Logik Teil 3: Mehr zur Prädikatenlogik erster Stufe

Übersicht Teil 3

Sequenzenkalkül

Wir betrachten einen Kalkül für Gültigkeit in der Prädikatenlogik.

Motivation:

- rekursive Aufzählbarkeit nachweisen
- einfacher Beweis für das Kompaktheitstheorem in FO

Im Prinzip könnten wir wieder Resolution verwenden
(Grundlage für Theorembeweiser der Logik erster Stufe)

Wir verwenden aber einen technisch einfacheren Ansatz:

Gentzens Sequenzenkalkül

Der Einfachheit halber verzichten wir auf das Gleichheitsprädikat.

Sequenzen

Definition Sequenz

Eine *Sequenz* ist ein Ausdruck der Form $\Gamma \Rightarrow \Delta$,
wobei Γ und Δ endliche Mengen von Sätzen sind. Wir nennen

- Γ das *Antezendenz* und
- Δ das *Sukzedenz*.

Die Sequenz $\Gamma \Rightarrow \Delta$ ist *gültig,* wenn $\bigwedge \Gamma \models \bigvee \Delta$, in Worten:

jedes Modell von $\bigwedge \Gamma$ macht auch mindestens einen Satz aus Δ wahr.

Ist eine Sequenz $\Gamma \Rightarrow \Delta$ gültig, so schreiben wir $\models \Gamma \Rightarrow \Delta$.

Beispiele für gültige Sequenzen:

- $\{\forall x\, P(x),\ Q(c)\} \ \Rightarrow\ \{P(c) \land Q(c),\ R(c,d)\}$
- $\{P(c) \lor Q(d)\} \ \Rightarrow\ \{P(c),\ Q(d)\}$

Sequenzenkalkül

Der Sequenzenkalkül erlaubt, alle gültigen Sequenzen abzuleiten.

Offensichtlich gilt:

- FO-Satz φ ist Tautologie gdw. die Sequenz $\emptyset \Rightarrow \{\varphi\}$ gültig ist
- FO-Satz φ ist unerfüllbar gdw. die Sequenz $\{\varphi\} \Rightarrow \emptyset$ gültig ist
  (denn $\bigvee \emptyset$ ist unerfüllbar)

Man kann den Sequenzenkalkül also auch als Kalkül zum Ableiten aller Tautologien bzw. aller unerfüllbaren *Formeln* ansehen.

Bestandteile des SK

Die zentralen Bestandteile des SK

Axiome
Sequenzen, die man ohne Beweis/Herleitung als gültig voraussetzt

Schlussregeln
Im Gegensatz zu Resolution/Hilbert hat der SK recht viele davon:

2 Stück pro Operator $\neg$, $\wedge$, $\vee$, $\forall$, $\exists$,
jeweils für die linke und die rechte Seite von Sequenzen
(positive und negative Form der Regel)

Axiome des SK

Zum Hervorheben von Formeln in Sequenzen schreiben wir

$$\Gamma, \varphi \Rightarrow \Delta, \psi \quad \text{statt} \quad \Gamma \cup \{\varphi\} \Rightarrow \Delta \cup \{\psi\}$$

Definition Axiome SK

Die *Axiome* des Sequenzenkalküls (SK) sind alle Sequenzen der Form $\Gamma, \varphi \Rightarrow \Delta, \varphi$.

Axiome sind offensichtlich gültige Sequenzen.

Schlussregeln des SK

$$(\neg\Rightarrow)\ \frac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma, \neg\varphi \Rightarrow \Delta} \qquad (\Rightarrow\neg)\ \frac{\Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}$$

$$(\vee\Rightarrow)\ \frac{\Gamma, \varphi \Rightarrow \Delta \qquad \Gamma, \psi \Rightarrow \Delta}{\Gamma, \varphi \vee \psi \Rightarrow \Delta} \qquad (\Rightarrow\vee)\ \frac{\Gamma \Rightarrow \Delta, \varphi, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}$$

$$(\wedge\Rightarrow)\ \frac{\Gamma, \varphi, \psi \Rightarrow \Delta}{\Gamma, \varphi \wedge \psi \Rightarrow \Delta} \qquad (\Rightarrow\wedge)\ \frac{\Gamma \Rightarrow \Delta, \varphi \qquad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}$$

$$(\exists\Rightarrow)\ \frac{\Gamma, \varphi[c] \Rightarrow \Delta}{\Gamma, \exists x\, \varphi(x) \Rightarrow \Delta}\ \ c \text{ nicht in } \Gamma,\ \Delta,\ \varphi(x) \qquad (\Rightarrow\exists)\ \frac{\Gamma \Rightarrow \Delta, \varphi[t]}{\Gamma \Rightarrow \Delta, \exists x\, \varphi(x)}$$

$$(\forall\Rightarrow)\ \frac{\Gamma, \varphi[t] \Rightarrow \Delta}{\Gamma, \forall x\, \varphi(x) \Rightarrow \Delta} \qquad (\Rightarrow\forall)\ \frac{\Gamma \Rightarrow \Delta, \varphi[c]}{\Gamma \Rightarrow \Delta, \forall x\, \varphi(x)}\ \ c \text{ nicht in } \Gamma,\ \Delta,\ \varphi(x)$$

T3.1

Ableitbarkeit im SK

Definition „ableitbare Sequenz“

Die Menge der *ableitbaren* Sequenzen ist die kleinste Menge von Sequenzen, die

- alle Axiome des SK enthält und
- abgeschlossen ist unter Regelanwendung: wenn Instanzen der Sequenzen in der oberen Zeile einer Schlussregel enthalten sind, so auch die entsprechende Instanz der unteren Zeile

Ist eine Sequenz $\Gamma \Rightarrow \Delta$ ableitbar, so schreiben wir: $\vdash \Gamma \Rightarrow \Delta$

Dabei bedeutet *Instanz:*
$\Gamma, \Delta, \varphi, \psi$ werden durch konkrete Formeln/Formelmengen ersetzt.

Beispiel T3.2

SK-Beweise

Definition SK-Beweis

Ein *SK-Beweis* ist ein Baum, dessen Knoten auf folgende Weise mit Sequenzen beschriftet sind:

- Jedes Blatt ist mit einem Axiom beschriftet
- Jeder innere Knoten ist mit einer Instanz der unteren Zeile einer Schlussregel beschriftet
- die Kinder dieses Knotens sind dann genau mit den entsprechenden Instanzen der Sequenzen in der oberen Zeile der Regel beschriftet.

Beachte:

- Jeder innere Knoten hat ein oder zwei Kinder.
- Eine Sequenz ist ableitbar gdw. sie als Knotenbeschriftung in einem SK-Beweis auftritt.

Beispiel T3.3

SK-Beweise

Zur Erinnerung:

In der Sequenz Γ, φ darf Γ auch φ enthalten, muss aber nicht

Darum darf man bei Anwendung von $(\Rightarrow \exists)$ und $(\forall \Rightarrow)$ im SK-Beweis die verwendete Teilformel „behalten“:

Beispiel $(\forall \Rightarrow)$:

$$(\forall \Rightarrow) \quad \frac{\Gamma, \varphi[t] \Rightarrow \Delta}{\Gamma, \forall x\, \varphi(x) \Rightarrow \Delta}$$

$$\frac{P(c) \Rightarrow P(c) \wedge P(d)}{\forall x\, P(x) \Rightarrow P(c) \wedge P(d)} \qquad \frac{\forall x\, P(x), P(c) \Rightarrow P(c) \wedge P(d)}{\forall x\, P(x) \Rightarrow P(c) \wedge P(d)}$$

(ohne Behalten) (mit Behalten)

Das gilt im Prinzip für alle Regeln, ist aber nur bei $(\Rightarrow \exists)$ und $(\forall \Rightarrow)$ nützlich (und notwendig!)

Korrektheit SK

Theorem (Korrektheit SK)

Wenn $\vdash \Gamma \Rightarrow \Delta$, dann $\models \Gamma \Rightarrow \Delta$ (jede ableitbare Sequenz ist gültig).

Beweis:

Es genügt zu zeigen:

1. Alle SK-Axiome sind gültig:

   Offensichtlich gilt $\bigwedge \Gamma \models \bigvee \Delta$, wenn es $\varphi \in \Gamma \cap \Delta$ gibt.

2. Wenn eine Sequenz $\Gamma \Rightarrow \Delta$ durch das Anwenden einer Schlussregel auf gültige Sequenzen entsteht, dann ist $\Gamma \Rightarrow \Delta$ gültig:

   Fallunterscheidung: ein Fall pro Regel. T3.4

Vollständigkeit SK

Theorem (Vollständigkeit SK)

Wenn $\models \Gamma \Rightarrow \Delta$, dann $\vdash \Gamma \Rightarrow \Delta$ (jede gültige Sequenz ist ableitbar).

Beweisskizze: (Details im Grädel-Skript)

Man beweist das Kontrapositiv:

wenn $\Gamma \Rightarrow \Delta$ nicht ableitbar, dann $\Gamma \Rightarrow \Delta$ nicht gültig, also $\bigwedge \Gamma \not\models \bigvee \Delta$.

Also zu zeigen: es gibt Modell $\mathfrak{A}$ für $\Gamma \cup \neg\Delta$, wobei $\neg\Delta = \{\neg\varphi \mid \varphi \in \Delta\}$

Im Prinzip möchten wir $\mathfrak{A}$ einfach aus Γ „ablesen“;

die Nicht-Ableitbarkeit von $\Gamma \Rightarrow \Delta$ soll sicherstellen, dass $\mathfrak{A} \models \neg\Delta$

Vollständigkeit SK

Theorem (Vollständigkeit SK)

Wenn $\models \Gamma \Rightarrow \Delta$, dann $\vdash \Gamma \Rightarrow \Delta$ (jede gültige Sequenz ist ableitbar).

„$\mathfrak{A}$ aus Γ ablesen“: wenn z. B.

$$\Gamma = \{Q_1(c), \neg Q_2(c), \exists x\, P(x), P(c)\} \qquad \Delta = \{Q_2(c), \neg P(c)\}$$

dann ist klar, wie $\mathfrak{A}$ aus Γ abgelesen wird und dass $\mathfrak{A} \models \neg\Delta$.

Das geht aber nicht immer so einfach:

$$\Gamma = \{Q_1(c) \vee Q_2(c), \exists x\, P(x)\} \qquad \Delta = \{\cdots\}$$

Man muss darum Γ und Δ erst vervollständigen. **T3.5**

Für später: das konstruierte Modell ist höchstens abzählbar unendlich.

Mehr zur Prädikatenlogik

Rekursive Aufzählbarkeit

Theorem (rekursive Aufzählbarkeit)

Für jede rekursiv aufzählbare Signatur τ sind rekursiv aufzählbar:

- die Menge aller Tautologien aus FO(τ)
- die Menge aller *un*erfüllbaren Sätze aus FO(τ)

Beweis:

1. Die Menge aller Sätze über Signatur τ ist rekursiv aufzählbar:
   - Erzeuge alle Strings über dem Alph. $\{\neg, \wedge, \vee, \exists, \forall, (,), =\} \cup \mathrm{VAR} \cup \tau$.
   - Gib diejenigen aus, die ein wohlgeformter FO-Satz sind.

Rekursive Aufzählbarkeit

Theorem (rekursive Aufzählbarkeit)
Für jede rekursiv aufzählbare Signatur τ sind rekursiv aufzählbar:

- die Menge aller Tautologien aus $\mathsf{FO}(\tau)$
- die Menge aller *un*erfüllbaren Sätze aus $\mathsf{FO}(\tau)$

Beweis:

2. Die Menge aller SK-Beweise über Signatur τ ist rekursiv aufzählbar:
   - Erzeuge alle Bäume mit max. binärer Verzweigung, deren Knoten mit Strings über dem Alphabet $\{\neg, \wedge, \vee, \exists, \forall, (,), =\} \cup \mathsf{VAR} \cup \tau$ markiert sind.
   - Gib diejenigen aus, die SK-Beweise sind.

Rekursive Aufzählbarkeit

Theorem (rekursive Aufzählbarkeit)
Für jede rekursiv aufzählbare Signatur τ sind rekursiv aufzählbar:

- die Menge aller Tautologien aus $\mathsf{FO}(\tau)$
- die Menge aller *un*erfüllbaren Sätze aus $\mathsf{FO}(\tau)$

Beweis:

3. Die Menge aller Tautologien ist rekursiv aufzählbar:
   - Erzeuge alle SK-Beweise
   - Für alle darin vorkommenden Sequenzen $\emptyset \Rightarrow \{\varphi\}$ gib φ aus

Begründung: φ ist Tautologie gdw. es SK-Beweis für $\emptyset \Rightarrow \{\varphi\}$ gibt (Korrektheit und Vollständigkeit des SK)

Analog für unerfüllbare Sätze: $\{\varphi\} \Rightarrow \emptyset$

Beachte: entscheidend ist hier die *Endlichkeit* von SK-Beweisen.

Rekursive Aufzählbarkeit

Korollar
Wenn τ mind. ein binäres Relationssymbol enthält, ist die Menge der *erfüllbaren* $\mathsf{FO}(\tau)$-Formeln *nicht* rekursiv aufzählbar.

Denn: Wären die erfüllbaren Formeln rekursiv aufzählbar, so wäre Erfüllbarkeit entscheidbar:

Um Erfüllbarkeit von φ zu prüfen, zähle simultan die erfüllbaren Formeln und die unerfüllbaren Formeln auf:

erfüllbar	unerfüllbar
φ_1	ψ_1
φ_2	ψ_2
$\vdots$	$\vdots$

Nach endlicher Zeit findet man Eingabeformel φ.

Rekursive Aufzählbarkeit

Über endlichen Strukturen kehrt sich die Situation um:

Theorem (Rekursive Aufzählbarkeit, endliche Modelle)
Über endlichen Modellen gilt:

1. die Menge der erfüllbaren Formeln ist rekursiv aufzählbar, für jede aufzählbare Signatur τ
2. die Menge der unerfüllbaren Formeln ist nicht rekursiv aufzählbar, ebensowenig die Menge der Tautologien

Beweis in der Übung.

Theorembeweiser

Rekursive Aufzählbarkeit liefert *Semi-Entscheidbarkeit* für Gültigkeit (und Unerfüllbarkeit):

- wenn Eingabe Tautologie, dann terminiert der Algorithmus nach endlicher Zeit und antwortet „gültig“;
- anderenfalls terminiert der Algorithmus nicht

Auf diesem Prinzip beruhen moderne Theorembeweiser wie `Vampire`, `Paradox`, `Spass`; allerdings wird ...

- meist Resolution verwendet (mit aufwendigen Optimierungstechniken)
- durch zusätzliche Verfahren in „vielen Fällen“ auch Terminierung auf Nicht-Tautologien erreicht

Kompaktheit

Der Kompaktheitssatz für FO ist wie in der Aussagenlogik formuliert:

Theorem (Kompaktheitssatz)

Für alle Mengen von Sätzen $\Gamma \subseteq$ FO und Sätze $\varphi \in$ FO gilt:

1. Γ ist erfüllbar gdw. jede endliche Teilmenge von Γ erfüllbar ist.
2. $\Gamma \models \varphi$ gdw. endliches $\Gamma_f \subseteq \Gamma$ existiert mit $\Gamma_f \models \varphi$.

Wichtige Anwendungen:

- Nicht-Ausdrückbarkeitsbeweise von Eigenschaften in FO
- fundamentale modelltheoretische Resultate wie die Sätze von Löwenheim-Skolem

Beweis des Kompaktheitssatzes verwendet Variation des Sequenzenkalküls.

Erweitertes Sequenzenkalkül

Beweis von Kompaktheit erfordert Variation des Sequenzenkalküls:

Anstatt für die Gültigkeit von Sequenzen $\models \Pi \Rightarrow \Delta$ interessiert man sich nun für die Folgerbarkeit von Sequenzen aus einer (eventuell unendlichen) Formelmenge Γ:

$$\Gamma \models \Pi \Rightarrow \Delta \quad \text{steht für} \quad \Gamma \models \bigwedge \Pi \rightarrow \bigvee \Delta$$

Für eine Menge von Sätzen $\Gamma \subseteq$ FO erhält man die Γ-*Erweiterung* des SK durch Hinzufügen der Regel

$$(\Gamma\text{-Regel}) \quad \frac{\Pi, \varphi \Rightarrow \Delta}{\Pi \Rightarrow \Delta} \quad \varphi \in \Gamma$$

Theorem (Korrektheit+Vollständigkeit erweiterter SK)

$\Pi \Rightarrow \Delta$ in der Γ-Erweiterung des SK ableitbar gdw. $\Gamma \models \Pi \Rightarrow \Delta$

Kompaktheit

Theorem (Kompaktheitssatz)

Für alle Mengen von Sätzen $\Gamma \subseteq$ FO und Sätze $\varphi \in$ FO gilt:

1. Γ ist erfüllbar gdw. jede endliche Teilmenge von Γ erfüllbar ist.
2. $\Gamma \models \varphi$ gdw. endliches $\Gamma_f \subseteq \Gamma$ existiert mit $\Gamma_f \models \varphi$.

Beweis mittels Γ-Erweiterung des Sequenzenkalküls, in der also wegen des vorigen Lemmas gilt:

Es gibt SK-Beweis für $\Pi \Rightarrow \Delta$ gdw. $\Gamma \models \bigwedge \Pi \rightarrow \bigvee \Delta$

T3.6

Beachte:

Es wird hier eine syntaktische Eigenschaft (Kalkül) in eine rein semantische (Erfüllbarkeit, Konsequenz) übertragen.

Nutzen der Kompaktheit

Wir nutzen die Kompaktheit zum Beweis einiger wichtiger modelltheoretischer Resultate, die …

- … sich auf die **Größe von Modellen** beziehen:
  - Wie groß können die Modelle einer gegebenen Formel werden?
  - Gibt es Formeln, die nur in endlichen/unendlichen/abzählbaren/ überabzählbaren Modellen erfüllbar sind?
- … uns erste Beobachtungen bezüglich der **Grenzen der Ausdrucksstärke** von FO erlauben:
  - Kann man eine Eigenschaft wie „das Modell ist endlich/unendlich/ abzählbar/überabzählbar“ in FO ausdrücken?

Unendliche Modelle

Theorem (unbeschränkte endliche Modelle)

Wenn ein FO-Satz φ beliebig große endliche Modelle besitzt (d. h. für jedes $n \geq 0$ gibt es Modell $\mathfrak{A}$ mit $|A| \geq n$),

dann hat φ auch ein unendliches Modell.

T3.7

Dieses Thm. impliziert eine **Beschränkung der Ausdrucksstärke** von FO:

Es gibt keinen FO-Satz φ, so dass $\mathfrak{A} \models \varphi$ gdw. $|A|$ endlich.

Das heißt: Endlichkeit ist *nicht* FO-ausdrückbar.

Für ein festes n ist „Modellgröße $\leq n$“ aber natürlich leicht ausdrückbar:

$$\forall x_0 \cdots \forall x_n \Big(\bigvee_{0 \leq i < j \leq n} x_i = x_j \Big)$$

Löwenheim-Skolem, aufsteigend

Theorem (*Aufsteigender* Satz von Löwenheim-Skolem)

Wenn ein FO-Satz φ ein unendliches Modell besitzt, dann gibt es für jede Menge U ein Modell $\mathfrak{A}$ von φ mit $|A| \geq |U|$.

T3.8

Beachte: Die Kardinalität von U ist beliebig!

Es folgt also z. B.:
wenn Γ unendliches Modell hat, dann auch überabzählbares Modell.

(Also ist auch Abzählbarkeit *nicht* FO-ausdrückbar.)

Korollar (Nicht-Standardmodell der Arithmetik)

$\mathsf{Th}(\mathbb{N}, +, \cdot, 0, 1)$ hat Modelle, die nicht isomorph zu $(\mathbb{N}, +, \cdot, 0, 1)$ sind.

Man kann sogar zeigen:
die Arithmetik $\mathsf{Th}(\mathbb{N}, +, \cdot, 0, 1)$ hat abzählbare Nichtstandardmodelle.

Löwenheim-Skolem, absteigend

Das im Vollständigkeitsbeweis des Sequenzenkalküls konstruierte Modell ist endlich oder abzählbar unendlich. Daher gilt:

Theorem (*Absteigender* Satz von Löwenheim-Skolem)

Wenn ein FO-Satz φ ein Modell besitzt, dann hat φ auch ein endliches oder abzählbar unendliches Modell.

T3.9

Es gibt also keine FO-Formeln, die nur überabzählbare Modelle haben.

Folgerung: Überabzählbarkeit *nicht* FO-ausdrückbar
(folgt nicht aus „Abzählbarkeit nicht FO-ausdrückbar“)

Übersicht Ausdrückbarkeit (bisher)

Eigenschaft: Modellgröße …	Ausdrückbar?	
$\leq n \ (n \in \mathbb{N})$	✔	$\forall x_0 \cdots \forall x_n \left(\bigvee_{0 \leq i < j \leq n} x_i = x_j \right)$
$< n, \ = n, \ \neq n, \ \geq n, \ > n$	✔	analog
… endlich	✘	Satz über unbeschränkte endl. Modelle
… abzählbar	✘	Satz von Löwenheim-Skolem, aufsteigend
… überabzählbar	✘	Satz von Löwenheim-Skolem, absteigend

Mehr zur Prädikatenlogik

Eigenschaften und Ausdrückbarkeit

In der Informatik ist die **Analyse der Ausdrucksstärke** von FO und anderen Logiken ein sehr wichtiges Thema, z. B.:

- **Zusammenhang „SQL als FO“:**
  Kann jede gewünschte Anfrage in SQL/FO ausgedrückt werden?
- **FO in der Verifikation von Soft-/Hardware:**
  Welche Systemeigenschaften können in FO beschrieben werden?
- **FO zur Definition von formalen Sprachen** (später)
  Welche formalen Sprachen können in FO definiert werden?

Ausdrückbarkeit meist leicht zu zeigen, Nicht-Ausdrückbarkeit schwierig!

Eigenschaften und Ausdrückbarkeit

Statt Anfragen/Systemeigenschaften/Sprachen betrachten wir verallgemeinernd *Eigenschaften* von Strukturen:

Sei R binäres Relationssymbol, T ternäres Relationssymbol

Beispiel 1: die Eigenschaft „$R^{\mathfrak{A}}$ ist eine Äquivalenzrelation“ ist FO-ausdrückbar:

$$\varphi = \forall x\, R(x,x) \ \wedge \ \forall x \forall y\, (R(x,y) \rightarrow R(y,x)) \ \wedge$$
$$\forall x \forall y \forall z\, (R(x,y) \wedge R(y,z) \rightarrow R(x,z))$$

Beispiel 2: ebenso die Eigenschaft „In $T^{\mathfrak{A}}$ sind die ersten beiden Spalten ein Primärschlüssel“:

$$\varphi = \forall x \forall y \forall z \forall z' \left(\left(T(x,y,z) \wedge T(x,y,z') \right) \rightarrow z = z' \right)$$

Eigenschaften und Ausdrückbarkeit

Definition Eigenschaft, Ausdrückbarkeit

Eine *Eigenschaft* ist eine Klasse von Strukturen, die unter Isomorphie abgeschlossen ist.

Eine Eigenschaft P ist *FO-ausdrückbar,* wenn es einen FO-Satz φ gibt, so dass für alle Strukturen $\mathfrak{A}$ gilt: $\mathfrak{A} \in P$ gdw. $\mathfrak{A} \models \varphi$.

Beispiele:

$P_1 = \{\mathfrak{A} \mid R^{\mathfrak{A}}$ ist eine Äquivalenzrelation$\}$

$P_2 = \{\mathfrak{A} \mid$ in $T^{\mathfrak{A}}$ sind die ersten beiden Spalten ein Primärschlüssel$\}$

Eigenschaften, die nicht unter Isomorphie abgeschlossen sind,

- sind trivialerweise nicht FO-ausdrückbar und
- „passen nicht zur Philosophie von FO".

Eigenschaften und Ausdrückbarkeit

Die **Sätze von Löwenheim/Skolem und verwandte Resultate** haben gezeigt, dass folgende Eigenschaften in FO nicht ausdrückbar sind:

- Endlichkeit von Strukturen
- Abzählbarkeit / Überabzählbarkeit von Strukturen

In der Informatik sind aber meist andere Eigenschaften relevant.

Im Folgenden: Werkzeuge zur Analyse der Ausdrucksstärke

- *Kompaktheitstheorem*
  ist das klassische Werkzeug aus der mathematischen Logik.
- *Ehrenfeucht-Fraïssé-Spiele*
  sind ein sehr flexibles Werkzeug, bieten viele Vorteile.

Nicht-Ausdrückbarkeit über Kompaktheit

Zur Erinnerung:

Ein ungerichteter Graph $G = (V, E)$ ist *zusammenhängend,*

wenn es für alle Knoten $v, v' \in V$ eine Knotenfolge $v_1, \dots, v_n$ gibt, so dass $v = v_1,\ v_n = v'$ und $\{v_i, v_{i+1}\} \in E$ für $1 \leq i < n$

Ungerichtete Graphen sind nichts anderes als $\{E\}$-Strukturen, E binäres Relationssymbol, das symmetrisch interpretiert wird.

Wir beweisen die Nicht-Ausdrückbarkeit von Zusammenhang mittels Kompaktheit.

Theorem

Zusammenhang von ungerichteten Graphen ist nicht FO-ausdrückbar.

T3.10

Nicht-Ausdrückbarkeit über Kompaktheit

Kann man also Zusammenhang auch in SQL nicht ausdrücken?

Leider können wir das nicht aus dem vorigen Resultat folgern, denn

- Datenbankinstanzen entsprechen *endlichen* Modellen.
- Der Kompaktheitssatz gilt auf endlichen Modellen *nicht!* T3.11

  Der eben geführte Beweis schließt also *nicht* aus, dass es einen FO-Satz φ gibt, so dass für alle *endlichen* Strukturen $\mathfrak{A}$ gilt:

  $\mathfrak{A} \models \varphi$ gdw. $\mathfrak{A}$ zusammenhängend

☛ **Wir brauchen ein besseres Werkzeug zur Analyse der Ausdrucksstärke!**

Ehrenfeucht-Fraïssé-Spiele

Ehrenfeucht-Fraïssé-Spiele sind eine elegante Beweistechnik, die es erlaubt, die Nicht-Ausdrückbarkeit von Eigenschaften in FO (und anderen Logiken) nachzuweisen.

Eine für die Informatik besonders wichtige Eigenschaft:

> Ehrenfeucht-Fraïssé-Spiele funktionieren auf endlichen und unendlichen Modellen gleichermaßen.

Wie wir gesehen haben, gilt das für viele andere Resultate nicht (z. B. Kompaktheit, rekursive Aufzählbarkeit von Tautologien).

Ehrenfeucht-Fraïssé-Spiele

- Zwei Spielerinnen: *Spoiler* (auch: Herausforderer) und *Duplicator*
- Das Spielbrett besteht aus zwei Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ (endlich oder unendlich).
- Die Spielerinnen wechseln sich ab; *Spoiler* beginnt.
- Die zu spielende Rundenzahl k ist beliebig, aber vorher festgelegt.
- In jeder Runde wählt *Spoiler* zunächst eine Struktur ($\mathfrak{A}$ oder $\mathfrak{B}$), dann ein Element der gewählten Struktur.
  Duplicator antwortet mit einem Element der anderen Struktur.
- Im Prinzip: *Spoiler* möchte zeigen, dass $\mathfrak{A}$ und $\mathfrak{B}$ unterschiedlich sind; *Duplicator*, dass sie gleich sind.
- Die genaue Gewinnbedingung werden wir gleich definieren.

T3.12

Gewinnbedingung

Der Einfachheit halber arbeiten wir im Folgenden mit *relationalen* Signaturen.

Wenn $\mathfrak{A}$ Struktur und $S \subseteq A$, so ist $\mathfrak{A}|_S$ die *Einschränkung* von $\mathfrak{A}$ auf S:

- das Universum von $\mathfrak{A}|_S$ ist S
- für alle n-stelligen Relationssymbole R:

$$R^{\mathfrak{A}|_S} = \{(a_1, \ldots, a_n) \in R^{\mathfrak{A}} \mid a_1, \ldots, a_n \in S\}$$

Definition: partieller Isomorphismus

Seien $\mathfrak{A}$ und $\mathfrak{B}$ τ-Strukturen und $\delta : A \to B$ eine partielle Funktion mit Definitionsbereich $\mathsf{dom}(\delta)$ und Wertebereich $\mathsf{ran}(\delta)$.

Dann ist δ ein *partieller Isomorphismus,*
wenn δ ein Isomorphismus von $\mathfrak{A}|_{\mathsf{dom}(\delta)}$ nach $\mathfrak{B}|_{\mathsf{ran}(\delta)}$ ist.

T3.13

Gewinnbedingung

Gewinnerin eines EF-Spiels:

- Angenommen, es wurden alle k Runden gespielt und in Runde i wurden die Elemente $a_i \in A$ und $b_i \in B$ ausgewählt
- Wenn die erreichte Menge

$$\{(a_1, b_1), \ldots, (a_k, b_k)\}$$

  ein partieller Isomorphismus ist, gewinnt *Duplicator*.
- Sonst gewinnt *Spoiler*.

Uns interessiert weniger die Gewinnerin eines einzelnen Spielverlaufs, sondern hauptsächlich die Gewinnerin *bei optimaler Spielweise.*

Gewinnstrategien

- Das Spiel auf $\mathfrak{A}$,$\mathfrak{B}$ mit k Zügen bezeichnen wir mit $\mathcal{G}_k(\mathfrak{A},\mathfrak{B})$.
- Eine Spielerin *hat eine Gewinnstrategie* für $\mathcal{G}_k(\mathfrak{A},\mathfrak{B})$, wenn sie dieses Spiel gewinnen kann, egal, was die Gegnerin tut.
- Gewinnstrategien für $\mathcal{G}_k(\mathfrak{A},\mathfrak{B})$ kann man anschaulich als endliche Spielbäume der Tiefe k darstellen.
- Für jedes Spiel $\mathcal{G}_k(\mathfrak{A},\mathfrak{B})$ hat *Spoiler* oder *Duplicator* eine Gewinnstrategie.

  (Denn das gilt für alle endlichen 2-Personen-Spiele, in denen kein Unentschieden möglich ist.)

Beispiele **T3.14**

Gewinnstrategien

Beachte:

- Abwechselnde Züge entsprechen Quantorenalternierungen.
- Gewinnstrategien für *Spoiler* und *Duplicator* sind dual.

Gewinnstrategie *Spoiler:*

$\exists$ Zug *Spoiler*, so dass
  $\forall$ Züge *Duplicator* gilt
    $\exists$ Zug *Spoiler*, so dass
      $\ddots$
        $\forall$ Züge *Duplicator* gilt
          Spiel ist kein part. Isom.

Gewinnstrategie *Duplicator:*

$\forall$ Züge *Spoiler* gilt
  $\exists$ Zug *Duplicator*, so dass
    $\forall$ Züge *Spoiler* gilt
      $\ddots$
        $\exists$ Zug *Duplicator*, so dass
          Spiel ist part. Isom.

Quantorenrang

Wir stellen nun den **Zusammenhang zwischen EF und FO** her.

Die Anzahl der Spielrunden entspricht dabei dem *Quantorenrang.*

Definition Quantorenrang

Der *Quantorenrang* qr(φ) einer Formel φ ist die Schachtelungstiefe von Quantoren in φ. Genauer:

- wenn φ ein Atom, dann qr$(\varphi) = 0$
- qr$(\neg\varphi)$ = qr(φ)
- qr$(\varphi \wedge \psi)$ = qr$(\varphi \vee \psi)$ = max{qr(φ), qr(ψ)}
- qr$(\exists x\, \varphi)$ = qr$(\forall x\, \varphi)$ = qr$(\varphi) + 1$

Beispiel:

$$\mathrm{qr}(\exists x\, (\forall y\, P(x,y) \vee \exists z\, \forall y\, Q(x,y,z))) = 3$$

Ehrenfeucht-Fraïssé-Theorem

Theorem (Ehrenfeucht-Fraïssé)

Seien $\mathfrak{A}$ und $\mathfrak{B}$ τ-Strukturen. Für alle $k \geq 0$ sind folgende Aussagen äquivalent:

1. $\mathfrak{A} \models \varphi$ gdw. $\mathfrak{B} \models \varphi$ für alle Sätze $\varphi \in$ FO(τ) mit qr$(\varphi) \leq k$
2. *Duplicator* hat Gewinnstrategie für $\mathcal{G}_k(\mathfrak{A},\mathfrak{B})$.

Beachte: $\mathfrak{A}$ und $\mathfrak{B}$ können hier endlich oder unendlich sein. **T3.15**

Beweisidee:

- per Induktion über k
- Damit die Induktion durchgeht, müssen wir Spiele betrachten, die schon einige Runden gespielt wurden.
- In Punkt 1 müssen wir dann auch freie Variablen betrachten.

Vollständiger Beweis im Skript von Grädel [StudIP]

Mehr zur Prädikatenlogik

Methodologie-Theorem

Grundlage für Beweise der Nicht-Ausdrückbarkeit mittels EF-Spielen:

Theorem (Methodologie-Theorem)

Sei P eine Eigenschaft. Wenn es für jedes $k \geq 0$ Strukturen $\mathfrak{A}_k$, $\mathfrak{B}_k$ gibt, so dass

1. $\mathfrak{A}_k \in P$ und $\mathfrak{B}_k \notin P$ und
2. *Duplicator* hat eine Gewinnstrategie für $\mathcal{G}_k(\mathfrak{A}_k, \mathfrak{B}_k)$,

dann ist P nicht FO-ausdrückbar.

T3.16

Funktioniert auch für jede Strukturklasse $\mathcal{K}$ (z. B. alle endlichen Strukturen), solange die Paare $\mathfrak{A}_k, \mathfrak{B}_k$ aus $\mathcal{K}$ stammen.

Parität

Wichtige Einschränkung: FO kann nicht „unbeschränkt zählen".

„Beschränktes Zählen" heißt Zählen bis zu Konstante n, z. B.:

$$\forall x_0 \cdots \forall x_n \Big(\bigvee_{0 \leq i < j \leq n} x_i = x_j \Big) \qquad \text{(„Struktur hat Größe } \leq n\text{")}$$

„Unbeschränktes Zählen" z. B.:

- FINITE $= \{\mathfrak{A} \mid |A| \text{ ist endlich (aber beliebig groß)}\}$
- EVEN $= \{\mathfrak{A} \mid |A| \text{ ist geradzahlig}\}$
  ODD $= \{\mathfrak{A} \mid |A| \text{ ist ungeradzahlig}\}$

  Unendliche Modelle können beliebig zu EVEN/ODD gehören oder nicht.

Theorem

EVEN und ODD sind nicht FO-ausdrückbar, weder in der Klasse aller Strukturen noch in der Klasse der endlichen Strukturen (jeweils über einer beliebigen Signatur τ).

T3.17

Parität

Also kann auch SQL nicht unbeschränkt zählen, Parität nicht ausdrücken.

Das gilt natürlich nicht nur für die Größe des Universums, z. B.

„finde alle Übungsgruppen mit ungeradzahlig vielen Studierenden"

auch nicht ausdrückbar (in reinem SQL / relation algebra).

Zusammenhang

Schon gesehen:
Zusammenhang von ungerichteten Graphen ist nicht FO-ausdrückbar.

Wir zeigen nun:
Dies gilt auch in der Klasse aller endlichen Strukturen
(und damit auch für SQL).

Wir wählen ungerichtete Graphen $\mathfrak{A}_k, \mathfrak{B}_k$ so dass:

- $\mathfrak{A}_k$ ein Kreis der Länge 2^k (also zusammenhängend)
- $\mathfrak{B}_k$ besteht aus zwei disjunkten Kreisen der Länge 2^k (also nicht zusammenhängend)

Wir müssen zeigen: *Duplicator* hat Gewinnstrategie für $\mathcal{G}_k(\mathfrak{A}_k, \mathfrak{B}_k)$

Skizze T3.18

Zusammenhang

Für zwei Knoten u, v ist die *Distanz* $d(u, v)$

- die Länge des kürzesten Pfades von u nach v wenn so ein Pfad existiert
- $d(u, v) = \infty$ wenn kein solcher Pfad existiert

Für $\ell \geq 0$ ist die *ℓ-Nachbarschaft* $N_\ell(u) = \{v \in V \mid d(u, v) \leq \ell\}$

Lemma

Duplicator kann $\mathcal{G}_k(\mathfrak{A}_k, \mathfrak{B}_k)$ so spielen, dass nach i Zügen ein Spielstand $\{(a_1, b_1), \ldots, (a_i, b_i)\}$ erreicht ist, so dass für $1 \leq j < \ell \leq i$:

$$(*) \quad d(a_j, a_\ell) = d(b_j, b_\ell) \quad \text{oder} \quad d(a_j, a_\ell),\ d(b_j, b_\ell) > 2^{k-i}$$

T3.19

Korollar

Duplicator hat Gewinnstrategie für $\mathcal{G}_k(\mathfrak{A}_k, \mathcal{B}_k)$.

T3.20

Zusammenhang

Korollar

Zusammenhang ist nicht FO-ausdrückbar, weder in der Klasse aller Strukturen noch in der Klasse aller endlichen Strukturen.

Erreichbarkeit

Für viele Anwendungen ist es nützlich,
Erreichbarkeit bezüglich einer binären Relation verwenden zu können.

Beispiel SQL:
Datenbank mit Direktverbindungen einer Fluggesellschaft;
Mittels Erreichbarkeit bekommt alle Verbindungen, mit und ohne Umsteigen.

Wichtiges Resultat:

Theorem

Sei E binäre Relation und $\tau = \{E\}$.

Es gibt keinen Satz $\varphi(x, y) \in \text{FO}(\tau)$, der Erreichbarkeit (entlang E) definiert, d. h. so dass für alle Strukturen $\mathfrak{A} = (A, E^{\mathfrak{A}})$ gilt:

$$\mathfrak{A} \models \varphi[a, b] \quad \text{gdw.} \quad \text{es einen Pfad in } \mathfrak{A} \text{ von } a \text{ nach } b \text{ gibt}$$

Erreichbarkeit

Theorem

Sei E binäre Relation und $\tau = \{E\}$.

Es gibt keine Formel $\varphi(x, y) \in \mathrm{FO}(\tau)$, die Erreichbarkeit (entlang E) definiert, d. h. so dass für alle Strukturen $\mathfrak{A} = (A, E^{\mathfrak{A}})$ gilt:

$\mathfrak{A} \models \varphi[a, b]$ gdw. es einen Pfad in $\mathfrak{A}$ von a nach b gibt

Beweis:

Angenommen, es gebe eine FO-Formel $\varphi(x, y)$ wie beschrieben.

Dann könnte man den Zusammenhang von ungerichteten Graphen mit dem folgenden Satz ausdrücken:

$$\forall x \, \forall y \, \varphi(x, y)$$

Dies widerspricht aber dem vorigen Korollar, dass Zusammenhang nicht FO-ausdrückbar ist. ❑

Nicht-Ausdrückbarkeit

Auch nicht FO-ausdrückbar z. B.:

- Azyklizität
- Graphen, die ein Baum sind
- Planarität
- k-Färbbarkeit für beliebiges (fixes) $k \geq 2$
- quasi jede algorithmisch interessante Eigenschaft von Graphen (wir werden in Teil 4 sehen, warum das so ist!)

Zusammenfassung Prädikatenlogik 1. Stufe

	Vorteile ☺	Nachteile ☹
Verwendung	Repräsentation von Strukturen aus Mathematik & Informatik Anwendungen: DB, Verifikation	
Ausdrucks-vermögen	viel ausdrucksstärker als Aussagenlogik	Grenzen der Ausdrucksstärke: unbegrenztes Zählen, algo. wichtige Graph-Eigenschaften
Berechenbar-/ Entscheidbarkeit	Auswertung entscheidbar; Tautologien rekursiv aufzählbar	Erfüllbarkeit usw. unentscheidbar (auch auf endlichen Strukturen) Erfüllbarkeit nicht semi-entscheidb.
Kalküle	viele, z. B. Sequenzenkalkül	
Tools	Theorembeweiser wie `Vampire, Paradox, Spass`	

Überblick Schlussfolgerungsprobleme

	Auswertungs-problem	Erfüllbarkeits-problem	Gültigkeits-problem	Folgerbarkeits-problem
Horn-Formeln	in Linearzeit	in Polyzeit	in Linearzeit	in Polyzeit
Aussagenlogik	in Linearzeit	NP-vollständig	co-NP-vollständig	co-NP-vollständig
Prädikatenlogik 1. Stufe	PSpace-vollständig	unentscheidbar nicht semi-entsch.	unentscheidbar semi-entsch.	unentscheidbar semi-entsch.
Prädikatenlogik 2. Stufe				