}$ wie folgt aussehen:




Diese Skizze soll bedeuten, dass z.B. $\langle \delta_2, \delta_3 \rangle, \langle \delta_3, \delta_4 \rangle \in p_\mathtt{s}^{\mathcal{I}}$. Wir verwenden ein Prädikatensymbol $p_\mathtt{a}$ für jedes Alphabetssymbol `a`.

## Unentscheidbarkeit (2)

Satz: Logisches Schließen (Erfüllbarkeit, Allgemeingültigkeit, logische Konsequenz) in der Prädikatenlogik ist unentscheidbar.

**Beweis (Fortsetzung):** Zusätzlich verwenden wir binäre Prädikatensymbole $p_A$ für jedes Nichtterminalsymbol A.

Die Kodierung von Grammatiken ist nun direkt möglich:

- Wir nehmen o.B.d.A. an, dass $G_1$ und $G_2$ keine Nichtterminale gemeinsam haben.
- Eine Produktionsregel $A \to \sigma_1 \cdots \sigma_n$ kodieren wir als Formel:

$$\forall x_0, \ldots, x_n.((p_{\sigma_1}(x_0, x_1) \wedge \ldots \wedge p_{\sigma_n}(x_{n-1}, x_n)) \to p_A(x_0, x_n))$$

- Idee: die Formel erkennt, ob eine gegebene Kette aus Terminalen und Nichtterminalen aus einem anderen Nichtterminal entstehen kann



Fortsetzung folgt . . .



## Zusammenfassung und Ausblick

Logisches Schließen ist ein Kernproblem der Prädikatenlogik; es entspricht verschiedenen konkreten Fragen (Folgerung, Erfüllbarkeit, Allgemeingültigkeit)

Logisches Schließen über logischen Aussagem mit Gleichheit kann auf logisches Schließen ohne Gleichheit reduziert werden

Logisches Schließen in Prädikatenlogik ist unentscheidbar (noch zu zeigen)

Was erwartet uns als nächstes?

- Abschluss des Unentscheidbarkeitsbeweises
- Ein konkretes Verfahren zum logischen Schließen
- Gödels Unvollständigkeitssätze



## Bildrechte

Folie 3: (von oben)

- Aristoteles-Büste, römische Kopie, nach einer Skulptur des Bildhauers Lysippos, gemeinfrei
- Gemälde von Johann Friedrich Wentzel d. Ä. (Ausschnitt), um 1700, gemeinfrei
- Fotografie von 1912, gemeinfrei
- Fotografie, um 1924, gemeinfrei