Teil I: Formale Grundlagen der Informatik I

Endliche Automaten und formale Sprachen

Teil II: Formale Grundlagen der Informatik II

Logik in der Informatik

Martin Ziegler

Professor für Angewandte Logik

TU Darmstadt, Fachbereich Mathematik

Sommer 2013

(Folien wesentlich basierend auf Prof. M Otto)

Inhalt

Logik und Logik in der Informatik

- formalisierte Aussagen
  über Eigenschaften von Systemen
  → *Spezifikation*
- systematisches Nachprüfen
  von Eigenschaften von Systemen
  → *Verifikation, model checking*
- logische Beziehungen & Kriterien
  – Folgerungen
  – Äquivalenzen
  – Erfüllbarkeit/Allgemeingültigkeit

SYNTAX und **SEMANTIK**

Logik und Logik in der Informatik

- formalisierte Eigenschaften
  von Elementen in Strukturen
  → z.B. DB Abfragen
- systematische Auswertung
  → z.B. Abfrageauswertung
- logische Beziehungen & Kriterien
  – Implikation (→)/Subsumption (⊆)
  – Äquivalenzen (z.B. zur Abfrageoptimierung)
  – Leerheitstest

SYNTAX und **SEMANTIK**

Logik und Logik in der Informatik

- systematisches logisches Schließen;
  Deduktion, formales Beweisen
  → Wissensrepräsentation, KI
  → automatisches/interaktives Beweisen, ...

SYNTAX und SEMANTIK

historisch: Grundlagen der Mathematik
formales Beweisen und seine Rechtfertigung

von Grundlagenfragen der Mathematik zu:
Fragen der Berechenbarkeit/Entscheidbarkeit (Church, Turing)
Kernfragen der theoretischen Informatik (vorweggenommen)

seither: immer neue praktische Anwendungen in der Informatik

Literatur

Burris: Logic for Mathematics and Computer Science
Prentice-Hall 1998.

Ben-Ari: Mathematical Logic for Computer Science
Springer 1993.

Ebbinghaus, Flum, Thomas:
Einführung in die mathematische Logik
Spektrum 1998.

Schöning: Logik für Informatiker
Spektrum 2000.

Teil 1: Aussagenlogik, AL

Gegenstandsbereich:

Verknüpfungen elementarer Aussagen mittels
Boolescher logischer Verknüpfungen

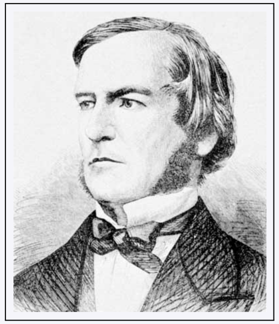
Boolesche Verknüpfungen (Junktoren): $\neg, \wedge, \vee, \rightarrow, \ldots$

Wesentlich:

- strukturierte Formalisierung komplexerer Eigenschaften
- modulare Semantik
- kombinatorisch-algebraischer Charakter der Logik (Boole)
- korrekte und vollständige Beweiskalküle

Motivierendes Beispiel:
$(\neg x \vee y) \wedge (\neg y \vee x) \wedge (\neg x \vee z) \wedge (\neg z \vee x) \wedge (y \vee z) \wedge (\neg y \vee \neg z)$

George Boole (1815–1864)



Algebraisierung/Mathematisierung der Logik

z.B. The Mathematical Analysis of Logic,
Being an Essay Towards a Calculus of Deductive Reasoning
1847

An Investigation of the Laws of Thought, 1854

AL Syntax Definition 1.1

Symbole: $0, 1$; $p, q, r, \ldots, p_1, p_2, \ldots$; $\neg, \wedge, \vee, \ldots$; $(,)$

$\mathrm{AL}(\mathcal{V})$, die Menge der AL-*Formeln über* $\mathcal{V}$
zu geg. AL-Variablenmenge $\mathcal{V}$, induktiv erzeugt:

atomare Formeln:	0, 1, p in $\mathrm{AL}(\mathcal{V})$ (wobei $p \in \mathcal{V}$).
Negation:	für $\varphi \in \mathrm{AL}(\mathcal{V})$ ist auch $\neg\varphi \in \mathrm{AL}(\mathcal{V})$.
Konjunktion:	für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ ist auch $(\varphi \wedge \psi) \in \mathrm{AL}(\mathcal{V})$.
Disjunktion:	für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ ist auch $(\varphi \vee \psi) \in \mathrm{AL}(\mathcal{V})$.

Übung: Kontextfreie Grammatik (für $\mathrm{AL}(\mathcal{V}_n)$)

AL Syntax

evtl. weitere Junktoren, offiziell hier nur als Abkürzungen:

z.B. $$(\varphi \rightarrow \psi) := (\neg\varphi \vee \psi),$$
$$(\varphi \leftrightarrow \psi) := ((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)).$$

statt allg. $\mathrm{AL}(\mathcal{V})$ oft auch für standardisierte Variablenmengen:

$$\mathrm{AL} := \mathrm{AL}(\mathcal{V}), \quad \mathcal{V} = \{p_i : i \geqslant 1\}$$
$$\mathrm{AL}_n := \mathrm{AL}(\mathcal{V}_n), \quad \mathcal{V}_n = \{p_i : 1 \leqslant i \leqslant n\}$$

Beispiele:
0
$\neg x \vee y$
$(\neg x \vee y) \wedge (\neg y \vee x) \wedge (\neg x \vee z) \wedge (\neg z \vee x) \wedge (y \vee z) \wedge (\neg y \vee \neg z)$

AL Semantik Definition 1.4

Interpretationen
von *Belegungen* der AL-Variablen
zu *Wahrheitswerten* für AL-Formeln: Wahrheitswerte in $\mathbb{B} = \{0, 1\}$

$\mathcal{V}$-Interpretation (Belegung): $$\boxed{\begin{array}{rcl} \mathfrak{I} : \mathcal{V} & \longrightarrow & \mathbb{B} \\ p & \longmapsto & \mathfrak{I}(p) \end{array}}$$

$$\mathfrak{I} \text{ interpretiert } p \text{ als } \begin{cases} \text{“wahr”} & \text{wenn } \mathfrak{I}(p) = 1, \\ \text{“falsch”} & \text{wenn } \mathfrak{I}(p) = 0. \end{cases}$$

zur Definition der Semantik von Formeln $\varphi \in \mathrm{AL}(\mathcal{V})$
über geg. $\mathcal{V}$-Interpretation $\mathfrak{I}$:

definiere Wahrheitswertfunktion $$\begin{array}{rcl} {}^{\mathfrak{I}} : \mathrm{AL}(\mathcal{V}) & \longrightarrow & \mathbb{B} \\ \varphi & \longmapsto & \varphi^{\mathfrak{I}} \end{array}$$

induktiv über den Aufbau der Formeln φ
als Fortsetzung der Variablen-Belegung

AL Semantik: Wahrheitswerte

Wahrheitswerte für Formeln $\varphi \in \mathrm{AL}(\mathcal{V})$
bzgl. einer geg. $\mathcal{V}$-Interpretation $\mathfrak{I}$

Funktion $\varphi \longmapsto \varphi^{\mathfrak{I}}$ induktiv:

atomare Formeln:	$0^{\mathfrak{I}} := 0$; $1^{\mathfrak{I}} := 1$; $p^{\mathfrak{I}} := \mathfrak{I}(p)$.
Negation:	$(\neg\varphi)^{\mathfrak{I}} := 1 - \varphi^{\mathfrak{I}}$.
Konjunktion:	$(\varphi \wedge \psi)^{\mathfrak{I}} := \min(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.
Disjunktion:	$(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.

Beispiel:
$((\neg x \vee y) \wedge (\neg y \vee x) \wedge (\neg x \vee z) \wedge (\neg z \vee x) \wedge (y \vee z) \wedge (\neg y \vee \neg z))^{\mathfrak{I}}$
$= 0$ für $\mathfrak{I} : x \mapsto 0, y \mapsto 0, z \mapsto 0$
$= 0$ für $\mathfrak{I} : x \mapsto 0, y \mapsto 0, z \mapsto 1$
$= 0$ für $\mathfrak{I} : x \mapsto 0, y \mapsto 1, z \mapsto 0$

AL Semantik: Modellbeziehung

aus Funktion $\varphi \longmapsto \varphi^{\mathfrak{I}}$ definiere:

$\boxed{\mathfrak{I} \textit{ erfüllt } \varphi \quad \text{gdw. } \varphi^{\mathfrak{I}} = 1}$

Schreibweise: $\mathfrak{I} \models \varphi$.

Sprechweisen: $\mathfrak{I}$ *erfüllt* φ,
$\mathfrak{I}$ *ist Modell von* φ,
φ *ist wahr unter* $\mathfrak{I}$.

Für Formel*mengen* $\Phi \subseteq \mathrm{AL}(\mathcal{V})$ entsprechend:

$\mathfrak{I} \models \Phi$ gdw. $\mathfrak{I} \models \varphi$ für alle $\varphi \in \Phi$.

Beispiel: $\mathfrak{I} : x \mapsto 0, y \mapsto 0$ erfüllt (ist Modell von) $\neg x \vee y$
$\mathfrak{I} : x \mapsto 0, y \mapsto 1$ erfüllt (ist Modell von) $\neg x \vee y$
$(\neg x \vee y) \wedge (\neg y \vee x) \wedge (\neg x \vee z) \wedge (\neg z \vee x) \wedge (y \vee z) \wedge (\neg y \vee \neg z)$
besitzt kein Modell.

AL Semantik: Wahrheitstafeln

für $\varphi \in \mathrm{AL}_n$ schreiben wir auch $\varphi = \varphi(p_1, \dots, p_n)$

für $(b_1, \dots, b_n) \in \mathbb{B}^n$ sei

$$\varphi[b_1, \dots, b_n] := \left\{ \begin{array}{l} \varphi^{\mathfrak{I}} \text{ für Interpretation } \mathfrak{I} \\ \text{mit } (\mathfrak{I}(p_i) = b_i)_{i=1,\dots,n} \end{array} \right.$$

der Wahrheitswert von φ auf $(b_1, \dots, b_n)$.

Wahrheitstafel:

Wertetabelle der Funktion $\left\{ \begin{array}{rcl} \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \dots, b_n) & \longmapsto & \varphi[b_1, \dots, b_n] \end{array} \right.$

Diese Information bestimmt die Semantik von φ vollständig!

AL Semantik: Wahrheitstafeln

Semantik der Junktoren anhand ihrer Wahrheitstafeln:

p	$\neg p$
0	1
1	0

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

grundlegende semantische Begriffe → Abschnitt 2.1

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

(1) Folgerungsbeziehung $\varphi \models \psi$

für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$:
ψ *folgt aus* φ, wenn für *jede* $\mathcal{V}$-Interpretation $\mathfrak{I}$ gilt:
aus $\mathfrak{I} \models \varphi$ folgt $\mathfrak{I} \models \psi$.

Entsprechend $\Phi \models \psi$ für Formel*mengen* Φ

(2) Allgemeingültigkeit $\models \varphi$

$\varphi \in \mathrm{AL}(\mathcal{V})$ *allgemeingültig*, wenn für *alle* $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:
$\mathfrak{I} \models \varphi$.

Beispiele
$\varphi \models \varphi \vee \psi$, $\quad \varphi \models (\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi)$, $\quad \models \varphi \vee \neg\varphi$

grundlegende semantische Begriffe → Abschnitt 2.2

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

(3) Logische Äquivalenz $\varphi \equiv \psi$

$\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ heißen *logisch äquivalent* (Schreibweise: $\varphi \equiv \psi$)
wenn für *alle* $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:
$\mathfrak{I} \models \varphi$ gdw. $\mathfrak{I} \models \psi$ d.h. identische Wahrheitstafeln!

Es gilt:
$\varphi \equiv \psi$ gdw. $\varphi \models \psi$ und $\psi \models \varphi$ gdw. $\models \varphi \leftrightarrow \psi$

Beispiele: $\neg\neg p \equiv p, \quad p \vee 0 \equiv p, \quad p \wedge 0 \equiv 0, \quad \dots$

$p \vee q \equiv q \vee p, \quad (p \vee q) \vee r \equiv p \vee (q \vee r), \quad \dots$

$(p \vee q) \equiv \neg(\neg p \wedge \neg q), \quad (p \wedge q) \equiv \neg(\neg p \vee \neg q)$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r), \quad p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

grundlegende semantische Begriffe → Abschnitt 2.3

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

Erfüllbarkeit

$\varphi \in \mathrm{AL}(\mathcal{V})$ *erfüllbar*,
wenn es *mindestens eine* $\mathcal{V}$-Interpretation $\mathfrak{I}$ *gibt* mit $\mathfrak{I} \models \varphi$.

analog für Formelmengen $\Phi \subseteq \mathrm{AL}$:
Φ erfüllbar, wenn $\mathfrak{I} \models \Phi$ für mindestens ein $\mathfrak{I}$.

wichtig:

$\boxed{\varphi \text{ erfüllbar} \quad \text{gdw.} \quad \neg\varphi \textit{ nicht } \text{allgemeingültig}}$

Beispiel für eine *un*erfüllbare Formelmenge:
$\{\neg x \vee y,\ \neg y \vee x,\ \neg x \vee z,\ \neg z \vee x,\ y \vee z,\ \neg y \vee \neg z\}$

Beispiel für eine erfüllbare Formel:
$\neg x \vee y$; $x \wedge \neg y$ ist nicht allgemeingültig

Erfüllbarkeit

Zentrale Rolle der Erfüllbarkeit (SAT):

- $\models \varphi$ gdw. $\neg\varphi$ *nicht* erfüllbar.
- $\varphi \models \psi$ gdw. $\varphi \wedge \neg\psi$ *nicht* erfüllbar.
- $\Phi \models \psi$ gdw. $\Phi \cup \{\neg\psi\}$ *nicht* erfüllbar.
- $\varphi \equiv \psi$ gdw. $(\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$ *nicht* erfüllbar.

AL Erfüllbarkeitsproblem (SAT(AL)) entscheidbar:

$\mathrm{SAT(AL)} = \{\varphi \in \mathrm{AL} \colon \varphi \text{ erfüllbar } \}$ entscheidbar

– wie?

– mit welchem Aufwand? (Komplexität)

– wie sieht ein Zertifikat aus für Un-/Erfüllbarkeit? ($\mathcal{P}$ vs. $\mathcal{NP}$)

AL und Boolesche Funktionen → Abschnitt 3

$\mathcal{B}_n$: die Menge aller n-stelligen Booleschen Funktionen

$$\begin{array}{rcl} f : \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \dots, b_n) & \longmapsto & f(b_1, \dots, b_n) \end{array}$$

speziell für $\varphi \in \mathrm{AL}_n$:

$$\boxed{\left.\begin{array}{rcl} f_\varphi : \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \dots, b_n) & \longmapsto & \varphi[b_1, \dots, b_n] \end{array}\right\} \in \mathcal{B}_n}$$

beachte: $f_\varphi = f_\psi$ gdw. $\varphi \equiv \psi$

$$\text{also:} \quad \begin{array}{rcl} \mathrm{AL}_n /\!\equiv & \longrightarrow & \mathcal{B}_n \\ [\varphi]_\equiv & \longmapsto & f_\varphi \end{array} \quad \text{injektiv!}$$

Fragen:

- wieviele n-stellige Boolesche Funktionen gibt es?; $|\mathcal{B}_n| = ?$
- ist jedes $f \in \mathcal{B}_n$ durch AL-Formel $\varphi \in \mathrm{AL}_n$ darstellbar?

Disjunktive und konjunktive Normalformen, DNF, KNF

Nomenklatur: p bzw. $\neg p$ (für $p \in \mathcal{V}$) heißen *Literale*

Disjunktionen von Konjunktionen von Literalen: **DNF**-Formeln
Konjunktionen von Disjunktionen von Literalen: **KNF**-Formeln

Beispiel:
$(\neg x \vee y) \wedge (\neg y \vee x) \wedge (\neg x \vee z) \wedge (\neg z \vee x) \wedge (y \vee z) \wedge (\neg y \vee \neg z)$

"große" Konjunktion/Disjunktion (Schreibweisen):

für endliche Formelmenge $\Phi = \{\varphi_1, \dots, \varphi_n\}$:

$\bigwedge \Phi := \bigwedge_{i=1}^{n} \varphi_i \; = \; \varphi_1 \wedge \dots \wedge \varphi_n$

$\bigvee \Phi := \bigvee_{i=1}^{n} \varphi_i \; = \; \varphi_1 \vee \dots \vee \varphi_n$

Konvention: auch *leere* Disjunktionen/Konjunktionen zulässig
mit der Interpretation $\bigvee \emptyset \equiv 0$ (!) und $\bigwedge \emptyset \equiv 1$ (!)

Funktionale Vollständigkeit

Funktionale Vollständigkeit von AL_n für $\mathcal{B}_n$:

zu jedem $f \in \mathcal{B}_n$ existiert DNF-Formel $\varphi \in \mathrm{AL}_n$ mit $f = f_\varphi$.

($\Rightarrow$ bijektive Korrespondenz zw. $\mathcal{B}_n$ und $\mathrm{AL}_n/\!\equiv$)

Beweis:

betrachte $\varphi_f := \bigvee \{\varphi_{\mathbf{b}} \colon f(\mathbf{b}) = 1\}$

wo $\varphi_{\mathbf{b}} = \bigwedge \{p_i \colon b_i = 1\} \wedge \bigwedge \{\neg p_i \colon b_i = 0\}$

Korollar: Satz über DNF und KNF

zu $\varphi \in \mathrm{AL}_n$ existieren stets: $\begin{cases} \text{DNF-Formel } \varphi_1 \in \mathrm{AL}_n \text{ mit } \varphi_1 \equiv \varphi, \\ \text{KNF-Formel } \varphi_2 \in \mathrm{AL}_n \text{ mit } \varphi_2 \equiv \varphi. \end{cases}$

Dualität Konjunktion/Disjunktion → Abschnitt 3.2

nützliche Umformungen/Rechenregeln

$\neg(\varphi_1 \wedge \varphi_2) \equiv \neg\varphi_1 \vee \neg\varphi_2$ verallgemeinert sich zu $\boxed{\neg(\bigwedge \Phi) \equiv \bigvee \Phi^{\neg}}$

wobei $\Phi^{\neg} := \{\neg\varphi \colon \varphi \in \Phi\}$

$\neg(\varphi_1 \vee \varphi_2) \equiv \neg\varphi_1 \wedge \neg\varphi_2$ verallgemeinert sich zu $\boxed{\neg(\bigvee \Phi) \equiv \bigwedge \Phi^{\neg}}$

für **KNF** $\overset{\neg}{\longleftrightarrow}$ **DNF**:

$$\boxed{\neg \underbrace{\bigwedge_{i=1}^{k} \big(\bigvee C_i\big)}_{\text{KNF}} \equiv \underbrace{\bigvee_{i=1}^{k} \big(\bigwedge C_i^{\neg}\big)}_{\text{DNF }(*)}}$$

$C_1, \dots, C_k$ (endl.) Mengen von Literalen
* Doppelnegationen in den $C_i^{\neg}$ eliminieren

Beispiel für exponentiellen "blow-up"

$$\boxed{\varphi_m = \varphi_m(p_1, \dots, p_{2m}) \; := \; \bigwedge_{i=1}^{m} \neg(p_{2i-1} \leftrightarrow p_{2i}) \; \in \mathrm{AL}_{2m}}$$

- φ_m hat genau 2^m erfüllende Interpretationen in $\mathbb{B}^{2m}$
- KNF von Länge $\sim m$ (linear in m):
  $\varphi_m \equiv \bigwedge_{i=1}^{m} \big((p_{2i-1} \vee p_{2i}) \wedge (\neg p_{2i-1} \vee \neg p_{2i})\big)$
- DNF in Länge $\sim 2m2^m$ (exponentiell in m):
  $\varphi_m \equiv \bigvee \{\varphi_{\mathbf{b}} \colon \mathbf{b} \in \mathbb{B}^{2m}, \varphi_m[\mathbf{b}] = 1\}$
- **keine kürzere DNF:** $\begin{cases} \text{keine kürzeren Disjunktionsglieder!} \\ \text{keine redundanten Disjunktionsglieder!} \end{cases}$

Vollständige Systeme von Junktoren → Abschnitt 3.3

Für $n \geqslant 1$ ist jede Funktion in $\mathcal{B}_n$ darstellbar durch AL_n-Formel, die nur die Junktoren $\neg$ und $\wedge$ (nur $\neg$ und $\vee$) benutzt.

Begr.: Eliminiere $\vee$ oder $\wedge$ mit $\begin{cases} \varphi_1 \vee \varphi_2 \equiv \neg(\neg\varphi_1 \wedge \neg\varphi_2) \\ \varphi_1 \wedge \varphi_2 \equiv \neg(\neg\varphi_1 \vee \neg\varphi_2) \end{cases}$

Systeme von Junktoren (Booleschen Funktionen) mit dieser Eigenschaft heißen *vollständig*.

weitere Beispiele vollständiger Systeme:

- $|$ mit der Definition $p \mid q := \neg(p \wedge q)$ (NAND)
  benutze z.B.: $\neg p \equiv p \mid p$; $p \wedge q \equiv \neg(p \mid q) \equiv (p \mid q) \big| (p \mid q)$.
- $\rightarrow$ zusammen mit 0
  benutze z.B.: $\neg p \equiv p \rightarrow 0$; $p \vee q \equiv \neg p \rightarrow q \equiv (p \rightarrow 0) \rightarrow q$.

nicht vollständig sind z.B. $\begin{cases} \{\wedge, \vee\} & \text{(Monotonie);} \\ \{\rightarrow\} & (0 \in \mathcal{B}_n \text{ nicht darstellbar).} \end{cases}$

Kompaktheitssatz (Endlichkeitssatz) (Satz 4.1)

Erfüllbarkeit von unendlichen Formelmengen hängt nur von je endlich vielen ab, i.d.S.d.

für alle $\Phi \subseteq \mathrm{AL}$ gilt:

$\boxed{\mathbf{\Phi} \text{ erfüllbar} \quad \text{gdw.} \quad \text{jedes endliche } \mathbf{\Phi_0} \subseteq \mathbf{\Phi} \text{ erfüllbar}}$ $(*)$

für alle $\Phi \subseteq \mathrm{AL}, \psi \in \mathrm{AL}$ gilt:

$\boxed{\mathbf{\Phi} \models \psi \quad \text{gdw.} \quad \mathbf{\Phi_0} \models \psi \text{ für ein endliches } \mathbf{\Phi_0} \subseteq \mathbf{\Phi}}$ $(**)$

Konsequenz:
Unerfüllbarkeit einer unendlichen Formelmenge lässt sich durch ein endliches Zertifikat nachweisen. (Warum?)

Bemerkung: Aussagen $(*)$ und $(**)$ sind äquivalent.

Kompaktheitssatz: Beweis → Abschnitt 4

für $\Phi \subseteq \mathrm{AL}(\mathcal{V})$, $\mathcal{V} = \{p_i : i \geqslant 1\}$

Sei jedes endliche $\Phi_0 \subseteq \Phi$ erfüllbar.

Konstruiere induktiv $\mathfrak{I}_0, \mathfrak{I}_1, \mathfrak{I}_2, \ldots$ so, dass für jedes n:

- $\mathfrak{I}_n$ eine $\mathcal{V}_n$-Interpretation ist.
- $\mathfrak{I}_{n+1}$ verträglich ist mit $\mathfrak{I}_n$: $\mathfrak{I}_{n+1}(p_i) = \mathfrak{I}_n(p_i)$ für $1 \leqslant i \leqslant n$.
- Für jedes endliche $\Phi_0 \subseteq \Phi$
  gibt es ein erfüllendes $\mathfrak{I}$,
  das mit $\mathfrak{I}_n$ verträglich ist.

Dann ist $\mathfrak{I} \models \Phi$ für die Interpretation $\begin{cases} \mathfrak{I} : \mathcal{V} & \longrightarrow & \mathbb{B} \\ \quad p_n & \longmapsto & \mathfrak{I}_n(p_n) \end{cases}$

Frage: Wie kommt man von $\mathfrak{I}_n$ zu $\mathfrak{I}_{n+1}$?

Kompaktheitssatz: Konsequenzen

vgl. auch Skript u. Aufgaben

Lemma von König (ignoriere Beweis von Lemma 4.4)

Ein endlich verzweigter Baum mit unendlich vielen Knoten muss einen unendlichen Pfad haben. beachte Voraussetzung!

k-Färbbarkeit

Ein Graph ist genau dann k-färbbar, wenn jeder endliche Teilgraph k-färbbar ist.

Domino-Parkettierungen

Ein endliches Domino-System erlaubt genau dann eine Parkettierung der Ebene, wenn sich beliebig große endliche Quadrate parkettieren lassen.

Lemma von König aus AL-Kompaktheit

Betrachte $\mathcal{T} = (V, E, \lambda)$ Baum mit

– Wurzel λ und abzählbar unendlicher Knotenmenge V,

– endlich verzweigter Kantenrelation E:
$E[u] = \{v \in V : (u, v) \in E\}$ endlich für alle $u \in V$.

– Pfaden $\lambda \xrightarrow{E} \dots \xrightarrow{E} u$ jeder endlichen Länge (warum?)

Abk. $\psi(\{x_1, \dots, x_n\}) \;:=\; \left(\bigvee_{j=1}^{n} x_j\right) \wedge \bigwedge_{1 \leqslant i < j \leqslant n} (\neg x_i \vee \neg x_j)$

Kodierung in $\mathrm{AL}(\mathcal{V})$ mit $\mathcal{V} := \{p_u : u \in V\}$:

$\varphi_u \;:=\; p_u \rightarrow \psi(\{p_v : v \in E[u]\})$

"wenn u gewählt wird, dann auch genau ein direkter Nachfolger von u"

Für $\Phi := \{p_\lambda\} \cup \{\varphi_u : u \in V\}$ gilt:

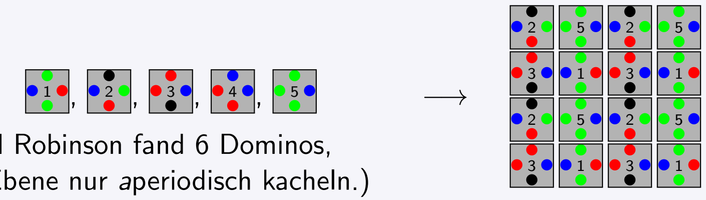
- jedes endliche $\Phi_0 \subseteq \Phi$ ist erfüllbar, also auch Φ insgesamt.
- wenn $\mathfrak{I} \models \Phi$, so liefert dies einen unendlichen Pfad
  $\lambda = u_0 \xrightarrow{E} u_1 \xrightarrow{E} u_2 \xrightarrow{E} \dots$ mit $\mathfrak{I}(u_i) = 1$.

Domino-Parkettierung

ein interessantes, algorithmisch unentscheidbares Problem

Zu gegebener Menge von Kacheln mit gefärbten Rändern: Kann man damit beliebig große Quadrate kacheln?

Beispiel:



(Raphael Robinson fand 6 Dominos,
die die Ebene nur *a*periodisch kacheln.)

Mit AL-Kompaktheit lässt sich zeigen:

Ein endlicher Kachel-Satz erlaubt genau dann eine Parkettierung der unendlichen $\mathbb{N} \times \mathbb{N}$–Ebene (oder auch der $\mathbb{Z} \times \mathbb{Z}$–Ebene), wenn sich beliebig große endliche Quadrate parkettieren lassen.

Domino-Parkettierung mittels Kompaktheit

Ein endlicher Kachel-Satz erlaubt genau dann eine Parkettierung der unendlichen $\mathbb{Z} \times \mathbb{Z}$–Ebene, wenn sich beliebig große endliche Quadrate parkettieren lassen.

Beweis: Fixiere K Kacheln und Relationen $R_\uparrow$ bzw. $R_\leftarrow$ auf $\{1, \dots, K\}$, die besagen, ob Kachel $\#k$ direkt oberhalb bzw. links von Kachel $\#j$ platzierbar ist: $(k, j) \in R_\uparrow$ bzw. $(k, j) \in R_\leftarrow$

Für jedes $x, y \in \mathbb{Z}$ und $1 \leqslant k \leqslant K$ betrachte Variablen $p_{x,y,k}$;

Intuition: $p_{x,y,k} = 1$ heißt, an Position (x, y) liegt Kachel $\#k$.

Wähle Φ als Menge folgender Formeln:

- $\bigvee_{k=1}^{K} p_{x,y,k}$, $\quad x, y \in \mathbb{Z}$
- $\bigwedge_{1 \leqslant k < j \leqslant K} (\neg p_{x,y,k} \vee \neg p_{x,y,j})$, $\quad x, y \in \mathbb{Z}$
- $\bigwedge_{k} \left(p_{x,y+1,k} \rightarrow \bigvee_{j:(k,j) \in R_\uparrow} p_{x,y,j}\right)$, $\quad x, y \in \mathbb{Z}$
- $\bigwedge_{k} \left(p_{x-1,y,k} \rightarrow \bigvee_{j:(k,j) \in R_\leftarrow} p_{x,y,j}\right)$, $\quad x, y \in \mathbb{Z}$

Logikkalküle: Deduktion und Refutation

Logikkalküle: rein syntaktische Formate für formale Beweise.

Formale Beweise: syntaktische Zeichenketten,
nach einfach nachprüfbaren syntaktischen Regeln aufgebaut
(Regelsystem: *Kalkül*).

Ableitung: Erzeugung von (regelkonformen) formalen Beweisen.

Korrektheit nur semantisch korrekte Sachverhalte sind formal beweisbar (ableitbar).

Vollständigkeit jeder semantisch korrekte Sachverhalt ist formal beweisbar (ableitbar).

Resolution: ein *Widerlegungskalkül* für die *Unerfüllbarkeit* von KNF-Formeln.

Sequenzenkalkül: ein *Deduktionskalkül* für *Allgemeingültigkeit* beliebiger AL-Formeln.

KNF in Klauselform → Abschnitt 5.1

KNF: Konjunktionen von Disjunktionen von Literalen.

Notation: L für Literal; $\overline{L}$ für komplementäres Literal; $\overline{L} \equiv \neg L$.

Klausel: endliche Menge von Literalen
$C = \{L_1, \dots, L_k\}$ steht für $\bigvee C \equiv L_1 \vee \dots \vee L_k$
$\square$ steht für die leere Klausel.
Erinnerung: $\square \equiv \bigvee \emptyset \equiv 0$.

Klauselmenge: Menge von Klauseln
$K = \{C_1, \dots, C_\ell\}$ steht für $\bigwedge K \equiv C_1 \wedge \dots \wedge C_\ell$
Erinnerung: $\bigwedge \emptyset \equiv 1$.

$\boxed{\text{endliche Klauselmengen} \approx \text{KNF-Formeln}}$

Resolutionskalkül arbeitet mit KNF in Klauselform
Ableitungsziel: Nachweis der Unerfüllbarkeit einer geg. Klauselmenge durch Ableitung der leeren Klausel $\square$

Resolution → Abschnitt 5.2

$C = \{L_1, \dots, L_k\}$ steht für $\bigvee C \equiv L_1 \vee \dots \vee L_k$, $\quad \square \equiv \bigvee \emptyset \equiv 0$.
$K = \{C_1, \dots, C_\ell\}$ steht für $\bigwedge K \equiv C_1 \wedge \dots \wedge C_\ell$

Beispiele: $L, \overline{L} \in C \;\Rightarrow\; C \equiv 1$ allgemeingültig.

$C \equiv 1 \;\Rightarrow\; K \equiv K \setminus \{C\}$.

$\square \in K \;\Rightarrow\; K \equiv 0$ (unerfüllbar).

$K \models C \;\Leftrightarrow\; K \equiv K \cup \{C\}$.

Resolventen und Resolutionslemma

$$L \in C_1, \overline{L} \in C_2 \;\Rightarrow\; \{C_1, C_2\} \models \underbrace{(C_1 \setminus \{L\}) \cup (C_2 \setminus \{\overline{L}\})}_{\textit{Resolvente}} =: C$$

Beispiele: $y \in C_1,\, y \in C_2 \;\rightsquigarrow\; y \in C$

$y \in C_1,\, \neg y \in C_2 \;\rightsquigarrow\; y, \neg y \in C$ Tautologie

Resolution

diagrammatisch:

$$\begin{tikzcd}
C_1 = \{\dots, L\} \arrow[dr] & & C_2 = \{\dots, \overline{L}\} \arrow[dl] \\
& C = (C_1 \setminus \{L\}) \cup (C_2 \setminus \{\overline{L}\}) &
\end{tikzcd}$$

$$\begin{tikzcd}
\{p, \underline{\neg q}, r\} \arrow[dr] & & \{p, \underline{q}, s, t\} \arrow[dl] \\
& \{p, r, s, t\} &
\end{tikzcd}$$

Bemerkung:
Ist C die Resolvente von C_1 und C_2 und X ein neues Literal,
so ist $C \cup \{X\}$ Resolvente von $C_1 \cup \{X\}$ und C_2.

Resolutionslemma (Lemma 5.5)

Seien $C_1, C_2 \in K$, C Resolvente von C_1 und C_2.
Dann ist $K \equiv K \cup \{C\}$. [also $K \models C$]

Res(K) und Res*(K)

$\mathrm{Res}(K) := K \cup \{C\colon\; C$ Resolvente von Klauseln in $K\}$.

Klausel C heißt (im Resolutionskalkül) *ableitbar* aus K,
gdw. $\quad C \in \underbrace{\mathrm{Res} \cdots \mathrm{Res}}_{n\text{-mal}}(K)$ für ein $n \in \mathbb{N}$.

$\mathrm{Res}^*(K)$: die Menge aller aus K ableitbaren Klauseln.

Korrektheit / Vollständigkeit

Korrektheit: $\square \in \mathrm{Res}^*(K) \;\Rightarrow\; K \equiv 0$ (unerfüllbar). [R-Lemma]

Vollständigkeit: K unerfüllbar $\;\Rightarrow\; \square \in \mathrm{Res}^*(K)$.

Resolutionskalkül: Vollständigkeit

→ Abschnitt 5.3

z.z.: K über $\mathcal{V}_n = \{p_1, \dots, p_n\}$ unerfüllbar $\Rightarrow$ $\Box \in \mathrm{Res}^*(K)$.

Beweis durch Induktion über n.

Induktionsschritt von n nach n + 1

Aus $K = \{C_1, \dots, C_k\}$ über $\mathcal{V}_{n+1}$ gewinne K_0 und K_1 über $\mathcal{V}_n$ mit

$K_0 \equiv K \cup \{\{\neg p_{n+1}\}\}$ und $K_1 \equiv K \cup \{\{p_{n+1}\}\}$ (wie?)

K unerfüllbar $\Rightarrow$ K_0 und K_1 unerfüllbar
$\Rightarrow$ $\Box \in \mathrm{Res}^*(K_0)$ und $\Box \in \mathrm{Res}^*(K_1)$.

Dann ist $\Box \in \mathrm{Res}^*(K)$ oder $\left\{\begin{array}{l} \{p_{n+1}\} \in \mathrm{Res}^*(K) \\ \text{und} \\ \{\neg p_{n+1}\} \in \mathrm{Res}^*(K) \end{array}\right.$

und demnach jedenfalls $\Box \in \mathrm{Res}^*(K)$.

Resolutionsalgorithmus

breadth-first-search, Breitensuche

Eingabe: K	[Klauselmenge, endlich]
$R := K$	
WHILE $(\mathrm{Res}(R) \neq R$ and $\Box \notin R)$ DO $R := \mathrm{Res}(R)$ OD	
IF $\Box \in R$ THEN output "unerfüllbar"	
ELSE output "erfüllbar"	

Beweis im Resolutionskalkül

Ableitungsbaum für $\Box$:
– Knoten mit Klauseln beschriftet
– $\Box$ an der Wurzel
– Resolventen an binären Verzweigungen
– Klauseln aus K an den Blättern

Hornklauseln

→ Abschnitt 5.4

- interessanter Spezialfall für KI Anwendungen,
- AL-HORN-SAT-Problem effizient entscheidbar
- logische Programmierung (Prolog: FO Horn-Formeln)

Hornklausel:
Klausel mit *höchstens einem positiven* Literal
z.B. $C = \{\neg q_1, \dots, \neg q_r, q\} \equiv (q_1 \wedge \dots \wedge q_r) \to q$;
auch $\Box$ ist Hornklausel.

Spezialfälle: C besteht nur aus positivem Literal: *positiv*.
C ohne positive Literale: *negativ*.

Beobachtungen:

Mengen von negativen Hornklauseln trivial erfüllbar ($p_i \mapsto 0$).
Mengen von nicht-negativen Hornklauseln besitzen eindeutige *minimale* erfüllende Interpretationen.

Hornklauseln

Form: $(q_1 \wedge \dots \wedge q_r) \to q$; negativ: $\neg q_1 \vee \dots \vee \neg q_r$

Effizienter Horn-Erfüllbarkeitstest: Grundidee

H Hornklauselmenge; $H^- \subseteq H$ negative Klauseln in H
$H_0 := H \setminus H^-$ nicht negative Klauseln

1. Schritt: Berechne minimale Interpretation $\mathfrak{I}_0 \models H_0$.
2. Schritt: Prüfe, ob $\mathfrak{I}_0 \models H^-$.

Korrektheit

$\mathfrak{I}_0 \models H^- \quad \Rightarrow \quad \mathfrak{I}_0 \models H$.

$\mathfrak{I} \models H \quad \Rightarrow \quad \mathfrak{I} \models H_0$, also $\mathfrak{I}_0 \leqslant \mathfrak{I}$.
$\mathfrak{I} \models H^- \Rightarrow \mathfrak{I}_0 \models H^-$ (und $\mathfrak{I}_0 \models H$).

Sequenzenkalkül allgemeiner Beweiskalkül

Sequenzen

$\Gamma \vdash \Delta$ $\quad$ $\Gamma, \Delta \subseteq \mathrm{AL}$, endlich
auch: $\Gamma; \Delta$ oder Γ, Δ
Γ, Δ als ungeordnete Listen ...

$\Gamma \vdash \Delta$ *allgemeingültig* gdw. $\bigwedge \Gamma \models \bigvee \Delta$

wichtig: links Konjunktion (der Voraussetzungen)
rechts Disjunktion (möglicher Konsequenzen)

Bsp.: $\Phi \vdash \psi$ allgemeingültig gdw. $\Phi \models \psi$.
$\emptyset \vdash \psi$ allgemeingültig gdw. ψ allgemeingültig.
$\Phi \vdash \emptyset$ allgemeingültig gdw. Φ unerfüllbar.

Sequenzenkalkül

Syntakt. Regeln zur Erzeugung aller allgemeingültigen Sequenzen

AL Sequenzenkalkül $\rightarrow$ Abschnitt 6.2

Erzeugung allgemeingültiger Sequenzen durch Sequenzenregeln

$\Gamma \vdash \Delta$ *allgemeingültig* gdw. $\bigwedge \Gamma \models \bigvee \Delta$
Schreibweise $\Gamma, \psi \vdash \Delta, \varphi$

Sequenzenregeln

erzeuge neue Sequenzen aus bereits abgeleiteten Sequenzen

Format: $\dfrac{\text{Prämissen}}{\text{Konklusion}}$

Beispiele: $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$ oder $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$

Korrektheit

einer Regel: sind die Prämissen allgemeingültig,
so auch die Konklusion.
des Kalküls: jede ableitbare Sequenz ist allgemeingültig.

AL Sequenzenkalkül $\mathcal{SK}$

(Ax) $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$	
(0-Ax) $\dfrac{}{\Gamma, 0 \vdash \Delta}$	(1-Ax) $\dfrac{}{\Gamma \vdash \Delta, 1}$
$(\neg\mathrm{L})$ $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$	$(\neg\mathrm{R})$ $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$
$(\vee\mathrm{L})$ $\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$	$(\vee\mathrm{R})$ $\dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$
$(\wedge\mathrm{L})$ $\dfrac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$	$(\wedge\mathrm{R})$ $\dfrac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$

Korrektheit nachprüfen!

sogar rückwärts (ohne Informationsverlust!)

Beispiel

Ableitung der allgemeingültigen Sequenz $p \vdash (p \wedge q) \vee \neg q$:

$$\cfrac{\cfrac{\cfrac{}{p \vdash p, \neg q}\;(\mathrm{Ax}) \qquad \cfrac{\cfrac{}{p, q \vdash q}\;(\mathrm{Ax})}{p \vdash q, \neg q}\;(\neg\mathrm{R})}{p \vdash (p \wedge q), \neg q}\;(\wedge\mathrm{R})}{p \vdash (p \wedge q) \vee \neg q}\;(\vee\mathrm{R})$$

Ax: $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$ $\quad$ $\neg$R: $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$ $\quad$ $\wedge$R: $\dfrac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$

Vollständigkeit

→ Abschnitt 6.3

Jede allgemeingültige Sequenz ist ableitbar.
Beweisidee: systematische Beweissuche rückwärts

> zu jeder Formel in einer Konklusions-Sequenz existiert (genau) eine Regel mit Prämissen, in der diese Formel abgebaut ist.

in rückwärts von der Zielsequenz generiertem Beweisbaum gilt:

Zielsequenz allgemeingültig $\Leftrightarrow$ alle Sequenzen an den Blättern sind allgemeingültig

eine Sequenz aus Variablen ist allgemeingültig $\Leftrightarrow$ Instanz von (Ax), Axiom

Beispiel Beweissuche

für eine *nicht* allgemeingültige Sequenz

$$\text{(}\vee\text{L)}\;\dfrac{\text{(}\wedge\text{R)}\;\dfrac{\text{(Ax)}\;\dfrac{}{p \vdash p} \qquad \mathbf{p \vdash q}}{p \vdash p \wedge q} \qquad \text{(}\wedge\text{R)}\;\dfrac{\mathbf{q \vdash p} \qquad \text{(Ax)}\;\dfrac{}{q \vdash q}}{q \vdash p \wedge q}}{p \vee q \vdash p \wedge q}$$

Man liest ab, dass z.B. die Interpretation $p \mapsto 1\,;\; q \mapsto 0$ ein Gegenbeispiel liefert.

Satz

Der AL Sequenzenkalkül ist korrekt und vollständig für die Ableitung aller allgemeingültigen AL Sequenzen.

Schnittregeln, von $\mathcal{SK}$ zu $\mathcal{SK}^+$

Hinzunahme weiterer *korrekter* Regeln erhält Korrektheit und Vollständigkeit

Schnittregel erlaubt direkte Nachbildung von $\left\{\begin{array}{l}\textbf{Kettenschlüssen}\\ \textbf{indirektem Beweis}\end{array}\right.$

- Kettenschluss: aus $(A \Rightarrow B)$ und $(B \Rightarrow C)$ gewinne $(A \Rightarrow C)$ klassische Schlussfigur des "modus ponens"
- indirekter Beweis: aus $(\neg A \Rightarrow \bot)$ gewinne A

(modus ponens) $\dfrac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta}$

korrekt (nachprüfen!)

Bem.: Anwendung von modus ponens 'schluckt' Hilfsformel φ; problematisch für (rückwärtsgerichtete) Beweissuche

Schnittregeln, von $\mathcal{SK}$ zu $\mathcal{SK}^+$

→ Abschnitt 6.4

(modus ponens) $\dfrac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta}$

Widerspruchsregel:

(Kontradiktion) $\dfrac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \neg\varphi}{\Gamma, \Gamma' \vdash \emptyset}$

jede konkrete Instanz von modus ponens oder Kontradiktion ist in $\mathcal{SK}$ eliminierbar (warum?)

Kontradiktion lässt sich direkt in $\mathcal{SK}$ + modus ponens herleiten

ebenso z.B. für die Schlussfigur des indirekten Beweises:

(Widerspruch) $\dfrac{\Gamma, \neg\varphi \vdash \psi \qquad \Gamma, \neg\varphi \vdash \neg\psi}{\Gamma \vdash \varphi}$

Teil 2: Logik erster Stufe (Prädikatenlogik), FO

Gegenstandsbereich:

S-Strukturen mit Belegungen für Element-Variablen

Ausdrucksmöglichkeiten:

atomare Aussagen über Terme Funktionen, Konstanten, Variablen

$\wedge, \vee, \neg$ (wie in AL)

Quantifizierung $\forall, \exists$ über Elemente

wesentliche Charakteristika von FO

- höheres Ausdrucksniveau
- strukturierte Formalisierung komplexerer Eigenschaften
- modulare Semantik
- korrekte und vollständige Beweiskalküle
- Kompaktheit
- nicht mehr entscheidbar

Motivierende Beispiele:

- $\forall x \, \exists y \; : \; x = y \cdot y$
- $\forall x \, \forall y \; : \; x \cdot y = y \cdot x$
- $1 + 1 = 0$
- $\forall x \, \exists y \;\; y > x \; \wedge \; \texttt{isprime}(y) \; \wedge \; \texttt{isprime(y+2)}$
- colinear$(\vec{x}, \vec{y}, \vec{z})$
- $\det\binom{x \; a}{y \; b}$

Strukturen zu Signatur S

$\rightarrow$ Abschnitt 1.1

Symbole:		
	$x, y, z, \ldots, x_1, x_2, x_3, \ldots$	Variablensymbole
	$c, d, e, \ldots$	Konstantensymbole
	$f, g, \ldots$	Funktionssymbole
	$P, Q, R, \ldots$	Relationssymbole

Signatur S: (vgl. *Klasse* beim OOP)
Auswahl von Konstanten-, $\underbrace{\text{Funktions- und Relationssymbolen}}_{\text{mit spezifizierten Stelligkeiten: Syntax!}}$

S-Struktur: (vgl. *Instanz* beim OOP)

$\mathcal{A} = (A, c^{\mathcal{A}}, \ldots, f^{\mathcal{A}}, \ldots, R^{\mathcal{A}}, \ldots)$ (Semantik)

besteht aus: Trägermenge $A \neq \emptyset$
für $c \in S$: ausgezeichnetes Element $c^{\mathcal{A}} \in A$.
für n-st. $f \in S$: n-st. Funktion $f^{\mathcal{A}} \colon A^n \rightarrow A$.
für n-st. $R \in S$: n-st. Relation $R^{\mathcal{A}} \subseteq A^n$.

Beispiel: $\mathcal{N} = \big(\mathbb{N}, +^{\mathcal{N}}, \cdot^{\mathcal{N}}, <^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}}\big)$ zu $S = \{+, \cdot, <, 0, 1\}$

Beispiele von Strukturtypen

unter vielen anderen

Wortstrukturen zu Signatur $S := \{<\} \cup \{P_a \colon a \in \Sigma\}$

$w = a_1 \ldots a_n \quad \longleftrightarrow \quad \mathcal{W} := \big(\{1, \ldots, n\}, <^{\mathcal{W}}, (P_a^{\mathcal{W}})_{a \in \Sigma}\big),$
$<^{\mathcal{W}} := \{(i,j) \colon 1 \leqslant i < j \leqslant n\},$
$P_a^{\mathcal{W}} := \{i \colon a_i = a\}.$

Graphen zu Signatur $S := \{E\}$

$u \bullet \xrightarrow{(u,v) \in E^{\mathcal{G}}} \bullet\, v$

$\mathcal{G} := \big(V, E^{\mathcal{G}}\big),$
mit Knotenmenge V
Kantenrelation $E^{\mathcal{G}} \subseteq V \times V$.

Transitionssysteme (NFA) zu Signatur $S := \{E_a \colon a \in \Sigma\}$

$(\Sigma, Q, \Delta) \quad \longleftrightarrow \quad \mathcal{A} := \big(Q, (E_a^{\mathcal{A}})_{a \in \Sigma}\big),$
$E_a^{\mathcal{A}} := \{(q, q') \colon (q, a, q') \in \Delta\}.$

Relationale Datenbanken, ...

Beispiele von Strukturen

natürliche Zahlen:
$\mathcal{N} = (\mathbb{N}, +^{\mathcal{N}}, \times^{\mathcal{N}}, <^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}})$ zu Signatur $\{+, \times, <, 0, 1\}$
alternativ (Peano): $(\mathbb{N}, ++^{\mathcal{N}}, =^{\mathcal{N}}, 0^{\mathcal{N}})$ zu $\{\text{succ}, =, 0\}$

ganze Zahlen:
$\mathcal{Z} = (\mathbb{Z}, -^{\mathcal{Z}}, \times^{\mathcal{Z}}, <^{\mathcal{Z}}, 1^{\mathcal{N}})$ zu Signatur $\{-, \times, <, 1\}$
aber auch zu Signatur $\{x^y, \div, \mathtt{prim}, \pi\}$ (!)

rationale Zahlen:
$\mathcal{Q} = (\mathbb{Q}, -^{\mathcal{Q}}, \times^{\mathcal{Q}}, \div^{\mathcal{Q}}, <^{\mathcal{Q}}, 0^{\mathcal{Q}}, 1^{\mathcal{Q}})$ zu Signatur $\{-, \times, \div, <, 0, 1\}$

ebenso **reelle Zahlen:** $\mathcal{R} = (\mathbb{R}, -^{\mathcal{R}}, \times^{\mathcal{R}}, \div^{\mathcal{R}}, <^{\mathcal{R}}, 0^{\mathcal{R}}, 1^{\mathcal{R}})$

komplexe Zahlen: $\mathcal{C} = (\mathbb{C}, -^{\mathcal{C}}, \times^{\mathcal{C}}, \div^{\mathcal{C}}, =^{\mathcal{C}}, 0^{\mathcal{C}}, 1^{\mathcal{C}})$

Bits: $\mathcal{B} = (\mathbb{B}, \mathtt{xor}, \wedge, \neq, 0, 1)$ zu $\{+, \times, <, 0, 1\}$

Terme

→ Abschnitt 1.2

Variablen aus $\mathcal{V} := \{x_1, x_2, \dots\}$ bzw. $\mathcal{V}_n := \{x_1, \dots, x_n\}$

S-Terme

$T(S)$ (über Variablen aus $\mathcal{V}$) induktiv erzeugt durch:

$x \in T(S)$ für $x \in \mathcal{V}$.
$c \in T(S)$ für $c \in S$.
$ft_1 \dots t_n \in T(S)$ für $f \in S$ (n-st.), $t_1, \dots, t_n \in T(S)$.

$T_n(S) \subseteq T(S)$: S-Terme über Variablen aus $\mathcal{V}_n$.

Beispiele wohlgeformter S-Terme

$S = \{f, c\}$, f 2-st.: c, $ffccc$, $fcfcc$, $\dots$, x_{17}, fx_1c, ffx_5cx_2, $\dots$

$S = \{+, \cdot, 0, 1\}$, $+, \cdot$ 2-st.: $\cdot + 11 + +111$,
$+ \cdot + + 111\, x_3\, x_1$, $\dots$

Konvention: Funktionsterme mit Klammern, 2-st. auch infix
$\big(((1+1)+1) \cdot x_3 + x_1\big)$ statt $+ \cdot + + 111 x_3 x_1$

Belegungen:

→ Abschnitt 1.3

weisen den Variablensymbolen Elemente einer S-Struktur zu

Belegung
über S-Struktur $\mathcal{A} = (A, c^{\mathcal{A}}, \dots, f^{\mathcal{A}}, \dots)$:

$$\begin{aligned} \beta \colon \mathcal{V} &\longrightarrow A \\ x &\longmapsto \beta(x) \end{aligned}$$

Idee: eine Belegung liefert *Interpretation* der Variablensymbole in S-Struktur

diese Interpretation läßt sich natürlich auf alle S-Terme erweitern (wie?)

$\longrightarrow$ **die Semantik von Termen**

Semantik von S-Termen

→ Abschnitt 1.2/3

in **S-Interpretation:** S-Struktur + Belegung $\mathfrak{I} = (\mathcal{A}, \beta)$

Semantik von Termen

induktiv über $T(S)$ für gegebene S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$:

Interpretation von $t \in T(S)$: $t^{\mathfrak{I}} \in A$ induktiv geg. durch

- $t = x$ ($x \in \mathcal{V}$ Variable) : $t^{\mathfrak{I}} := \beta(x)$.
- $t = c$ ($c \in S$ Konstante) : $t^{\mathfrak{I}} := c^{\mathcal{A}}$.
- $t = ft_1 \dots t_n$ ($f \in S$, n-st.) : $t^{\mathfrak{I}} := f^{\mathcal{A}}(t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}})$.

beachte Format dieser Interpretation als Abbildung

$$\boxed{\begin{aligned} T(S) &\longrightarrow A \\ t &\longmapsto t^{\mathfrak{I}} \end{aligned}}$$

und Abhängigkeit von S-Struktur $\mathcal{A}$ *und* Belegung β.

Herbrand-Struktur: die syntaktische Interpretation

für funktionales S (ohne Relationssymbole)

Herbrand-Struktur
$\mathcal{T} = \mathcal{T}(S) = \big(T(S), \ldots, c^{\mathcal{T}(S)}, \ldots, f^{\mathcal{T}(S)}, \ldots\big)$

- $c \in S$: $\quad c^{\mathcal{T}} := c \in T(S)$.
- $f \in S$ (n-st.): $\quad \begin{array}{rcl} f^{\mathcal{T}}\colon T(S)^n & \longrightarrow & T(S) \\ (t_1, \ldots, t_n) & \longmapsto & ft_1 \ldots t_n. \end{array}$

(die einzig plausible Wahl . . . , warum?)

Beobachtung (Übung 1.7, vgl. auch FGdI I)

für jede S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$ ist die Abbildung

$$\begin{array}{rcl} h\colon T(S) & \longrightarrow & A \\ t & \longmapsto & t^{\mathfrak{I}} \end{array}$$

ein Homomorphismus von $\mathcal{T}(S)$ nach $\mathcal{A}$.

Logik erster Stufe: Syntax von $\mathrm{FO}(S)$ → Abschnitt 2.1

Symbole: Symbole in S zusammen mit Variablen $x \in \mathcal{V}$, AL-Junktoren, $=$, $\forall, \exists$, Klammern

induktive Definition der Menge der $\mathrm{FO}(S)$ Formeln:

- **atomare Formeln**: für $t_1, t_2 \in T(S)$: $\quad t_1 = t_2 \in \mathrm{FO}(S)$.
  für $R \in S$ (n-st.)*, $t_1, \ldots, t_n \in T(S)$: $\quad Rt_1 \ldots t_n \in \mathrm{FO}(S)$.
  * für $n = 2$: auch infixe Notation
- **AL-Junktoren**: für $\varphi, \psi \in \mathrm{FO}(S)$: $\quad \neg\varphi \in \mathrm{FO}(S)$.
  $(\varphi \wedge \psi) \in \mathrm{FO}(S)$.
  $(\varphi \vee \psi) \in \mathrm{FO}(S)$.
- **Quantifizierung**: für $\varphi \in \mathrm{FO}(S)$, $x \in \mathcal{V}$: $\quad \exists x\varphi \in \mathrm{FO}(S)$.
  $\forall x\varphi \in \mathrm{FO}(S)$.

Gleichheitsfreie Logik erster Stufe, $\mathrm{FO}^{\neq} \subseteq \mathrm{FO}$:
genauso, aber ohne Atome $t_1 = t_2$.

Syntax: freie Variablen (Definition 2.2)

induktiv über Aufbau der Formeln definiere Funktion

$$\boxed{\begin{array}{rcl} \mathrm{frei}\colon \mathrm{FO}(S) & \longrightarrow & \mathcal{P}(\mathcal{V}) \\ \varphi & \longmapsto & \mathrm{frei}(\varphi) \subseteq \mathcal{V} \end{array}}$$

induktiv gemäß: $\mathrm{frei}(\varphi) := \mathrm{var}(\varphi)$ für atomare φ.
$\mathrm{frei}(\neg\varphi) := \mathrm{frei}(\varphi)$.
$\mathrm{frei}(\varphi \wedge \psi) = \mathrm{frei}(\varphi \vee \psi) := \mathrm{frei}(\varphi) \cup \mathrm{frei}(\psi)$.
$\mathrm{frei}(\exists x\varphi) = \mathrm{frei}(\forall x\varphi) := \mathrm{frei}(\varphi) \setminus \{x\}$.

Formeln ohne freie Variablen: **Sätze**

$\mathrm{FO}_n(S) := \{\varphi \in \mathrm{FO}(S) \colon \mathrm{frei}(\varphi) \subseteq \mathcal{V}_n\}$.

Schreibweise: $\varphi(x_1, \ldots, x_n)$ für $\varphi \in \mathrm{FO}_n(S)$.

Variablen in φ, die nicht frei vorkommen: *gebunden*

Beispiele: $\mathrm{frei}(0 < fx) = \{x\}$ $\quad \mathrm{frei}(0 < fx \wedge \forall x\, \neg x = fx) = \{x\}$
$\mathrm{frei}(\forall x\, \neg x = fx) = \emptyset$

Syntax: Quantorenrang (Definition 2.3)

induktiv über Aufbau der Formeln definiere Funktion

$$\boxed{\begin{array}{rcl} \mathrm{qr}\colon \mathrm{FO}(S) & \longrightarrow & \mathbb{N} \\ \varphi & \longmapsto & \mathrm{qr}(\varphi) \in \mathbb{N} \end{array}}$$

induktiv gemäß: $\mathrm{qr}(\varphi) = 0$ für atomares φ.
$\mathrm{qr}(\neg\varphi) := \mathrm{qr}(\varphi)$.
$\mathrm{qr}(\varphi \wedge \psi) = \mathrm{qr}(\varphi \vee \psi) := \max(\mathrm{qr}(\varphi), \mathrm{qr}(\psi))$.
$\mathrm{qr}(\exists x\varphi) = \mathrm{qr}(\forall x\varphi) := \mathrm{qr}(\varphi) + 1$.

Formeln von Quantorenrang 0 heißen *quantorenfrei*.

Beispiele: $\mathrm{qr}(0 < fx) = 0$
$\mathrm{qr}(\forall x \exists y\, x < y) = 2$
$\mathrm{qr}(0 < fx \wedge \forall x \exists y\, x < y) = 2$

Alfred Tarski (1901–1983)

Logiker, der die semantische Sicht auf FO wesentlich geprägt hat

Semantik von FO(S) → Abschnitt 2.2

Wahrheitswerte $\varphi^{\mathfrak{I}}$ für $\mathrm{FO}(S)$-Formeln über S-Interpretation $\mathfrak{I}$

induktive Definition von $\varphi^{\mathfrak{I}}$

atomare φ: $(t_1 = t_2)^{\mathfrak{I}} = 1$ gdw. $t_1^{\mathfrak{I}} = t_2^{\mathfrak{I}}$.
$(Rt_1 \dots t_n)^{\mathfrak{I}} = 1$ gdw. $(t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}}) \in R^{\mathcal{A}}$.

Negation: $(\neg\varphi)^{\mathfrak{I}} := 1 - \varphi^{\mathfrak{I}}$.

Konjunktion: $(\varphi \wedge \psi)^{\mathfrak{I}} := \min(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.

Disjunktion: $(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.

Quantoren: $(\exists x\varphi)^{\mathfrak{I}} = \max\big(\varphi^{\mathfrak{I}[x\mapsto a]} : a \in A\big)$.
$(\forall x\varphi)^{\mathfrak{I}} = \min\big(\varphi^{\mathfrak{I}[x\mapsto a]} : a \in A\big)$.

Semantik der Quantoren arbeitet mit *modifizierten Belegungen*

$$\beta[x \mapsto a](y) := \begin{cases} \beta(y) & \text{für } y \in \mathcal{V} \setminus \{x\} \\ a & \text{für } y = x \end{cases}$$

$$\mathfrak{I}[x \mapsto a] = (\mathcal{A}, \beta[x \mapsto a])$$

Semantik von FO(S)

Wahrheitswert $\varphi^{\mathfrak{I}} \in \mathbb{B}$ definiert für alle $\varphi \in \mathrm{FO}(S)$ und S-Interpretationen $\mathfrak{I} = (\mathcal{A}, \beta)$

Sprech- und Schreibweisen:

für $\varphi^{\mathfrak{I}} = 1$: φ *wahr* unter $\mathfrak{I}$
$\mathfrak{I}$ erfüllt φ
$\mathfrak{I}$ Modell von φ
$\mathfrak{I} \models \varphi$

für $\varphi^{\mathfrak{I}} = 0$: φ *falsch* unter $\mathfrak{I}$
$\mathfrak{I}$ erfüllt φ nicht
$\mathfrak{I}$ kein Modell von φ
$\mathfrak{I} \not\models \varphi$

Beispiel: Ist $(\mathbb{Q}, 0, 1, \cdot, +)$ ein Modell von
$\forall x\, \exists y : \; x = 0 \;\vee\; x \cdot y = 1$?

Belegungen und freie Variablen

Werte der Belegung $\beta(x) \in A$ über $\mathcal{A}$ nur relevant für $x \in \mathrm{frei}(\varphi)$.

Beweis durch Induktion über $\varphi \in \mathrm{FO}(S)$!

Für $\varphi(x_1, \dots, x_n) \in \mathrm{FO}_n(S)$ (d.h. $\mathrm{frei}(\varphi) \subseteq \mathcal{V}_n = \{x_1, \dots, x_n\}$),
$(a_1, \dots, a_n) = \big(\beta(x_1), \dots, \beta(x_n)\big) \in A^n$:

$$\mathcal{A} \models \varphi[a_1, \dots, a_n] \quad :\text{gdw.} \left[\begin{array}{l} (\mathcal{A}, \beta) \models \varphi \text{ für ein/alle } \beta \text{ mit} \\ \beta(x_i) = a_i \text{ für } i = 1, \dots n \end{array}\right].$$

Beispiel: $\varphi(x) = \forall y Rxy$ beschreibt eine Eigenschaft von x,
$\varphi^{\mathfrak{I}}$ hängt nicht von $\beta(y)$ ab, aber von $\beta(x)$

speziell für **Sätze** φ (d.h. mit $\mathrm{frei}(\varphi) = \emptyset$):
$\varphi^{\mathfrak{I}}$ hängt nur von $\mathcal{A}$ ab; entweder $\mathcal{A} \models \varphi$ oder $\mathcal{A} \not\models \varphi$,
*un*abhängig von β

semantische Grundegriffe → Abschnitt 2.3

übertragen sich direkt von AL auf FO!

Folgerungsbeziehung, $\varphi \models \psi$: f.a. $\mathfrak{I}$ gilt $(\mathfrak{I} \models \varphi \;\Rightarrow\; \mathfrak{I} \models \psi)$.

logische Äquivalenz, $\varphi \equiv \psi$: f.a. $\mathfrak{I}$ gilt $(\mathfrak{I} \models \varphi \;\Leftrightarrow\; \mathfrak{I} \models \psi)$.
vgl. *Erfüllbarkeitsäquivalenz* (später)

Erfüllbarkeit, $\varphi \in \mathrm{SAT}(\mathrm{FO})$: es gibt $\mathfrak{I}$ mit $\mathfrak{I} \models \varphi$.

Allgemeingültigkeit: für alle $\mathfrak{I}$ gilt $\mathfrak{I} \models \varphi$.

Äquivalent?
- $\forall x \forall y \varphi(x,y) \;\equiv\; \forall y \forall x \varphi(x,y)$?
- $\forall x \varphi \;\equiv\; \neg\exists x \neg\varphi$?

Erfüllbar?
- $\forall x \exists y Rxy \;\wedge\; \neg\exists y \forall x Rxy$?
- $\forall x \forall y (Rxy \;\wedge\; \neg Ryx)$?
- $\forall x \forall y \big(x = y \;\vee (Rxy \leftrightarrow \neg Ryx)\big)$?

Variationen: relationale Semantik → Abschnitt 2.4

mit $\varphi(x_1,\dots,x_n) \in \mathrm{FO}_n(S)$ und S-Struktur $\mathcal{A}$
assoziiere die n-stellige Relation

$$\boxed{[\![\varphi]\!]^{\mathcal{A}} := \big\{\mathbf{a} = (a_1,\dots,a_n) \in A^n \colon \mathcal{A} \models \varphi[\mathbf{a}]\big\} \;\subseteq\; A^n}$$

$\longrightarrow$ relationale Algebra

Korrespondenzen:
Konjunktion $\wedge$ — Durchschnitt $\cap$
Disjunktion $\vee$ — Vereinigung $\cup$
Negation $\neg$ — Komplement
existenzielle Quant. $\exists$ — Projektion

$\longrightarrow$ relationale Datenbanken, SQL

Variationen: Spielsemantik → Abschnitt 2.4

model checking Spiel für φ in Negations-Normalform (NNF)

NNF: alle Negationen nach innen;
Aufbau mit nur $\forall, \exists, \wedge, \vee$ (ohne $\neg$)
aus Atomen und negierten Atomen

allgemeiner Ansatz:

zu geg. $\mathfrak{I}$ und φ Spiel zwischen zwei Spielern

Verifizierer **V** will $\mathfrak{I} \models \varphi$ *nachweisen*
Falsifizierer **F** will $\mathfrak{I} \models \varphi$ *widerlegen*

Spiel-Positionen: $(\psi, \mathbf{a}) \in \mathrm{SF}(\varphi) \times A^n$

Spiel-Züge/Regeln so gemacht, dass

$$\left.\begin{array}{l}\mathbf{V}\\ \mathbf{F}\end{array}\right\} \text{ Gewinnstrategie in Position } (\psi,\mathbf{a}) \text{ hat, gdw. } \left\{\begin{array}{l}\mathcal{A} \models \psi[\mathbf{a}]\\ \mathcal{A} \not\models \psi[\mathbf{a}]\end{array}\right.$$

Spielsemantik – Semantik-Spiel

zu $\varphi(x_1,\dots,x_n) \in \mathrm{FO}_n(S)$ über $\mathcal{A}$ in NNF

mit Spielpositionen $(\psi, \mathbf{a}) \in \mathrm{SF}(\varphi) \times A^n$

Züge in Position $(\psi, \mathbf{a})$, $\mathbf{a} = (a_1,\dots,a_n)$:

$\psi = \psi_1 \wedge \psi_2$	**F** am Zug zieht nach $(\psi_1, \mathbf{a})$ oder nach $(\psi_2, \mathbf{a})$.
$\psi = \psi_1 \vee \psi_2$	**V** am Zug zieht nach $(\psi_1, \mathbf{a})$ oder nach $(\psi_2, \mathbf{a})$.
$\psi = \forall x_i \psi_0$	**F** am Zug zieht nach einem $(\psi_0, \mathbf{a}[x_i \mapsto a_i'])$.
$\psi = \exists x_i \psi_0$	**V** am Zug zieht nach einem $(\psi_0, \mathbf{a}[x_i \mapsto a_i'])$.

Spiel-Ende in Positionen $(\psi, \mathbf{a})$, ψ atomar oder negiert atomar.

Gewinner: **V** gewinnt in Endposition $(\psi, \mathbf{a})$, wenn $\mathcal{A} \models \psi[\mathbf{a}]$.
F gewinnt in Endposition $(\psi, \mathbf{a})$, wenn $\mathcal{A} \not\models \psi[\mathbf{a}]$.

Spielsemantik – Semantik-Spiel

Satz:

$\mathcal{A} \models \psi[\mathbf{a}] \;\Leftrightarrow\;$ **V** hat Gewinnstrategie in Position $(\psi, \mathbf{a})$.

reduziert Auswertung auf Spielanalyse
oft mit algorithmisch optimaler Komplexität

Frage: Spiel für φ, das nicht in NNF ist?

das Konzept der Gleichung in der Algebra Robert Recorde

Arzt und früher Popularisierer der "Algebra"

der Erfinder des Gleichheitszeichens!

FO mit oder ohne = ? → Abschnitt 2.5

FO und $\mathrm{FO}^{\neq}$

- Gleichheit ist Bestandteil der *Logik* in FO;
  anders als interpretierte Relationen $R \in S$.
- natürliche Formalisierungen brauchen oft $=$,
  z.B.: Injektivität, algebraische Identitäten, ...
- dennoch möglich: Reduktion von FO auf $\mathrm{FO}^{\neq}$;
  Idee: modelliere $=$ durch interpretierte Relation $\sim$.

$\hat{S} := S \cup \{\sim\}$

Verträglichkeitsbedingungen:
$\sim$ Kongruenzrelation bzgl. aller $R, f \in S$

erhalte Modelle $\mathcal{A}_0$ mit echter Gleichheit als $\sim$-Quotienten:

$\mathcal{A}_0 = \mathcal{A}/\!\sim^{\mathcal{A}} = \big(A/\!\sim^{\mathcal{A}}, \ldots, [c^{\mathcal{A}}]_{\sim^{\mathcal{A}}}, \ldots, f^{\mathcal{A}}/\!\sim^{\mathcal{A}}, \ldots, R^{\mathcal{A}}/\!\sim^{\mathcal{A}}\big)$

$\sim$-Äquivalenzklassen als Elemente

Pränexe Normalform → Abschnitt 3.1

$\varphi \in \mathrm{FO}(S)$ in *pränexer Normalform* (PNF):

$$\boxed{\begin{array}{l}\varphi = Q_1 x_{i_1} \ldots Q_k x_{i_k} \psi, \\ Q_i \in \{\forall, \exists\},\; k \in \mathbb{N},\; \psi \text{ quantorenfrei.}\end{array}}$$

Beispiele

$$\exists y (Exy \wedge \forall x (Eyx \rightarrow x = y)) \;\equiv\; \exists y \forall z \big(Exy \wedge (Eyz \rightarrow z = y)\big)$$

$$\exists y \forall x Exy \vee \neg \exists y Exy \;\equiv\; \exists y_1 \forall y_2 \forall y_3 \big(Ey_2 y_1 \vee \neg Exy_3\big)$$

Satz über PNF

Jede FO-Formel ist logisch äquivalent zu einer Formel in PNF.

Beweis durch Induktion über $\varphi \in \mathrm{FO}(S)$.

Substitution → Abschnitt 3.2

das semantisch korrekte Einsetzen von Termen

gesucht: für $t \in T(S)$ und $\varphi(x) \in \mathrm{FO}(S)$,
$\varphi' := \varphi(t/x) \in \mathrm{FO}(S)$ so, dass:

$$\boxed{\mathfrak{I} \models \varphi' \quad \Leftrightarrow \quad \mathfrak{I}[x \mapsto t^{\mathfrak{I}}] \models \varphi.}$$

Vorsicht! Naives Ersetzen von x durch t tut's nicht!

- beachte, dass x frei und gebunden auftreten kann.
- beachte, dass Variablen in t nicht fälschlich gebunden werden.

Methode
Induktive Definition, die intern gebundene Variablen so umbenennt, dass Konflikte vermieden werden.

Beispiel: $\varphi(x) = \forall y \big(Exy \wedge \exists x \neg Exy\big)$

$\varphi(fy/x) = ?$

Thoralf Skolem (1887–1963)

Logik, Modelltheorie, Mengenlehre

Skolemisierung: alles universell ? → Abschnitt 3.3

universell-pränexe Formeln: $\forall x_{i_1} \dots \forall x_{i_k}\, \psi$, ψ quantorenfrei

- nicht jede Formel ist logisch äquivalent zu universell-pränexer Formel, z.B. $\varphi = \forall x \exists y\, Exy$
- aber jede Formel ist *erfüllbarkeitsäquivalent* zu universell-pränexer Formel.

Idee: neue Funktionen, die *ggf.* Existenzbeispiele liefern
[vgl. $\exists$-Züge für **V** im Semantik Spiel]

Beispiel

$\varphi = \forall x \exists y\, Exy \quad \longmapsto \quad \varphi' = \forall x\, Exfx \qquad$ (für *neues* f)

dann gilt:

(i) $\mathcal{A}' = (A, E^{\mathcal{A}}, \dots, f^{\mathcal{A}'}) \models \varphi' \;\Rightarrow\; \mathcal{A} = (A, E^{\mathcal{A}}, \dots) \models \varphi$

(ii) $\mathcal{A} = (A, E^{\mathcal{A}}, \dots) \models \varphi \;\Rightarrow\;$ es gibt $f^{\mathcal{A}}$ über A, sodass $\mathcal{A}' = (A, E^{\mathcal{A}}, \dots, f^{\mathcal{A}'}) \models \varphi'$

Skolemnormalform (Satz 3.6)

Satz über die Skolemnormalform

Jedes $\varphi \in \mathrm{FO}$ ist *erfüllbarkeitsäquivalent* zu einer universell-pränexen Formel φ' (in einer erweiterten Signatur).

Man erhält φ' aus einer zu φ logisch äquivalenten Formel in PNF durch Substitution von *Skolemfunktions*termen für existentiell abquantifizierte Variablen.

Zur Erfüllbarkeitsäquivalenz gilt sogar:

- $\varphi' \models \varphi$.
- jedes Modell von φ lässt sich zu Modell von φ' erweitern.

Jacques Herbrand (1908–1931)

Logiker und Algebraiker

Satz von Herbrand → Abschnitt 3.4

zur Erfüllbarkeit von universellen $\mathrm{FO}^{\neq}$-Sätzen in Herbrand-Modellen

- S enthalte mindestens ein Konstantensymbol
- geg. $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$: Satzmenge, *universell & gleichheitsfrei*

Herbrand-Struktur (Erinnerung):
die S_{F}-Termstruktur $\mathcal{T}_0(S)$ über $T_0(S)$ (variablenfreie S-Terme)

Herbrand-Modell:
Expansion der Termstruktur $\mathcal{T}_0(S)$ zu S-Struktur,
— durch Interpretation von R (n-st.) als Teilmenge von $T_0(S)^n$ —
zu einem Modell von Φ

Gleichheitsfreiheit notwendig,
z.B. $x \cdot x + 2x + 1 = (x+1) \cdot (x+1)$.

Es gibt ein abzählbares Modell von $(\mathbb{R}, +, \times, 0, 1, <)$

Satz von Herbrand (Satz 3.10)

Satz von Herbrand

Sei $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ Menge von *universellen, gleichheitsfreien* Sätzen;
S habe mindestens ein Konstantensymbol.

Dann gilt: $\boxed{\Phi \text{ erfüllbar } \Leftrightarrow \text{ es existiert ein Herbrand-Modell } \mathcal{H} = (\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}) \models \Phi.}$

Vgl. Computeralgebrasysteme:
symbolisches Rechnen mit Relationen zwischen Termen. . .

Beweis

"$\Leftarrow$": offensichtlich.
"$\Rightarrow$": Gelte $\mathcal{A} \models \Phi$, dann setze
$R^{\mathcal{H}} := \{(t_1, \dots, t_n) : t_j \in \mathcal{T}_0(S),\ (t_1^{\mathcal{A}}, \dots, t_n^{\mathcal{A}}) \in R^{\mathcal{A}}\}$.

Erfüllbarkeit: Reduktion auf AL → Abschnitt 3.5

Reduktions-Idee: $\Phi \subseteq \mathrm{FO}(S)$ (bel. Formelmenge)

erf.-äquiv.

$\Phi' \subseteq \mathrm{FO}_0(S_1)$ (Satzmenge)

erf.-äquiv.

$\Phi'' \subseteq \mathrm{FO}_0^{\neq}(S_2)$ (gleichheitsfrei)

erf.-äquiv.

$\Phi''' \subseteq \mathrm{FO}_0^{\neq}(S_3)$ (universell(-pränex))

$\boxed{\Phi \text{ erfüllbar } \Leftrightarrow \Phi''' \text{ erfüllbar } \Leftrightarrow \Phi''' \text{ in Herbrand-Modell erfüllbar}}$

und Bedingungen an Herbrand-Modell lassen sich in AL kodieren!

Beispiel

$S = \{R, Q, f\}$ R (2-st.), Q (1-st.), Relationssymbole
f (1-st.), Funktionssymbol

Behauptung: $\Phi : \begin{cases} \varphi_1 = \forall x \forall y \big(Rxy \to (Qx \leftrightarrow \neg Qy)\big) \\ \varphi_2 = \forall x (Rxfx \vee Rfxx) \\ \varphi_3 = \forall x \forall y \big(\neg Rxy \to Rxffy\big) \end{cases}$

ist unerfüllbar

$S_c := S \cup \{c\}$ $T_0(S_c) = \{c, fc, ffc, fffc, \dots\} = \{f^n c \colon n \in \mathbb{N}\}$

AL-Variablen für die Reduktion:

q_n $(= p_{\mathtt{Qf^n c}})$ für die Atome $Qf^n c$, $(n \in \mathbb{N})$,
$r_{\ell,m}$ $(= p_{\mathtt{Rf^\ell cf^m c}})$ für die Atome $Rf^\ell cf^m c$, $(\ell, m \in \mathbb{N})$.

wir erhalten z.B. für φ_1 die AL-Formelmenge

$$[\![\varphi_1]\!]^{\mathrm{AL}} = \big\{ r_{\ell,m} \to (q_\ell \leftrightarrow \neg q_m) : \ell, m \in \mathbb{N} \big\}$$

Beispiel (fortges.)

zugeh. AL-Formelmengen zu $\varphi_1, \varphi_2, \varphi_3$:

$$\begin{cases} [\![\varphi_1]\!]^{\mathrm{AL}} = \big\{ r_{\ell,m} \to (q_\ell \leftrightarrow \neg q_m) : \ell, m \in \mathbb{N} \big\} \\ [\![\varphi_2]\!]^{\mathrm{AL}} = \big\{ r_{\ell,\ell+1} \vee r_{\ell+1,\ell} : \ell \in \mathbb{N} \big\} \\ [\![\varphi_3]\!]^{\mathrm{AL}} = \big\{ \neg r_{\ell,m} \to r_{\ell,m+2} : \ell, m \in \mathbb{N} \big\} \end{cases}$$

Unerfüllbarkeit von Φ folgt daher z.B. aus AL-Unerfüllbarkeit von

$$\underbrace{\begin{array}{l} r_{0,0} \to (q_0 \leftrightarrow \neg q_0), \\ r_{0,1} \to (q_0 \leftrightarrow \neg q_1), \\ r_{1,0} \to (q_1 \leftrightarrow \neg q_0), \\ r_{0,2} \to (q_0 \leftrightarrow \neg q_2), \\ r_{1,2} \to (q_1 \leftrightarrow \neg q_2), \\ r_{2,1} \to (q_2 \leftrightarrow \neg q_1), \end{array}}_{\in [\![\varphi_1]\!]^{\mathrm{AL}}} \quad \underbrace{\begin{array}{l} r_{0,1} \vee r_{1,0}, \\ r_{1,2} \vee r_{2,1}, \end{array}}_{\in [\![\varphi_2]\!]^{\mathrm{AL}}} \quad \underbrace{\neg r_{0,0} \to r_{0,2}}_{\in [\![\varphi_3]\!]^{\mathrm{AL}}}$$

Erfüllbarkeit: Reduktion auf AL

für universell-pränexes $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ über S mit Konstanten

Φ erfüllbar $\Leftrightarrow$ Φ hat ein Herbrand-Modell
$\mathcal{H} = (\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}) \models \Phi$

$\Leftrightarrow$ für alle $R \in S$ (n-st.) existieren $R^{\mathcal{H}} \subseteq T_0(S)^n$,
sodass $\mathcal{H} = (\mathcal{T}_0(S), (R^{\mathcal{H}})_{R \in S}) \models \Phi$

$$\mathcal{V} := \big\{ p_\alpha \colon \alpha \text{ relationales Atom über } T_0(S) \big\}$$

$$\alpha = \mathtt{R}\mathtt{t}_1 \dots \mathtt{t}_n;\, R \in S;\, t_1, \dots, t_n \in T_0(S),\ R \in S \ (n\text{-stellig})$$

$\mathcal{V}$-Interpretationen $\mathfrak{I}$ beschreiben dann mögliche $\mathcal{H}$:
bijektive Korrepondenz $\mathcal{H} \leftrightarrow \mathfrak{I}$:

---

von $\mathfrak{I}$ zu $\mathcal{H} = \mathcal{H}(\mathfrak{I})$: $R^{\mathcal{H}} = \big\{ (t_1, \dots, t_n) \in T_0(S)^n \colon \mathfrak{I}(p_{\mathtt{Rt_1 \dots t_n}}) = 1 \big\}$

von $\mathcal{H}$ zu $\mathfrak{I} = \mathfrak{I}(\mathcal{H})$: $\mathfrak{I} \colon \mathcal{V} \longrightarrow \mathbb{B}$

$$p_\alpha \longmapsto \begin{cases} 1 & \text{falls } \mathcal{H} \models \alpha, \\ 0 & \text{falls } \mathcal{H} \models \neg\alpha. \end{cases}$$

Erfüllbarkeit: Reduktion auf AL

Beispiel $\xi(\mathbf{t})^{\mathbf{AL}} \in \mathbf{AL}(\mathcal{V})$

$\left.\begin{array}{r} \xi = Rxfy \vee (Ufx \to Wxyfz) \\ \mathbf{t} = (c, fc, d) \text{ für } (x, y, z) \end{array}\right\}$ liefert

$$\xi(c, fc, d)^{\mathrm{AL}} = p_{\mathtt{Rcffc}} \vee (p_{\mathtt{Ufc}} \to p_{\mathtt{Wcfcfd}})$$

$\left.\begin{array}{r} \xi = Rxy \to (Qx \leftrightarrow \neg Qy) \\ \mathbf{t} = (f^n c, f^m c) \text{ für } (x, y) \end{array}\right\}$ liefert

$$\xi(f^n c, f^m c)^{\mathrm{AL}} = p_{\mathtt{Rf^n f^m c}} \to (p_{\mathtt{Qf^n c}} \leftrightarrow \neg p_{\mathtt{Qf^m c}})$$

Erfüllbarkeit: Reduktion auf AL

für $\varphi = \forall x_1 \ldots \forall x_n\, \xi(x_1, \ldots, x_n) = \forall \mathbf{x}\, \xi(\mathbf{x})$, ξ quantorenfrei
und $\mathcal{H} = \mathcal{H}(\mathfrak{I})$ gilt:

$\mathcal{H} \models \varphi$ gdw. $\mathcal{H} \models \xi[\mathbf{t}]$ für alle $\mathbf{t} = (t_1, \ldots, t_n) \in T_0(S)^n$

gdw. $\mathfrak{I} \models \xi(\mathbf{t})^{\mathrm{AL}}$ für alle $\mathbf{t} = (t_1, \ldots, t_n) \in T_0(S)^n$

dabei erhält man $\xi(\mathbf{t})^{\mathrm{AL}} \in \mathrm{AL}(\mathcal{V})$ aus $\xi(\mathbf{t})$
durch Ersetzen von Atomen $\alpha = \mathtt{R}\ldots$
durch AL-Variablen p_α

für $[\![\Phi]\!]^{\mathrm{AL}} := \bigcup_{\forall \mathbf{x}\xi \in \Phi} \{\xi(\mathbf{t})^{\mathrm{AL}} \colon \mathbf{t} \text{ in } T_0(S)\}$ gilt:

$$\boxed{\mathbf{\Phi} \textbf{ erfüllbar gdw. } [\![\mathbf{\Phi}]\!]^{\mathrm{AL}} \textbf{ erfüllbar}}$$

FO Kompaktheit (Satz 4.1)

Kompaktheitssatz (Endlichkeitssatz)

Version 1: (Erfüllbarkeit)

Für $\Phi \subseteq \mathrm{FO}$ sind äquivalent:

(i) Φ erfüllbar.

(ii) Jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ ist erfüllbar.

Version 2: (Folgerungsbeziehung)

Für $\Phi \subseteq \mathrm{FO}, \varphi \in \mathrm{FO}$ sind äquivalent:

(i) $\Phi \models \varphi$.

(ii) $\Phi_0 \models \varphi$ für eine endliche Teilmenge $\Phi_0 \subseteq \Phi$.

Version 1 $\Leftrightarrow$ Version 2 (zur Übung!)
Version 1 für universell-pränexes $\Phi \subseteq \mathrm{FO}_0^{\neq}$: Reduktion auf AL

FO Kompaktheit → Abschnitt 4

Konsequenzen: die Stärken des Endlichkeitssatzes
die Grenzen von FO

mit Kompaktheit findet man:

beliebig große endliche Modelle $\Rightarrow$ unendliche Modelle

zu Φ betrachte $\Phi \cup \{\exists x_1 \ldots \exists x_n \bigwedge_{1 \leqslant i < j \leqslant n} \neg x_i = x_j \colon n \geqslant 1\}$

unendliche Modelle $\Rightarrow$ beliebig große unendliche Modelle

zu Φ betrachte $\Phi \cup \{\neg c_i = c_j \colon i \neq j; i, j \in I\}$
für neue Konstanten $(c_i)_{i \in I}$

$\Rightarrow$ *keine* unendliche Struktur in FO
bis auf Isomorphie charakterisierbar

FO Kompaktheit

Konsequenzen: Grenzen von FO

mit Kompaktheitsargumenten findet man:

Nichtstandardmodelle

von (unendlichen) Standardmodellen
in FO ununterscheidbare Strukturen

z.B. $\mathcal{N}^*$ zu $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$
Nichtstandardmodell der Arithmetik mit
'unendlich großen natürlichen Zahlen'

zur vollständigen FO-Theorie von $\mathcal{N}$, $\Phi := \{\varphi \in \mathrm{FO} \colon \mathcal{N} \models \varphi\}$

betrachte $\Phi \cup \{\underbrace{1 + \cdots + 1}_{n} < c \colon n \geqslant 2\}$ für neue Konstante c

Vgl. Nichtstandard Analysis, u.a. Detlev Laugwitz:
"*Infinitesimalkalkül: Kontinuum und Zahlen*", BI (1978).

Einschub: Axiome der natürlichen Zahlen

Peano: Signatur $S := (0, N)$ mit unärem Funktionssymbol N

1) $\forall x\, \neg 0 = Nx$, $\quad \forall x\, \exists y\; x = 0 \vee x = Ny$
2) $\forall x, y\; x = y \vee \neg Nx = Ny$

3') Die *natürlichen Zahlen* sind die kleinste Menge mit 1)+2)

3) Für jedes $\varphi(x) \in \mathrm{FO}(S)$ gilt:

$$\varphi(0) \wedge (\forall x \varphi(x) \rightarrow \varphi(Nx)) \rightarrow \forall x \varphi(x)$$

Arithmetik: Signatur $(0, 1, +, \cdot, \leqslant)$

- $1 := N0, \quad x + 0 := x, \quad x + Ny := N(x + y)$
- $x + y = y + x, \quad (x + y) + z = x + (y + z)$
- $x \cdot 0 := 0, \quad x \cdot Ny := x \cdot y + x$
- $x \cdot y = y \cdot x, \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $x \cdot (y + z) = x \cdot y + x \cdot z$
- $x \leqslant y \quad :\Leftrightarrow \quad \exists z : y = x + z$
- $x \leqslant y \;\rightarrow\; x + z \leqslant y + z \;\wedge\; x \cdot z \leqslant y \cdot z$

Sequenzenkalküle

→ Abschnitt 6.1

vgl. AL Sequenzenkalkül

Allgemeingültigkeitsbeweise (für bel. FO-Formeln/Sätze)

Gegenstand: FO-*Sequenzen* $\Gamma \vdash \Delta$
für endliche $\Gamma, \Delta \subseteq \mathrm{FO}_0(S)$

$\Gamma \vdash \Delta$ *allgemeingültig* wenn $\bigwedge \Gamma \models \bigvee \Delta$

Beweisziel: Ableitung allgemeingültiger Sequenzen

Ableitungsschritte: Anwendung von *Regeln*
(zur Erzeugung von Sequenzen)

Korrektheit: jede ableitbare Sequenz ist allgemeingültig.

Vollständigkeit: jede allgemeingültige Sequenz ist ableitbar.
(schwache Form, wird später verschärft)

Sequenzenkalkül: Regeln und Korrektheit

Format von *Sequenzenregeln* (wie in AL): $\dfrac{\text{Prämissen}}{\text{Konklusion}}$

Konklusionen von Regeln ohne Prämissen: *Axiome*

ableitbare Sequenzen:
ausgehend von Axiomen (in endlich vielen Schritten) durch Anwendung von Sequenzenregeln erzeugte Sequenzen

Korrektheit: jede ableitbare Sequenz ist allgemeingültig

folgt aus der Korrektheit der einzelnen Regeln:

- die Axiome sind allgemeingültige Sequenzen;
- für Regeln mit Prämissen:
  Prämissen allgemeingültig $\Rightarrow$ Konklusion allgemeingültig.

Sequenzenkalkül: Regeln

FO Sequenzenkalkül $\mathcal{SK}$, drei Gruppen von Regeln:

- *AL Regeln* (analog zum AL-Sequenzenkalkül).
- *Quantorenregeln*: Einführung von $\forall$ oder $\exists$ links/rechts.
  $(\forall\mathrm{L})$, $(\forall\mathrm{R})$, $(\exists\mathrm{L})$, $(\exists\mathrm{R})$.
- *Gleichheitsregeln*: Umgang mit Term-Gleichheiten.
  $(=)$, (Sub-L), (Sub-R).

AL + Quantorenregeln: vollständiger Beweiskalkül $\mathcal{SK}^{\neq}$ für $\mathrm{FO}^{\neq}$
$\mathcal{SK}^{\neq}$ + Gleichheitsregeln: vollständiger Beweiskalkül $\mathcal{SK}$ für FO

Zusätzlich (nicht notwendig aber natürlich) in $\mathcal{SK}^{+}$:

- *Schnittregeln*: Kettenschlüsse und Beweise durch Widerspruch.

Sequenzenkalkül: Quantorenregeln

$(\forall L)\ \dfrac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, \forall x \varphi(x) \vdash \Delta}$ $\qquad(\forall R)\ \dfrac{\Gamma \vdash \Delta, \varphi(c/x)}{\Gamma \vdash \Delta, \forall x \varphi(x)}$

falls c nicht in $\Gamma, \Delta, \varphi(x)$

$(\exists L)\ \dfrac{\Gamma, \varphi(c/x) \vdash \Delta}{\Gamma, \exists x \varphi(x) \vdash \Delta}$ $\qquad(\exists R)\ \dfrac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma \vdash \Delta, \exists x \varphi(x)}$

falls c nicht in $\Gamma, \Delta, \varphi(x)$

Korrektheit prüfen!

Beachte bspw. $\forall x \varphi(x) \Rightarrow \varphi(t/x)$

Sequenzenkalkül: Gleichheitsregeln

$(=)\ \dfrac{\Gamma, t = t \vdash \Delta}{\Gamma \vdash \Delta}$

(Sub-L) $\dfrac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, t = t', \varphi(t'/x) \vdash \Delta}$ $\qquad$ (Sub-R) $\dfrac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma, t = t' \vdash \Delta, \varphi(t'/x)}$

und analoge Regeln mit $t' = t$ statt $t = t'$

Korrektheit prüfen!

“Extensionalität”;

vgl. Implementationsunabhängigkeit
(*Information Hiding/Encapsulation*)

Sequenzenkalkül: Schnittregeln (optional)

(modus ponens) $\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma' \vdash \varphi}{\Gamma, \Gamma' \vdash \Delta}$

(Kontradiktion) $\dfrac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \neg\varphi}{\Gamma, \Gamma' \vdash \emptyset}$

Korrektheit prüfen!

Bem.: Kontradiktionsregel (lokal) mit modus ponens simulierbar

beide Regeln lassen sich (nicht lokal) eliminieren

(vgl. AL-Sequenzenkalkül)

unterscheide *schnittfreie* Kalküle wie $\mathcal{SK}$
von solchen mit Schnittregeln wir $\mathcal{SK}^+$

im Sequenzenkalkül mit Schnittregeln:

Satz

Für konsistentes Γ:
$\Gamma \cup \{\neg\varphi\}$ *in*konsistent gdw. $\Gamma \vdash \varphi$.

Begründung:

(1) Falls $\Gamma \vdash \varphi$ ableitbar ist, so auch $\Gamma, \neg\varphi \vdash \emptyset$ mit $(\neg L)$

(2) Falls $\Gamma, \neg\varphi \vdash \emptyset$ ableitbar, so auch $\Gamma \vdash \varphi$:

$$\dfrac{\dfrac{\Gamma, \neg\varphi \vdash \emptyset}{\Gamma \vdash \neg\neg\varphi}\,(\neg R) \qquad \dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi}\,(Ax)}{\emptyset \vdash \neg\varphi, \varphi}\,(\neg R)}{\neg\neg\varphi \vdash \varphi}\,(\neg L)}{\Gamma \vdash \varphi}\,(\text{mod. pon.})$$

Bem: Ebenso auch $\Gamma \cup \{\varphi\}$ *in*konsistent gdw. $\Gamma \vdash \neg\varphi$.

Ziel: Vollständigkeit → Abschnitt 6.3

Definitionen:

Ableitbarkeit aus Theorie $\Phi \subseteq \mathrm{FO}_0$:

φ **ableitbar aus** $\boldsymbol{\Phi}$ $[\Phi \vdash \varphi]$ gdw.

für geeignetes $\Gamma \subseteq \Phi$ (Voraussetzungen) ist $\Gamma \vdash \varphi$ ableitbar.

$\boldsymbol{\Phi}$ **konsistent** (widerspruchsfrei) gdw. *nicht* $\Phi \vdash \emptyset$.

Vollständigkeit (starke Form) ... **Korrektheit**

$\Phi \models \varphi \;\Rightarrow\; \Phi \vdash \varphi$

Φ konsistent $\Rightarrow$ Φ erfüllbar

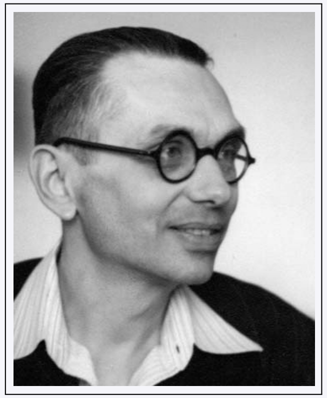
$\Phi \vdash \varphi \;\Rightarrow\; \Phi \models \varphi$

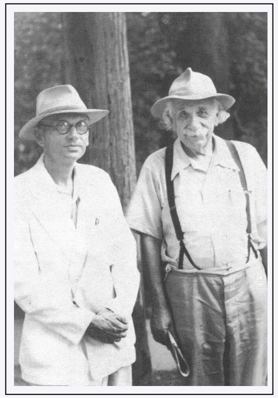
Φ erfüllbar $\Rightarrow$ Φ konsistent

alles, was wahr ist, ist ableitbar

alles, was ableitbar ist, ist wahr

Kurt Gödel (1906–1978)





mit Albert Einstein

der Logiker des 20. Jahrhunderts

Gödelscher Vollständigkeitssatz (Satz 6.7)

(Vollständigkeit & Korrektheit des Sequenzenkalküls)

Für jede Satzmenge $\Phi \subseteq \mathrm{FO}_0(S)$
und jeden Satz $\varphi \in \mathrm{FO}_0(S)$ gelten:

- $\Phi \models \varphi$ gdw. $\Phi \vdash \varphi$.
- Φ erfüllbar gdw. Φ konsistent.

Zentrale Folgerungen

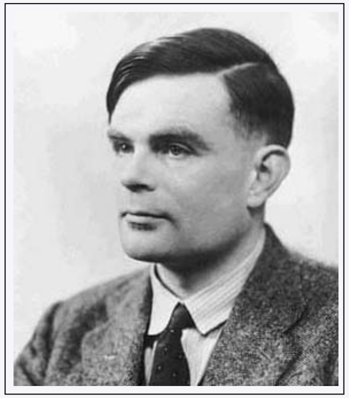
Kompaktheitssatz (wesentlich neuer Zugang)

Allgemeingültigkeit rekursiv aufzählbar,
Unerfüllbarkeit semi-entscheidbar

(später: nicht entscheidbar)

Unentscheidbarkeit Church–Turing

Church (1903–1995)



Turing (1912–1954)

Unentscheidbarkeit von SAT(FO) $\rightarrow$ Abschnitt 7.1

Satz von Church und Turing
SAT(FO) ist unentscheidbar.
genauer: nicht rekursiv aufzählbar.

Beweis: Reduktion des Halteproblems

FO ausreichend ausdrucksstark für Kodierung des Verhaltens von TM (in einzelnen Sätzen)

Finde berechenbare Zuordnung

$$\mathcal{M}, w \longmapsto \varphi_{\mathcal{M},w} \in \mathrm{FO}_0(S_{\mathcal{M}}),$$

$$\boxed{\varphi_{\mathcal{M},w} \text{ erfüllbar gdw. } w \xrightarrow{\mathcal{M}} \infty}$$

Idee: $\varphi_{\mathcal{M},w}$ besagt, dass die Konfigurationenfolge in der Berechnung von $\mathcal{M}$ auf w nicht abbricht.

Reduktion des Halteproblems auf SAT(FO)

einfache Variante

zu $\mathcal{M} = (\Sigma, Q, q_0, \delta, q^+, q^-)$
wähle als Signatur $S_{\mathcal{M}}$:

succ	Nachfolgerfunktion, 1-st.	(Schritt-/Positionszähler)
0	Konstante	
R_a	2-st. Relation für $a \in \Sigma \cup \{\Box\} =: \Gamma$	(Bandbeschriftung)
Z_q	1-st. Relation für $q \in Q$	(Zustände)
K	2-st. Relation	(Kopfpositionen)

intendierte Interpretation über $\mathbb{Z}$:

$(t, i) \in R_a$: zum Zeitpunkt $\#t$ steht in Zelle $\#i$ das Symbol a.
$t \in Z_q$: zum Zeitpunkt $\#t$ ist $\mathcal{M}$ im Zustand q.
$(t, i) \in K$: zum Zeitpunkt $\#t$ steht der Kopf auf Zelle $\#i$.

Reduktion: zu $\mathcal{M} = (\Sigma, Q, q_0, \delta, q^+, q^-)$, $w = a_1 \dots a_n$

$$\varphi_{\mathcal{M},w} := \varphi_0 \wedge \varphi_{\text{start}} \wedge \varphi_\delta \wedge \varphi_\infty, \qquad \varphi_\infty := \forall t\, \neg(Z_{q^+} t \vee Z_{q^-} t)$$

$$\varphi_0 := \begin{cases} \forall x, y\ \big((\operatorname{succ} x = \operatorname{succ} y \rightarrow x = y) \ \wedge\ 0 \neq \operatorname{succ} x\big) \\ \forall t \forall y\ \Big(\bigvee_{a \in \Gamma} R_a t y \ \wedge\ \bigwedge_{a \neq a' \in \Gamma} \neg(R_a t y \wedge R_{a'} t y)\Big) \\ \forall t\ \Big(\bigvee_{q \in Q} Z_q t \ \wedge\ \bigwedge_{q \neq q' \in Q} \neg(Z_q t \wedge Z_{q'} t)\Big) \\ \forall t \Big(\forall y \forall y'\ ((K t y \wedge K t y') \rightarrow y = y') \ \wedge\ \exists y\ K t y\Big) \end{cases}$$

$$\varphi_{\text{start}} := K00 \ \wedge\ Z_{q_0} 0 \ \wedge\ \begin{bmatrix} \bigwedge_{i=1}^n R_{a_i} 0 \operatorname{succ}^i 0 \\ \wedge \forall y\ \big((\bigwedge_{i=1}^n \neg y = \operatorname{succ}^i 0) \rightarrow R_\Box 0 y\big) \end{bmatrix}$$

$$\varphi_\delta := \forall t \forall t'\ (t' = \operatorname{succ} t \rightarrow \psi(t, t'))$$

$\psi(t, t')$, z.B. Beitrag für $\delta(q, b) = (b', >, q')$:
$\forall y\ \big((Z_q t \wedge K t y \wedge R_b t y) \rightarrow (Z_{q'} t' \wedge K t' \operatorname{succ} y \wedge R_{b'} t' y)\big)$

- $w \xrightarrow{\mathcal{M}} \infty \ \Rightarrow\ \varphi_{\mathcal{M},w}$ erfüllbar
- $w \xrightarrow{\mathcal{M}} \mathrm{STOP} \ \Rightarrow\ \varphi_{\mathcal{M},w}$ unerfüllbar

weitere Unentscheidbarkeitsaussagen $\rightarrow$ Abschnitt 7.2

FINSAT(FO): Sätze, die in *endlichen* Modellen erfüllbar sind

beachte: FINSAT(FO) ist rekursiv aufzählbar (warum, wie?)

Variation der Reduktion aus Church/Turing liefert:

Satz von Traktenbrot
FINSAT(FO) ist unentscheidbar.

tiefliegender:

Satz von Tarski
$\mathrm{Th}(\mathcal{N})$ ist unentscheidbar,
nicht rekursiv axiomatisierbar.

$\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$, $\quad \mathrm{Th}(\mathcal{N}) := \{\varphi \in \mathrm{FO}_0 : \mathcal{N} \models \varphi\}$
die erststufige Theorie der Arithmetik

Ausblick: andere Logiken (Beispiele) → Abschnitt 7.3

Ausdrucksstärke — gute algorithmische Eigenschaften

Modallogiken

Anwendungen in der Wissensrepräsentation, KI
Fragment(e) von FO: eingeschränkte Quantifizierung
längs Kanten in Transitionssystemen;
Formeln mit einer freien Variablen
SAT entscheidbar

Temporallogiken LTL, CTL, μ-Kalkül

Anwendungen in Verfikation, model checking für
Transitionssysteme, (verzweigte) Prozesse, etc.

SAT entscheidbar, für viele Zwecke ausdrucksstärker als FO

Ausblick: andere Logiken Beispiele

Monadische Logik zweiter Stufe, MSO

monadische zweite Stufe MSO:

Quantifizierung auch über Teilmengen der Trägermenge
es existiert *kein* vollständiges Beweissystem
Allgemeingültigkeit nicht einmal rekursiv aufzählbar

aber $\mathrm{SAT}(\mathrm{MSO})$ entscheidbar über interessanten
Strukturklassen: z.B. Wortmodelle, lineare Ordnungen, Bäume

enger Zusammenhang mit Automatentheorie

Satz von Büchi:

reguläre Sprachen = MSO definierbare Wortmodellklassen

Ausblick: entscheidbare Fragmente von FO

über relationalen Signaturen ist SAT z.B. entscheidbar für:

- pränexe $\exists^*\forall^*$-Sätze
- pränexe gleichheitsfreie $\exists^*\forall\forall\exists^*$-Sätze
- pränexe $\exists^*\forall\exists^*$-Sätze
- FO-Sätze mit nur zwei Variablensymbolen

Ausblick: entscheidbare Theorien

Beispiele

entscheidbar	dagegen unentscheidbar
MSO-Theorie von Bäumen (Rabin)	Graphentheorie, FO
$\mathrm{FO}\text{-}\mathrm{Th}(\mathbb{R},+,\cdot,0,1,<)$ (Tarski)	$\mathrm{FO}\text{-}\mathrm{Th}(\mathbb{N},+,\cdot,0,1,<)$
$\mathrm{FO}\text{-}\mathrm{Th}(\mathbb{N},+,0,1,<)$ (Presburger)	
FO-Theorie abelscher Gruppen	Gruppentheorie, FO

Ausdrucksstärke verschiedener Logiken → Abschnitt 8

Fragen: Welche Struktureigenschaften können in gegebener Logik formalisiert werden?

Welche Eigenschaften sind nicht ausdrückbar?

z.B. *nicht* in FO: Endlichkeit der Trägermenge
Zusammenhang von (endlichen) Graphen
gerade Länge endlicher linearer Ordnungen
...

→ **Modelltheorie**

die Methode zur Analyse der Ausdrucksstärke:

$\boxed{\text{Ehrenfeucht-Fraïssé Spiele}}$

Fragen der Ausdrucksstärke

Kernfrage: $\boxed{\textbf{welche Logik wofür?}}$

zB bei der Wahl einer Logik als Sprache für

Spezifikation, Verifikation, Deduktion
Wissensrepräsentation, Datenbankabfragen

Kriterien: algorithmische Eigenschaften
beweistheoretische Eigenschaften
Ausdrucksstärke

- wie kann man analysieren, was ausdrückbar ist?
- wie erkennt/beweist man, dass etwas *nicht* ausdrückbar ist?

Ausdrucksstärke: Beispiele

Es gibt keine Satzmenge in $\mathrm{FO}(\{E\})$, die den Zusammenhang von Graphen (V, E) formalisiert (analog für Erreichbarkeitsfragen).

Es gibt keinen Satz in $\mathrm{FO}(\{E\})$, der den Zusammenhang von endlichen Graphen (V, E) formalisiert (analog für Erreichbarkeit).

Jeder Satz in $\mathrm{FO}(\{<\})$, der formalisiert, dass $<$ eine lineare Ordnung ist, benutzt mehr als zwei Variablen.

Es gibt keinen Satz in $\mathrm{FO}(\{<\})$, der von einer endlichen linearen Ordnung $(A, <)$ besagt, dass sie ungerade Länge hat.

Jeder Satz in $\mathrm{FO}(\{<\})$, der von einer linearen Ordnung $(A, <)$ besagt, dass sie mindestens die Länge 17 hat, hat mindestens Quantorenrang 5.

Ehrenfeucht–Fraïssé Spiele → Abschnitt 8.1

vgl. auch Semantikspiel zwischen Verifizierer und Falsifizierer

Idee: Spielprotokoll für zwei Spieler **I** und **II**
zum *Vergleich* zweier Strukturen so, dass
$\mathcal{A}$ und $\mathcal{B}$ ähnlich (ununterscheidbar in L)
wenn Spieler **II** Gewinnstrategie hat.

Spieler **II** muss in der jeweils anderen Struktur nachmachen,
was **I** in einer der Strukturen vorgibt

Spieler **I** versucht das Spiel auf Unterschiede zu lenken,
die das für **II** unmöglich machen

Verwendung
wenn $\mathcal{A}$ und $\mathcal{B}$ ununterscheidbar in L,
aber verschieden hinsichtlich Eigenschaft E,
dann lässt sich E *nicht* in L ausdrücken

MSO: monadische zweite Stufe

hier über Σ-Wortstrukturen, zu $S = \{<\} \cup \{P_a \colon a \in \Sigma\}$
Elementvariable: $x_1, x_2, \dots$

Mengenvariable: $X_1, X_2, \dots$ für Teilmengen der Trägermenge

zu Syntax und Semantik von $\mathrm{MSO}(S)$

atomare Formeln: $x_i = x_j$, $x_i < x_j$, $P_a x_i$, $X_i x_j$
AL Junktoren $\wedge, \vee, \neg$ wie üblich
Quantifizierung über Elemente: $\forall x_i \varphi$, $\exists x_i \varphi$ wie in FO
Quantifizierung über Teilmengen: $\forall X_i \varphi$, $\exists X_i \varphi$

Beispiele für Ausdrucksmöglichkeiten:

Ordnungen/Wörter ungerader Länge
allgemeiner: reguläre Sprachen
MSO-Kodierung von DFA/NFA

Beispiele zur Ausdrucksstärke von MSO_1

hier für Graphstrukturen $G = (V, E)$,
Quantifikation über Teilmengen von V
(aber nicht von $V \times V$ oder von E etc.)

connected$(x, y; G) \quad \Leftrightarrow$
$\forall X : \; x \in X \wedge \big(\forall u, v : \; u \in X \wedge (u, v) \in E \rightarrow v \in X\big) \;\rightarrow\; y \in X$

3colorable$(G) \quad \Leftrightarrow$
$\exists R, G, B : \quad (\forall v : v \in R \vee v \in G \vee v \in B) \quad \wedge$
$\wedge \quad (\forall u, v : (u \in R \wedge v \in R) \vee (u \in G \wedge v \in G) \vee (u \in B \wedge v \in B) \rightarrow \neg(u, v) \in E)$

Ebenfalls ausdrückbar: **planar**(G) (Satz von Kuratowski)

Wiederholung

– was Sie unbedingt wissen/können müssen

Formalismen

Syntax (AL, FO, Formeln, Terme, freie Variablen, etc.)

Normalformen (DNF, KNF, pränexe Normalform)
syntaktische Manipulationen: Substitution, Skolemisierung

Beweiskalküle (Resolutionsmethode, Sequenzenregeln)

Inhaltliches Verstehen

Semantik von Formeln, Modellbeziehung

Formeln lesen können, Terme/Formeln in Strukturen auswerten

Formalisierungen in AL und FO angeben

semantische Beziehungen: Äquivalenzen, Folgerungsbeziehung, Erfüllbarkeitsäquivalenz
semantische Kriterien: Erfüllbarkeit, Allgemeingültigkeit, Korrektheit, ...

Wiederholung

zentrale Begriffe/Konzepte inhaltlich beherrschen
im Kontext sinnvoll anwenden
zentrale Sätze und Resultate: kennen
interpretieren
anwenden

zentrale Sätze

Kompaktheit (Endlichkeitssätze),
Herbrand-Modelle,
Reduktionschritte von FO auf AL,
Korrektheits- und Vollständigkeitsaussagen zu Kalkülen
Entscheidbarkeit und Unentscheidbarkeit

Wiederholung: Beispiele

AL-Formeln auswerten (systematisch: Wahrheitstafel)

AL-Formeln auf Folgerung bzw. Äquivalenz untersuchen

natürlichsprachliche Bedingungen in AL formalisieren

Unerfüllbarkeit mittels Resolution nachweisen

Allgemeingültigkeit formal im Sequenzenkalkül nachweisen

Folgerungsbeziehungen reduzieren auf
Unerfüllbarkeit/Allgemeingültigkeit

Kompaktheitssatz anwenden

Kalküle rechtfertigen (z.B. Korrektheit von Regeln)

Wiederholung: Beispiele

Umgang mit Strukturen

auch spezielle Strukturen und Klassen wie z.B.
Graphen, Transitionssysteme, relationale DB-Strukturen,
Wortmodelle, linear-temporale Abfolgen, $\mathcal{N}$

Auswerten von Termen und Formeln in Strukturen

PNF, Skolemisieren, Substitutionen ausführen

Herbrandmodelle beschreiben/untersuchen

Unerfüllbarkeit nachweisen, bspw. durch Reduktion auf AL

(GI-Resolution und) Sequenzenkalkül in Beispielen

etc.

entscheidbar? rekursiv aufzählbar? → Übung G1

$\mathrm{SAT(AL)} := \{\varphi \in \mathrm{AL} : \varphi$ erfüllbar$\}$

$\mathrm{FOLG(AL)} := \{(\varphi, \psi) \in \mathrm{AL} : \varphi \models \psi\}$

$\mathrm{SAT(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ erfüllbar$\}$

$\mathrm{VAL(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ allgemeingültig$\}$

$\mathrm{UNSAT(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ unerfüllbar$\}$

$\mathrm{FINSAT(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ hat ein endliches Modell$\}$

$\mathrm{INFVAL(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ im Unendlichen allgemeingültig$\}$

$\mathrm{INF_0(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ in unendlichen Modellen erfüllbar$\}$

$\mathrm{INF_1(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ nur in unendlichen Modellen erfüllbar$\}$

$\mathrm{INF_2(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ hat beliebig große endliche Modelle$\}^{**}$

- Beispiele von Sätzen in/außerhalb?
  Inklusionen, Komplementbeziehungen, ...

FO-ausdrückbar in Graphen? → Übung G2

Distanz gerade oder unendlich (d.h., nicht endlich und gerade)

Kreisfreiheit

Existenz eines Kreis

uniform unendlicher Grad

uniform endlicher Grad

Herbrand-Modelle – Nichtstandard-Modelle $\rightarrow$ Übung G6

Kann man die Klasse der Herbrandmodelle einer gegebenen Satzmenge in FO axiomatisieren?

Kann man in FO-Satzmenge die Forderung spezifizieren, dass jedes Element der Trägermenge durch eine variablenfreien Term addressiert wird?

Kann die Menge der in einem Modell der Arithmetik durch variablenfreie Terme addressierten Elemente durch eine Formel $\varphi(x) \in \mathrm{FO}(S_{ar})$ definierbar sein?

($*$) Kann man in $\mathrm{MSO}(S_{ar})$ das Standardmodell der Arithmetik bis auf Isomorphie axiomatisieren?

Ist die Menge der Primzahlen im Standardmodell der Arithmetik durch eine Formel $\varphi(x) \in \mathrm{FO}(S_{ar})$ definierbar? In welchem Sinne gibt es in Nichtstandard-Modellen unendliche Primzahlen?

Was stimmt hiervon?

Man kann die Erfüllbarkeit von AL-Formeln in DNF effizient* entscheiden.

Zu jeder AL-Formel kann man eine logisch äquivalente AL-Formel in DNF berechnen.

Erfüllbarkeit von AL-Formeln ist effizient* entscheidbar.

$*$ in Laufzeit polynomial in der Länge der gegebenen Formel

Was stimmt hiervon?

Zu jeder FO-Formel gibt es

eine $\begin{cases} \text{logisch äquivalente } \mathrm{FO}^{\neq}\text{-Formel ?} \\ \text{erfüllbarkeitsäquivalente } \mathrm{FO}^{\neq}\text{-Formel ?} \end{cases}$

eine $\begin{cases} \text{logisch äquivalente pränexe } \mathrm{FO}\text{-Formel ?} \\ \text{logisch äquivalente universell-pränexe } \mathrm{FO}\text{-Formel ?} \\ \text{erfüllbarkeitsäquivalente universell-pränexe } \mathrm{FO}\text{-Formel ?} \end{cases}$

Wie findet man solche Formeln ggf. algorithmisch?

Was stimmt hiervon?

Man kann die Erfüllbarkeit von (universell-pränexen $=$-freien) FO-Sätzen auf ein AL-Erfüllbarkeitsproblem reduzieren.

Erfüllbarkeit von (universell-pränexen $=$-freien) FO-Sätzen ist entscheidbar.

Was stimmt hiervon?

Resolutionsalgorithmen produzieren schließlich alle Klauseln, die logische Folgerungen aus der gegebenen Klauselmenge sind.

Der (schnittfreie) AL-Sequenzenkalkül $\mathcal{K}$ erlaubt eine terminierende algorithmische Beweissuche.

Der (schnittfreie) FO-Sequenzenkalkül $\mathcal{K}$ erlaubt eine terminierende algorithmische Beweissuche.

Abstraktion und formale Grundlagen

oder: Ich verlass' mich lieber auf den gesunden Menschenverstand?

Abstraktion und abstraktes Verständnis:

- Überblick gegenüber Sicht von innen/unten?
- Vereinfachung & Klarheit?
- Was *ist* Anschaulichkeit?
- Wie kann man Anschauung, Intuition *schulen*?
- Ziel *Erkenntnisgewinn*?

Informatik ist eine Wissenschaft

Why do software systems crash and bridges (mostly) stand up?

Arbeitsgruppe Logik, Fachbereich Mathematik

Mathematische Logik und **Grundlagen der Informatik**

Kohlenbach	Beweistheorie mit Anwendungen
Otto	Modelltheorie, Logik in der Informatik
Streicher	Semantik von Programmiersprachen
Ziegler	reelle Berechenbarkeit und Komplexität

Einführungsvorlesungen, Spezialvorlesungen, Seminare, ...

die sich insbesondere auch an interessierte Informatiker wenden

"Anwendungsfach" Logik: Nebenfach Mathematik mit Schwerpunkt aus obigen Bereichen

für FGdI suchen wir immer *interessierte Tutoren*