Beispiele zu Logik&Informatik: ACM Turing Awards

Lamport (2013)	concurrency, 'logical clocks'
Goldwasser/ Micali (2012)	complexity & cryptography, 'efficient verification of mathematical proofs'
Valiant (2010)	theory of computation
Clarke/Emerson/ Sifakis (2007)	model checking, verification
Pnueli (1996)	temporal logic
Milner (1991)	semantics & process logics 'mechanisation of logic'
Karp (1985)	NP-completeness
Cook (1982)	complexity of theorem proving procedures
Rabin/ Scott (1976)	automata & their decision problems

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
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

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:

Ehrenfeucht-Fraïssé Spiele

Fragen der Ausdrucksstärke

Kernfrage: **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

das klassische Ehrenfeucht-Fraïssé Spiel für FO

fixiere feste endliche relationale Signatur S

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

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 $q = 0$, $\mathbf{m} = (m_1, \ldots, m_k)$, $\mathbf{m}' = (m'_1, \ldots, m'_k)$:

$\mathcal{W}, \mathbf{m} \equiv_0 \mathcal{W}', \mathbf{m}'$ gdw. $\rho : (\mathbf{m_i} \mapsto \mathbf{m'_i})_{1 \leqslant i \leqslant k}$ **lokaler Isomorphismus**

Spielidee: **I** markiert sukzessive Elemente in $\mathcal{W}$ oder $\mathcal{W}'$,
II antwortet in der jeweils anderen Struktur,
II muss stets $\equiv_0$ (lokale Isomorphie) gewährleisten

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 $\mathbf{m} = (m_1, \ldots, m_k)$ und $\mathbf{m}' = (m'_1, \ldots, m'_k)$
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 $\mathcal{W}, \mathbf{m} \not\equiv_0 \mathcal{W}', \mathbf{m}'$ (kein lokaler Isomorphismus)

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

Ehrenfeucht-Fraïssé Satz (Satz 8.7)

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

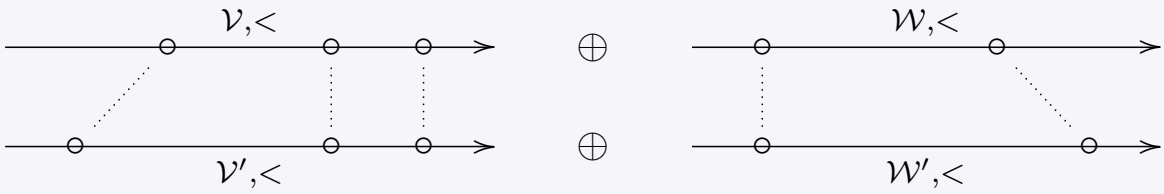
Gewinnstrategie für $q + 1$ Runden verlangt analog,
in der ersten Runde, Übereinstimmung hinsichtlich
aller Formeln $\exists z \varphi(\mathbf{x}, z)$ mit $\mathrm{qr}(\varphi) \leqslant q$

Spiele über Wortstrukturen und linearen Ordnungen

Kompatibilität mit Konkatenation (Beobachtung 8.11)

Gewinnstrategien für **II** sind verträglich mit Konkatenation

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



Modularität von Strategien:

$\equiv_q$ ist Kongruenzrelation bzgl. Konkatenation

für nackte endliche Ordnungen $\mathcal{O}_\mathbf{n} = (\{1,\ldots,\mathbf{n}\},<)$

es gibt Sätze $\varphi_q \in \mathrm{FO}(\{<\})$, $q \geqslant 1$: (vgl. Beobachtung 8.12)

- $\mathrm{qr}(\varphi_q) = q$
- $\mathcal{O}_n \models \varphi_q$ gdw. $n \geqslant 2^q - 1$

insbesondere: $\mathcal{O}_n \not\equiv_q \mathcal{O}_m$ für $n < 2^q - 1 \leqslant m$

(noch einfacher: $\psi_q(x,y)$ für "$x < y$ und $|(x,y)| \geqslant 2^q - 1$")

E-F Spiel-Analyse:

$\mathcal{O}_\mathbf{n} \equiv_\mathbf{q} \mathcal{O}_\mathbf{m}$ für $n, m \geqslant 2^q - 1$

genauer: in nackten linearen Ordnungen sind Distanzen ab 2^q mit Quantorenrang q *nicht* unterscheidbar

Strategien über nackten endlichen Ordnungen

vergleiche aufsteigende Tupel

$\mathbf{m} = (m_1, \ldots, m_k)$ in $\mathcal{O}_n = (\{1, \ldots, n\}, <)$ und

$\mathbf{m}' = (m'_1, \ldots, m'_k)$ in $\mathcal{O}_{n'} = (\{1, \ldots, n'\}, <)$

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): $2^q - 1$

$d \stackrel{q}{=} d' \;:\Leftrightarrow\; d = d'$ oder $d, d' \geqslant 2^q - 1$
"Gleichheit bis zur kritischen Intervalgröße"

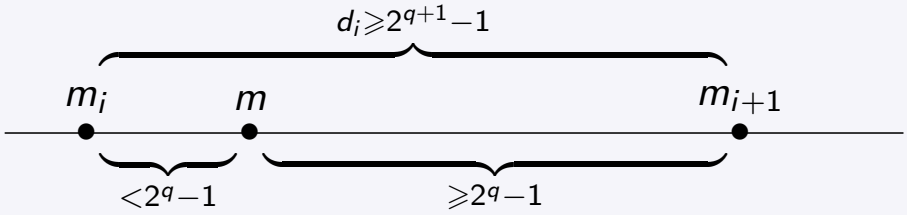
dann gilt:

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

Strategiefindung: Auszug

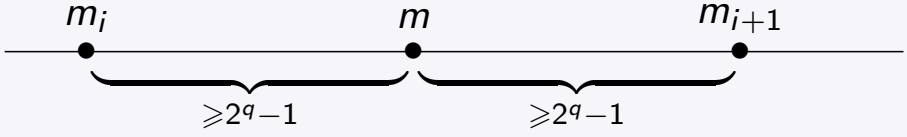
wie **II** auf Herausforderungszug von **I** auf $m \in (m_i, m_{i+1})$
antworten kann (3 Fälle)

(a)



(b)

(c)



Folgerungen

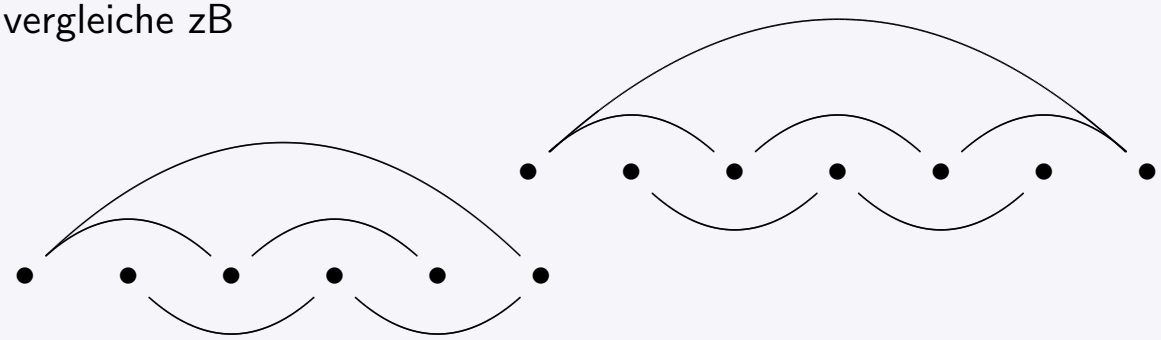
(1) **(un)gerade Länge endlicher linearer Ordnungen nicht in FO definierbar**

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



andere Logiken — andere Spiele → Abschnitt 8.2

am Beispiel zweier wichtiger (Familien von) Logiken in der Informatik

- **MSO, monadische Logik zweiter Stufe**
  Erweiterung von FO: Quantoren über Teilmengen
  → formale Sprachen, concurrency

- **ML, Modallogik**
  Fragment von FO: beschränkte Quantoren über Elemente
  → temporale Spezifikation, Wissensrepräsentation

hier: zugehörige Spiele und Beispiele für ihren Nutzen

MSO: monadische zweite Stufe

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

Mengenvariable: $X_1, X_2, \ldots$ 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

MSO-Kodierung von DFA/NFA-Läufen

für Lauf von $\mathcal{A} = (\Sigma, Q, q_0, \Delta, A)$ auf Wort $w = a_1 \ldots a_n \in \Sigma^n$:

expandiere Wortmodell $\mathcal{W}_w$ durch Färbung mit Zuständen

Farben $(P_a)_{a \in \Sigma}$ (für Buchstabenfolge von w)
$+$ Farben $(X_q)_{q \in Q}$ (für Zustandsfolge von w)

a_1	a_2	a_3	a_4		a_{n-1}	a_n	$\mathcal{W}_w$
q_1	q_2	q_3	q_4		q_{n-1}	q_n	$\mathbf{X}$

- finde $\varphi \in \mathrm{FO}(\{<\} \cup \{P_a : a \in \Sigma\} \cup \{X_q : q \in Q\})$:

  "die X_q beschreiben Zustandsfolge
  einer akzeptierenden Berechnung
  von $\mathcal{A}$ auf $\mathcal{W}$"

- dann ist $\exists \mathbf{X} \varphi \in \mathrm{MSO}(\{<\} \cup \{P_a : a \in \Sigma\})$ wie gewünscht

MSO-Spiel

Konfigurationen $(\mathcal{W}, \mathbf{Q}, \mathbf{m}; \mathcal{W}', \mathbf{Q}', \mathbf{m}')$
mit markierten Elementen $\mathbf{m}/\mathbf{m}'$ und Teilmengen $\mathbf{Q}/\mathbf{Q}'$

zwei Zugvarianten $\begin{cases} \text{weiteres Element markieren} \\ \text{weitere Teilmenge markieren} \end{cases}$

Ehrenfeucht-Fraïssé Satz für MSO:

II hat Gewinnstrategie in $G^q_{\mathrm{MSO}}(\mathcal{W}, \mathbf{Q}, \mathbf{m}; \mathcal{W}', \mathbf{Q}', \mathbf{m}')$
gdw. $\mathcal{W}, \mathbf{Q}, \mathbf{m} \equiv^{\mathrm{MSO}}_q \mathcal{W}', \mathbf{Q}', \mathbf{m}'$

auch im MSO-Spiel sind Gewinnstrategien
verträglich mit Konkatenation, und man gewinnt daraus:

Satz von Büchi

MSO-definierbare Eigenschaften von Σ-Wortstrukturen
entsprechen genau den regulären Σ-Sprachen

Beweisskizze zum Satz von Büchi

Annahme: $\{\mathcal{W}_w : w \in L\} = \{\mathcal{W}_w : \mathcal{W}_w \models \varphi\}$
für einen Satz $\varphi \in \mathrm{MSO}$

zu zeigen: L regulär, oder, nach Myhill–Nerode,

$\sim_L$ hat endlichen Index: $\boxed{\Sigma^*/\!\sim_L \text{ endlich}}$

sei dazu $\mathrm{qr}(\varphi) = q$,

dann verfeinert $\equiv_q$ die Relation $\sim_L$ (warum?)

$\equiv_q$ hat endlichen Index (warum?)

es folgt dass auch $\sim_L$ endlichen Index hat!

$\longrightarrow$ Automaten für MSO-model-checking