Ausblick: andere Logiken — Beispiele

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 Transitionssyteme, (verzweigte) Prozesse, etc.

SAT entscheidbar, für viele Zwecke ausdrucksstärker als FO

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: 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 SAT(MSO) entscheidbar über interessanten Strukturklassen: z.B. Wortmodelle, lineare Ordnungen, Bäume

enger Zusammenhang mit Automatentheorie
z.B. Satz von Büchi:

$\boxed{\text{reguläre Sprachen} = \text{MSO definierbare Wortmodellklassen}}$

Ausblick: entscheidbare Theorien

Beispiele

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

Ausblick: Ausdrucksstärke verschiedener Logiken

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

Ausdrucksstärke: Beispiele

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

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

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

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

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

Fragen der Ausdrucksstärke

Kernfrage $\boxed{\text{welche Logik wofür?}}$

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?

wesentliche Methode: Spiele, Ehrenfeucht-Fraïssé Spiele

vgl. 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

das klassische Ehrenfeucht-Fraïssé Spiel für FO

fixiere feste endliche relationale Signatur S

zB für Wortstrukturen zu Alphabet Σ: $S = \{<\} \cup \{P_a \colon a \in \Sigma\}$

Ununterscheidbarkeitsgrade $\mathcal{W}, \mathbf{m} \equiv_q \mathcal{W}', \mathbf{m}'$

f.a. $\varphi(\mathbf{x}) \in \mathrm{FO}(S)$ mit $\mathrm{qr}(\varphi) \leqslant q$:
$\mathcal{W} \models \varphi[\mathbf{m}] \;\Leftrightarrow\; \mathcal{W}' \models \varphi[\mathbf{m}']$

insbesondere für $q = 0$, $\mathbf{m} = (m_1, \dots, m_k)$, $\mathbf{m}' = (m'_1, \dots, m'_k)$
$\mathcal{W}, \mathbf{m} \equiv_0 \mathcal{W}', \mathbf{m}'$ gdw. $\rho \colon (m_i \mapsto m'_i)_{1 \leqslant i \leqslant k}$ lokaler Isomorphismus

Spielidee: **I** markiert zukzessive Elemente in $\mathcal{W}$ oder $\mathcal{W}'$,
II antwortet in der jeweils anderen Struktur,
II muss $\mathcal{W}, \mathbf{m} \equiv_0 \mathcal{W}', \mathbf{m}'$ gewährleisten

Ehrenfeucht-Fraïssé Satz

für alle $q \in \mathbb{N}$, S-Strukturen $\mathcal{W}$ und $\mathcal{W}'$ mit Parametern
$\mathbf{m} = (m_1, \dots, m_k)$ in $\mathcal{W}$ und $\mathbf{m}' = (m'_1, \dots, m'_k)$ in $\mathcal{W}'$
sind äquivalent:

(i) **II** hat Gewinnstrategie in $G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

(ii) $\mathcal{W}, \mathbf{m} \equiv_q \mathcal{W}', \mathbf{m}'$

Beweis per Induktion über q. Strategieanalyse!

$q = 0$: trivial.

Gewinnstrategie für eine Runde verlangt gerade
Übereinstimmung hinsichtlich Existenzbeispielen für z
in allen Formeln $\exists z \varphi(\mathbf{x}, z)$ mit quantorenfreiem φ (warum?)

Gewinnstrategie für $q + 1$ Runden verlangt analog,
in der ersten Runde, Übereinstimmung hinsichtlich
aller Formeln $\exists z \varphi(\mathbf{x}, z)$ mit $\mathrm{qr}(\varphi) \leqslant q$

die Spiele $G^q(\mathcal{W}, \mathcal{W}')$ und $G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

Konfigurationen:
$(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ mit $\mathbf{m} = (m_1, \dots, m_k)$ und $\mathbf{m}' = (m'_1, \dots, m'_k)$
wenn in $\mathcal{W}$ und $\mathcal{W}'$ jeweils k Elemente markiert sind

Zugabtausch in einer Runde:
I markiert in $\mathcal{W}$ oder in $\mathcal{W}'$ ein weiteres Element,
II ein Element in der jeweils anderen Struktur

von
$(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$
zu Nachfolgekonfiguration
$(\mathcal{W}, \mathbf{m}, m_{k+1}; \mathcal{W}', \mathbf{m}', m'_{k+1})$

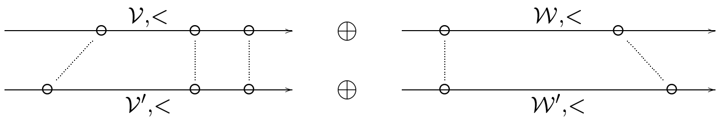
Gewinnbedingung:
II verliert wenn $\mathcal{W}, \mathbf{m} \not\equiv_0 \mathcal{W}', \mathbf{m}'$

$\boldsymbol{G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')}$:
Spiel über q Runden mit Startkonfiguration $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$

Bsp: Spiele über Wortstrukturen und linearen Ordnungen

(A) Gewinnstrategien für **II** sind verträglich mit Konkatenation

$$\left.\begin{array}{r} \mathcal{V}, \mathbf{m} \equiv_q \mathcal{V}', \mathbf{m}' \\ \mathcal{W}, \mathbf{n} \equiv_q \mathcal{W}', \mathbf{n}' \end{array}\right\} \;\Rightarrow\; \mathcal{V} \oplus \mathcal{W}, \mathbf{m}, \mathbf{n} \;\equiv_q\; \mathcal{V}' \oplus \mathcal{W}', \mathbf{m}', \mathbf{n}'$$



(Beobachtung 8.11)

(B) in (nackten) linearen Ordnungen sind Distanzen ab 2^q mit Quantorenrang q ununterscheidbar

diese Schranke ist i.w. scharf (Beobachtung 8.12)

Strategien über nackten endlichen Ordnungen

vergleiche aufsteigende Tupel
$\mathbf{m} = (m_1, \dots, m_k)$ in $\mathcal{O}_n = (\{1, \dots, n\}, <)$ und
$\mathbf{m}' = (m'_1, \dots, m'_k)$ in $\mathcal{O}_{n'} = (\{1, \dots, n'\}, <)$

Intervallgrößen:

i-ter Abschnitt: $m_i < x < m_{i+1}$ hat $d_i := m_{i+1} - m_i - 1$ Elemente

kritische Intervallgröße (für q weitere Runden): $2^q - 1$

$d \overset{q}{=} d' \;:\Leftrightarrow\; d = d'$ oder $d, d' \geqslant 2^q - 1$

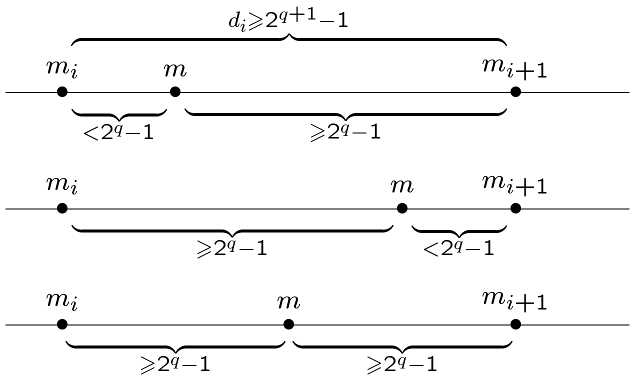
dann gilt:

$$\boxed{\mathcal{O}_n, \mathbf{m} \equiv_q \mathcal{O}_{n'}, \mathbf{m}' \quad \text{gdw.} \quad d_i \overset{q}{=} d'_i \text{ für } i = 0, \dots, k}$$

Strategiefindung: Auszug

wie **II** auf Herausforderungszug von **I** auf $m \in (m_i, m_{i+1})$ antworten kann (3 Fälle)

(a) (b) (c)



Folgerungen

(1) **(un)gerade Länge endlicher linearer Ordnungen nicht in FO definierbar**

vergleiche Ordnungen der Längen $2^q - 1$ und 2^q:
Quantorenrang q reicht nicht aus

(2) **Zusammenhang endlicher Graphen nicht in FO definierbar**

logische Übersetzung (Interpretation) liefert Reduktion auf (1)

vergleiche zB