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

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

$$\varphi_0 \;:=\; \left\{ \begin{array}{l} \forall x, y \; \big((\mathrm{succ}\, x = \mathrm{succ}\, y \to x = y) \;\wedge\; 0 \neq \mathrm{succ}\, x\big) \\ \forall t \forall y \; \Big(\bigvee_{a \in \Gamma} R_a t y \;\wedge\; \bigwedge_{a \neq a' \in \Gamma} \neg(R_a t y \wedge R_{a'} t y) \Big) \\ \forall t \; \Big(\bigvee_{q \in Q} Z_q t \;\wedge\; \bigwedge_{q \neq q' \in Q} \neg(Z_q t \wedge Z_{q'} t) \Big) \\ \forall t \Big(\forall y \forall y' \; ((K t y \wedge K t y') \to y = y') \;\wedge\; \exists y \; K t y \Big) \end{array} \right.$$

$$\varphi_{\mathrm{start}} := K00 \;\wedge\; Z_{q_0} 0 \;\wedge\; \left[\begin{array}{l} \bigwedge_{i=1}^{n} R_{a_i} 0 \,\mathrm{succ}^i\, 0 \\ \wedge \forall y \; \big((\bigwedge_{i=1}^{n} \neg y = \mathrm{succ}^i\, 0) \to R_{\Box} 0 y \big) \end{array} \right]$$

$\varphi_\delta \;:= \forall t \forall t' \; (t' = \mathrm{succ}\; t \to \psi(t, t'))$

$\psi(t, t')$, z.B. Beitrag für $\delta(q, b) = (b', >, q')$:

$\forall y \; \big((Z_q t \wedge K t y \wedge R_b t y) \to (Z_{q'} t' \wedge K t' \mathrm{succ}\, y \wedge R_{b'} t' y) \big)$

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

weitere Unentscheidbarkeitsaussagen $\to$ Abschnitt 7.2

$\mathrm{FINSAT(FO)}$: Sätze, die in *endlichen* Modellen erfüllbar sind

beachte: $\mathrm{FINSAT(FO)}$ ist rekursiv aufzählbar (warum, wie?)

Variation der Reduktion aus Church/Turing liefert:

> **Satz von Traktenbrot**
> $\mathrm{FINSAT(FO)}$ ist unentscheidbar.

tiefliegender:

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

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

Ausblick: andere Logiken (Beispiele) $\to$ 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 $\mathrm{SAT(MSO)}$ 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
$\mathrm{FO\text{-}Th}(\mathbb{R}, +, \cdot, 0, 1, <)$ (Tarski)	$\mathrm{FO\text{-}Th}(\mathbb{N}, +, \cdot, 0, 1, <)$
$\mathrm{FO\text{-}Th}(\mathbb{N}, +, 0, 1, <)$ (Presburger)	
FO-Theorie abelscher Gruppen	Gruppentheorie, FO

Ausdrucksstärke verschiedener Logiken $\rightarrow$ 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
...

$\rightarrow$ **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

$\rightarrow$ 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 $S = \{<\} \cup \{P_a : a \in \Sigma\}$
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

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,
(Reduktionen 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 durch Reduktion auf AL nachweisen)

(GI-Resolution und) Sequenzenkalkül in Beispielen

etc.

entscheidbar? rekursiv aufzählbar? $\rightarrow$ Übung G1

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

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

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

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

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

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

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

$\mathrm{INF}_0(\mathrm{FO}) := \{\varphi \in \mathrm{FO} : \varphi \text{ in unendlichen Modellen erfüllbar}\}$

$\mathrm{INF}_1(\mathrm{FO}) := \{\varphi \in \mathrm{FO} : \varphi \text{ nur in unendlichen Modellen erfüllbar}\}$

$\mathrm{INF}_2(\mathrm{FO}) := \{\varphi \in \mathrm{FO} : \varphi \text{ hat beliebig große endliche Modelle}\}^{**}$

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

FO-ausdrückbar in Graphen? $\rightarrow$ 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 { logisch äquivalente $\mathrm{FO}^{\neq}$-Formel ?
erfüllbarkeitsäquivalente $\mathrm{FO}^{\neq}$-Formel ?

eine { logisch äquivalente pränexe FO-Formel ?
logisch äquivalente universell-pränexe FO-Formel ?
erfüllbarkeitsäquivalente universell-pränexe FO-Formel ?

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*