Logik

Teil 2: Prädikatenlogik Grundlagen

Prädikatenlogik

Für viele Zwecke der Informatik (und Mathematik) abstrahiert die Aussagenlogik zu stark.

Betrachte z. B. die Beispiele aus der Einleitung:

Alle Menschen sind sterblich Sokrates ist ein Mensch	Jedes P ist auch ein Q x ist ein P
Sokrates ist sterblich	x ist ein Q

- $\forall n \in \mathbb{N} : \exists n' \in \mathbb{N} : n' = \mathsf{nf}(n)$
- $\forall n \in \mathbb{N} : \mathsf{nf}(n) \neq 0$
- $\cdots$

Bei diesen Aussagen geht es nicht nur um Wahrheitswerte:
Objekte (Menschen, natürliche Zahlen) und Quantifizierung sind zentral!

Prädikatenlogik

Die Prädikatenlogik wurde von Frege gegen Ende des 19. Jh. eingeführt.

Zentrale Elemente

1. Formeln zusammengesetzt aus Objektvariablen, Booleschen Operatoren und Quantoren

2. eine Semantik, die Objekte sowie deren Eigenschaften und Beziehungen erfasst

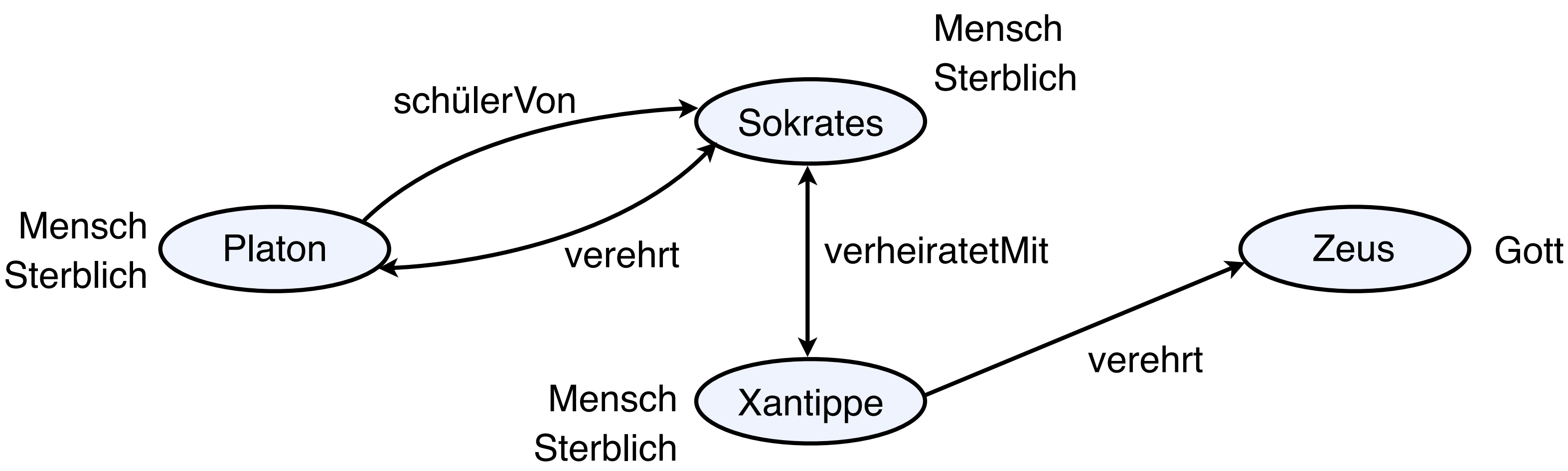
Prädikatenlogik spielt zentrale Rolle in Informatik, Mathematik, Philosophie

Andere Namen: Logik erster Stufe, First-order Logic, Predicate calculus

Abkürzung: FO

Vorschau

Eine semantische Struktur der Logik erster Stufe:



Zu dieser Struktur passende Beispielformeln:

$$\forall x\,(\text{Mensch}(x) \rightarrow \text{Sterblich}(x))$$

$$\exists x\,\big(\,\exists y\,(\,\text{verehrt}(x,y) \land \text{Gott}(y)\,)\,\land\,\exists y\,(\,\text{verheiratetMit}(x,y) \land \forall z\,(\,\text{verehrt}(y,z) \rightarrow \neg\text{Gott}(z)\,)\,)\,\big)$$

Übersicht Teil 2

Next

Strukturen

Die Semantik der Prädikatenlogik basiert auf so genannten **Strukturen.**

Man kann viele Dinge als Struktur repräsentieren:

- Graphen und Hypergraphen
- Relationale Datenbanken
- Transitionssysteme aus der Hard/Software-Verifikation
- Mathematische Strukturen wie Gruppen, Ringe, Körper
- Wörter (Strings) und Bäume
- etc.

Dies macht die Prädikatenlogik zu einem sehr generellen Werkzeug.

Signaturen

Die Namen, die in einer Struktur verwendet werden, bilden deren Signatur.

Definition 2.1 (Signatur)

Eine Signatur τ ist eine Menge von Relations- und Funktionssymbolen. Jedes dieser Symbole hat eine feste endliche Stelligkeit $n \geq 0$.

Nullstellige Funktionssymbole nennen wir Konstantensymbole.

Beispiel:

Die Signatur der Arithmetik ist $\{+, \cdot, 0, 1\}$, wobei

$+$ und $\cdot$ zweistellige Funktionssymbole

0 und 1 Konstantensymbole

(Es gibt in dieser speziellen Signatur keine Relationssymbole)

Signaturen

Mehr Beispiele:

- Die Signatur eines gerichteten Graphen ist $\{E\}$, mit E zweistelligem Relationssymbol (das die Kanten repräsentiert)

- Die Signatur einer Datenbank besteht aus je einem n-stelligen Relationssymbol für jede n-spaltige Tabelle

Eine Signatur heißt

- relational, wenn sie keine Funktionssymbole enthält, z.B. $\tau = \{E\}$
- funktional, wenn sie keine Relationssymbole enthält, z.B. $\tau = \{+, \cdot, 0, 1\}$

Signaturen

Notation: Normalerweise verwenden wir

- P, Q, R für Relationssymbole

  Relationssymbole nennen wir auch Prädikate

- f, g, h für Funktionssymbole

- c, d, e für Konstantensymbole

- τ für Signaturen

Statt „Stelligkeit“ sagen wir auch Arität.

Strukturen

Definition 2.2 (Struktur)

Sei τ eine Signatur. Eine τ-Struktur $\mathfrak{A}$ besteht aus

- einer nichtleeren Menge A, dem Universum von $\mathfrak{A}$
- für jedes n-stellige Relationssymbol $P \in \tau$ einer n-stelligen Relation $P^{\mathfrak{A}} \subseteq A^n$
- für jedes n-stellige Funktionssymbol $f \in \tau$ einer n-stelligen Funktion $f^{\mathfrak{A}} : A^n \to A$

$\mathfrak{A}$ hat also die Form $(A, P_1^{\mathfrak{A}}, P_2^{\mathfrak{A}}, \ldots, f_1^{\mathfrak{A}}, f_2^{\mathfrak{A}}, \ldots)$.

Beachte:

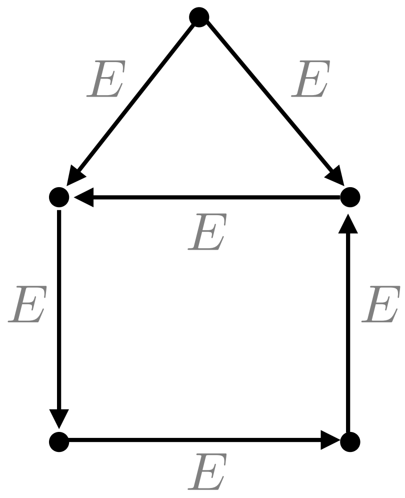
- jedes unäre Relationssymbol wird als Teilmenge von A interpretiert
- jedes Funktionssymbol wird als totale Funktion interpretiert
- jedes Konstantensymbol wird als Element von A interpretiert

Notation:

- Wenn die Signatur τ aus dem Kontext heraus klar ist, so sprechen wir einfach von Strukturen statt von τ-Strukturen
- Strukturen bezeichnen wir mit Buchstaben in Frakturschrift $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$,
- der entsprechende lateinische Buchstabe A, B, C steht für das Universum der Struktur
- die Elemente des Universums bezeichnen wir mit a, b

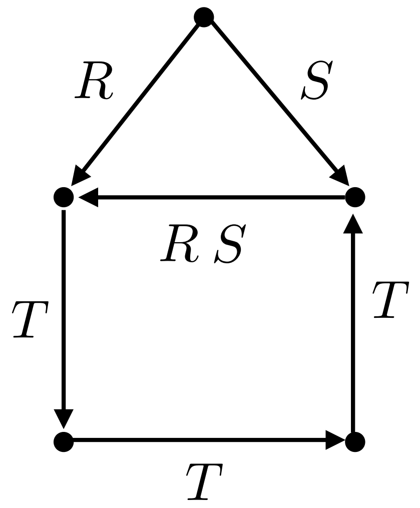
Strukturen generalisieren Graphen:

Struktur $(A, E^{\mathfrak{A}})$ mit E binärem Relationssymbol ist nichts weiter als ein gerichteter Graph (und umgekehrt)



Strukturen generalisieren Graphen:

Struktur $(A, E^{\mathfrak{A}})$ mit E binärem Relationssymbol ist nichts weiter als ein gerichteter Graph (und umgekehrt)

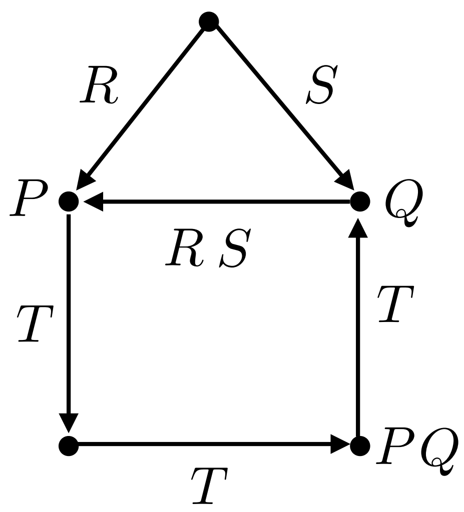


Mehrere binäre Relationssymbole liefern kantenbeschriftete Graphen

Struktur hat dann Form $(A, R^{\mathfrak{A}}, S^{\mathfrak{A}}, T^{\mathfrak{A}})$

Strukturen generalisieren Graphen:

Struktur $(A, E^{\mathfrak{A}})$ mit E binärem Relationssymbol ist nichts weiter als ein gerichteter Graph (und umgekehrt)



Mehrere binäre Relationssymbole liefern kantenbeschriftete Graphen

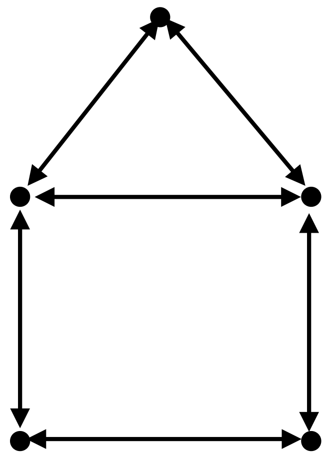
Struktur hat dann Form $(A, R^{\mathfrak{A}}, S^{\mathfrak{A}}, T^{\mathfrak{A}})$

Zusätzliche unäre Relationssymbole liefern Knotenbeschriftungen

Struktur hat dann Form $(A, R^{\mathfrak{A}}, S^{\mathfrak{A}}, T^{\mathfrak{A}}, P^{\mathfrak{A}}, Q^{\mathfrak{A}})$

Strukturen generalisieren Graphen:

Struktur $(A, E^{\mathfrak{A}})$ mit E binärem Relationssymbol ist nichts weiter als ein gerichteter Graph (und umgekehrt)



Ungerichtete Graphen z.B. über symmetrische Kanten repräsentierbar

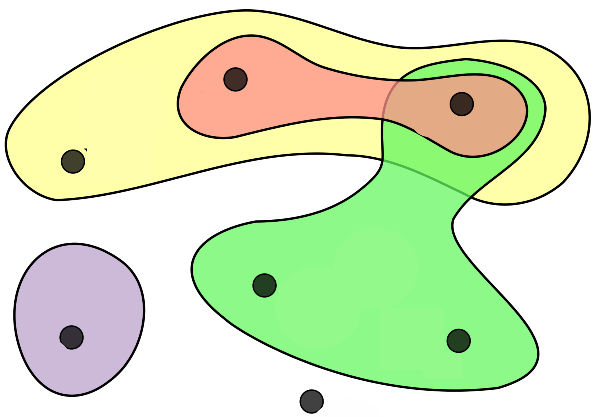
Strukturen, Graphen, Algebren

Strukturen generalisieren Graphen:

Struktur $(A, E^{\mathfrak{A}})$ mit E binärem Relationssymbol ist nichts weiter als ein gerichteter Graph (und umgekehrt)

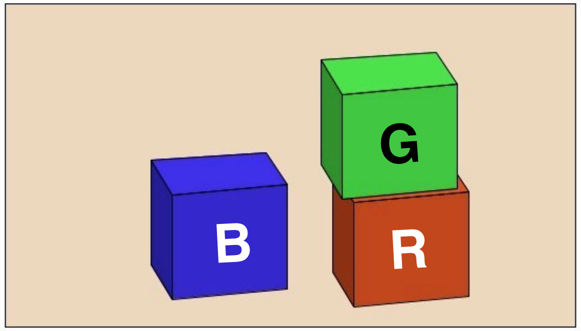
Und (gerichtete) Hypergraphen:

Strukturen über relationalen Signaturen beliebiger Stelligkeit sind kantenbeschriftete Hypergraphen und umgekehrt.



Strukturen – Beispiel 1

Blocks World



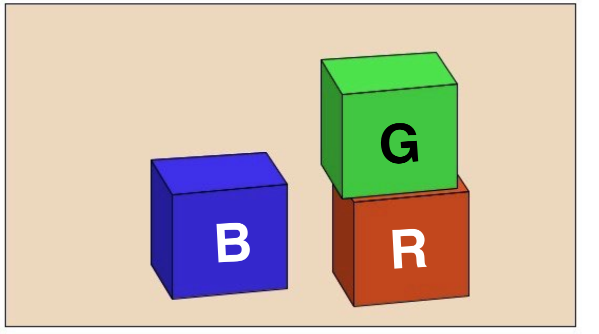
Signatur:

- unäre Relationssymbole Block, R, G, B
- binäre Relationssymbole auf, unter, neben
- Konstantensymbol lieblingsblock

Struktur $\mathfrak{A}$:

- $A = \{rb, gb, bb\}$
- $\text{Block}^{\mathfrak{A}} = \{rb, gb, bb\}$, $\text{R}^{\mathfrak{A}} = \{rb\}$, $\text{G}^{\mathfrak{A}} = \{gb\}$, $\text{B}^{\mathfrak{A}} = \{bb\}$
- $\text{auf}^{\mathfrak{A}} = \{(gb, rb)\}$, $\text{unter}^{\mathfrak{A}} = \{(rb, gb)\}$, $\text{neben}^{\mathfrak{A}} = \{(bb, rb), (rb, bb)\}$
- $\text{lieblingsblock}^{\mathfrak{A}} = rb$

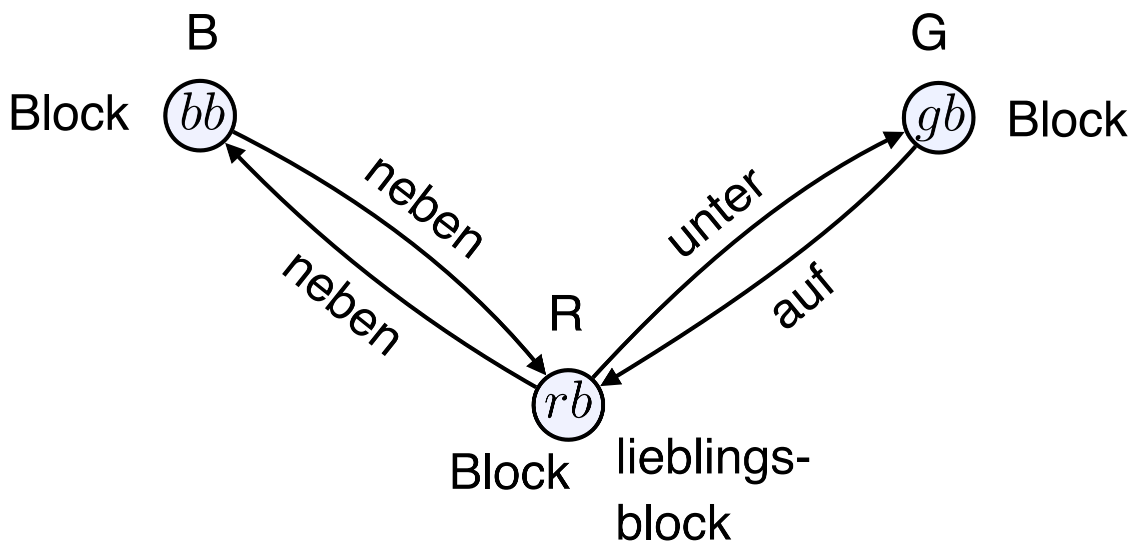
Strukturen – Beispiel 1

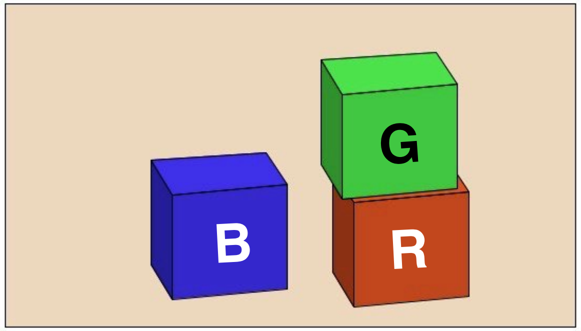


Struktur $\mathfrak{A}$:

- $A = \{rb, gb, bb\}$
- Block$^{\mathfrak{A}} = \{rb, gb, bb\}$, R$^{\mathfrak{A}} = \{rb\}$, G$^{\mathfrak{A}} = \{gb\}$, B$^{\mathfrak{A}} = \{bb\}$
- auf$^{\mathfrak{A}} = \{(gb, rb)\}$, unter$^{\mathfrak{A}} = \{(rb, gb)\}$, neben$^{\mathfrak{A}} = \{(bb, rb), (rb, bb)\}$
- lieblingsblock$^{\mathfrak{A}} = rb$

Strukturen – Beispiel 1





Struktur $\mathfrak{A}$:

- $A = \{rb, gb, bb\}$
- Block$^{\mathfrak{A}} = \{rb, gb, bb\}$, R$^{\mathfrak{A}} = \{rb\}$, G$^{\mathfrak{A}} = \{gb\}$, B$^{\mathfrak{A}} = \{bb\}$
- auf$^{\mathfrak{A}} = \{(gb, rb)\}$, unter$^{\mathfrak{A}} = \{(rb, gb)\}$, neben$^{\mathfrak{A}} = \{(bb, rb), (rb, bb)\}$
- lieblingsblock$^{\mathfrak{A}} = rb$

Strukturen – Beispiel 2

Relationale Datenbank ist eine endliche Sammlung von Tabellen

Jeder Tabelle T zugeordnet ist Spaltenzahl n

Z.B. Datenbank mit 2 Tabellen:

- Tabelle Film, 3 Spalten:
  - Titel (Typ String)
  - Jahr (Typ pos. Integer)
  - Regisseur (Typ String)
- Tabelle Schauspieler, 2 Spalten:
  - Name (Typ String)
  - Filmtitel (Typ String)

Beispielinstanz I:

Film:

Titel	Jahr	Regisseur
Die Vögel	1963	Hitchcock
Marnie	1964	Hitchcock
Goldfinger	1964	Hamilton

Schauspieler:

Name	Filmtitel
Connery	Marnie
Connery	Goldfinger
Hedren	Die Vögel

Strukturen – Beispiel 2

Relationale Datenbank ist eine endliche Sammlung von Tabellen

Jeder Tabelle T zugeordnet ist Spaltenzahl n

Z.B. Datenbank mit 2 Tabellen:

- Tabelle Film, 3 Spalten:
  - Titel (Typ String)
  - Jahr (Typ pos. Integer)
  - Regisseur (Typ String)
- Tabelle Schauspieler, 2 Spalten:
  - Name (Typ String)
  - Filmtitel (Typ String)

Konkrete Datenbankinstanz I kann als (endliche!) Struktur

$$\mathfrak{A} = (A, T_1^{\mathfrak{A}}, T_2^{\mathfrak{A}}, \ldots, T_k^{\mathfrak{A}})$$

repräsentiert werden, wobei

- $T_1, \ldots, T_k$ Relationssymbole für die Tabellen der Datenbank sind
- A die Vereinigung über alle Werte ist, die in den Tabellen vorkommen

Strukturen – Beispiel 2

Beispielinstanz I:

Film:

Titel	Jahr	Regisseur
Die Vögel	1963	Hitchcock
Marnie	1964	Hitchcock
Goldfinger	1964	Hamilton

Schauspieler:

Name	Filmtitel
Connery	Marnie
Connery	Goldfinger
Hedren	Die Vögel

Struktur $\mathfrak{A}$:

- $A = \{\mathsf{DieV\ddot{o}gel}, \mathsf{Marnie}, \mathsf{Goldfinger}, \mathsf{1963}, \mathsf{1964}, \mathsf{Hitchcock}, \mathsf{Hamilton}, \mathsf{Connery}, \mathsf{Hedren}\}$
- $\mathsf{Film}^{\mathfrak{A}} = \{(\mathsf{DieV\ddot{o}gel}, \mathsf{1963}, \mathsf{Hitchcock}), (\mathsf{Marnie}, \mathsf{1964}, \mathsf{Hitchcock}), (\mathsf{Goldfinger}, \mathsf{1964}, \mathsf{Hamilton})\}$
- $\mathsf{Schauspieler}^{\mathfrak{A}} = \{(\mathsf{Connery}, \mathsf{Marnie}), (\mathsf{Connery}, \mathsf{Goldfinger}), (\mathsf{Hedren}, \mathsf{DieV\ddot{o}gel})\}$

Strukturen – Beispiel 2

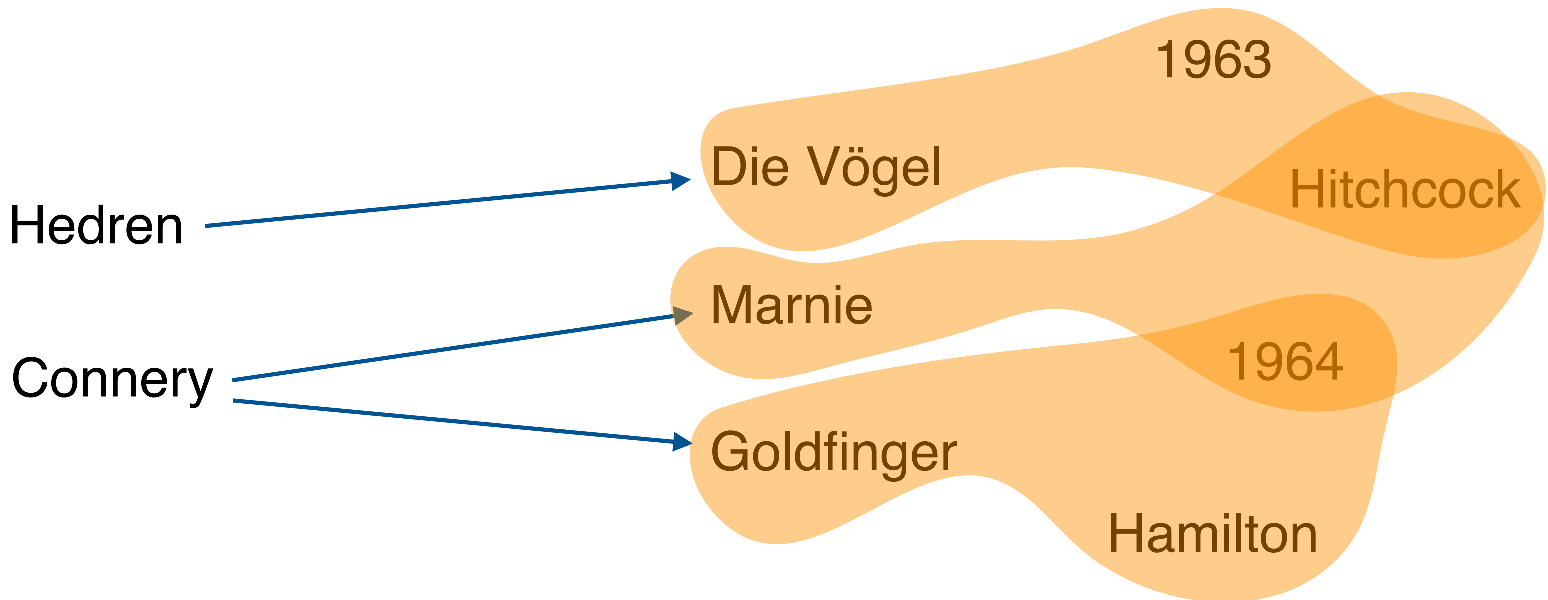
Beispielinstanz I:

Film:

Titel	Jahr	Regisseur
Die Vögel	1963	Hitchcock
Marnie	1964	Hitchcock
Goldfinger	1964	Hamilton

Schauspieler:

Name	Filmtitel
Connery	Marnie
Connery	Goldfinger
Hedren	Die Vögel

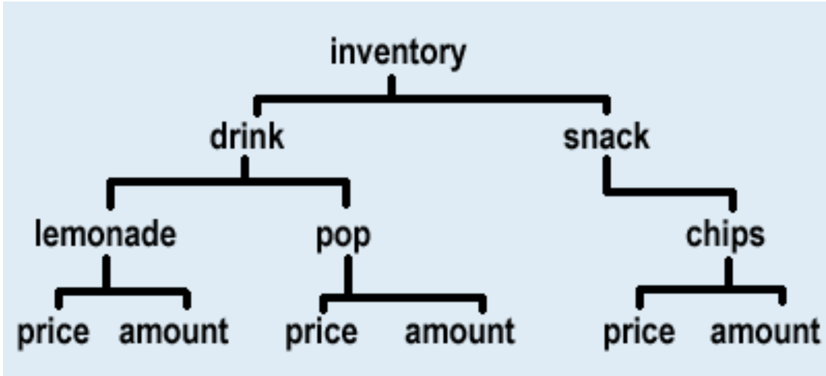


Strukturen – Beispiel 3

XML-Dokument kann als endliche, baumförmige Struktur gesehen werden

```
<inventory>
    <drink>
        <lemonade>
            <price>$2.50</price>
            <amount>20</amount>
        </lemonade>
        <pop>
            <price>$1.50</price>
            <amount>10</amount>
        </pop>
    </drink>

    <snack>
        <chips>
            <price>$4.50</price>
            <amount>60</amount>
        </chips>
    </snack>
</inventory>
```



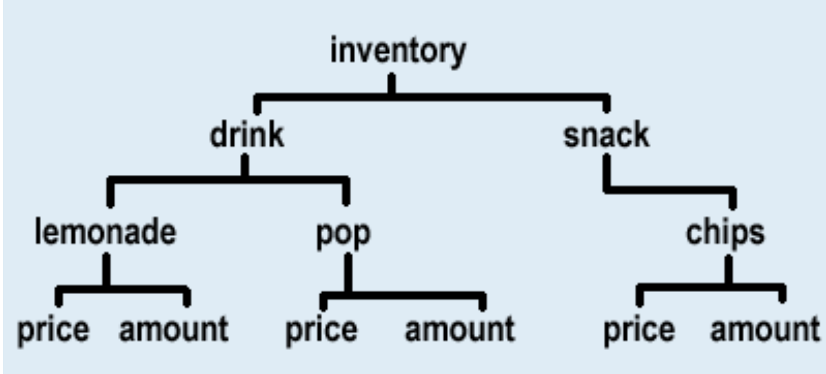
Signatur:

binäre Relationssymbole succ für „successor" und

sord für „successor order"

sowie ein unäres Relationssymbol für jedes Tag (drink, snack usw.)

Strukturen – Beispiel 3



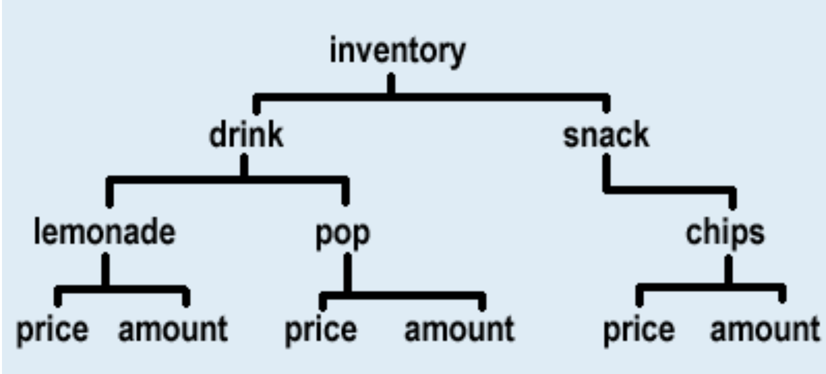
Signatur:

binäre Relationssymbole succ für „successor“ und

sord für „successor order“

sowie ein unäres Relationssymbol für jedes Tag (drink, snack usw.)

Strukturen – Beispiel 3



$$A = \{\varepsilon, 0, 1, 00, 01, 10, 000, 001, 010, 011, 100, 101\}$$

$$\mathsf{succ}^{\mathfrak{A}} = \{(w, w0) \mid w0 \in A\} \cup \{(w, w1) \mid w1 \in A\}$$

$$\mathsf{sord}^{\mathfrak{A}} = \{(w0, w1) \mid w0, w1 \in A\}$$

$$\mathsf{Inventory}^{\mathfrak{A}} = \{\varepsilon\}$$

$$\mathsf{Price}^{\mathfrak{A}} = \{000, 010, 110\}$$

Signatur:

binäre Relationssymbole succ für „successor“ und
sord für „successor order“

sowie ein unäres Relationssymbol für jedes Tag (drink, snack usw.)

Strukturen – Beispiel 4

Algebraische Strukturen aus der Mathematik (siehe “Diskrete Strukturen”)
z. B. Arithmetik der natürlichen Zahlen:

$$\mathfrak{N} = (\mathbb{N}, +^{\mathfrak{N}}, \cdot^{\mathfrak{N}}, 0^{\mathfrak{N}}, 1^{\mathfrak{N}}) \qquad \text{(unendlich!)}$$

wobei

- $+^{\mathfrak{N}}, \cdot^{\mathfrak{N}}$ die natürliche Interpretation von $+$ und $\cdot$ sind:

$$+^{\mathfrak{N}}(x, y) = x + y \qquad \cdot^{\mathfrak{N}}(x, y) = x \cdot y$$

- $0^{\mathfrak{N}} = 0$ und $1^{\mathfrak{N}} = 1$
  (0,1 sowohl Konstantensymbole als auch Elemente des Universums)

Bei offensichtlicher Interpretation lassen wir das $\cdot^{\mathfrak{N}}$ oft weg, also z.B.

$$\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$$

Analog definiert man z. B. $\mathfrak{R} = (\mathbb{R}, +, \cdot, 0, 1)$ (überabzählbar!)

Prädikatenlogik

Syntax

Analog zur Unterscheidung zwischen Relations- und Funktionssymbolen:

Formeln der Prädikatenlogik bestehen aus zwei Bestandteilen:

- Terme, die aus (Objekt)variablen, Konstanten- und Funktionssymbolen gebildet werden
- Formeln bestehen dann aus Termen, den Booleschen Operatoren, Quantoren und Relationssymbolen

Wir definieren die Syntax daher in zwei Schritten.

Syntax (Schritt 1)

Wir fixieren eine abzählbar unendliche Menge VAR $= \{x_1, x_2, x_3, \dots\}$ von Objektvariablen.

Definition 2.3 (Term)

Die Menge der Terme ist induktiv wie folgt definiert:

- jede Variable ist ein Term.
- wenn $t_1, \dots, t_n$ Terme sind und f ein n-stelliges Funktionssymbol, dann ist auch $f(t_1, \dots, t_n)$ ein Term

Beachte: jedes Konstantensymbol ist damit ebenfalls ein Term!

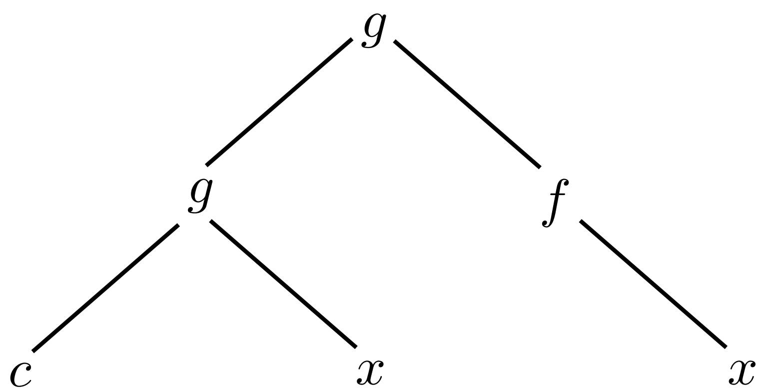
Beispiele:

$$x,\ c,\ f(x),\ g(x,x),\ g(f(x),c),\ g(g(c,c),f(x))$$

$$1 + ((1+1) \cdot 1) \qquad\qquad 1 + ((x+1) \cdot y)$$

Sprechweisen und Konventionen

- Wir bezeichnen Terme mit s und t
- Es ist oft nützlich, Terme als Bäume aufzufassen,
  z.B. $g(g(c, x), f(x))$ als



- Für Funktionssymbole wie $+$ und $\cdot$ verwenden wir Infix-Notation,
  also $x + c$ statt $+(x, c)$

Syntax (Schritt 2)

Definition 2.4 (FO-Formeln)

Die Menge der Formeln der Prädikatenlogik ist induktiv wie folgt definiert:

- sind t_1, t_2 Terme, dann ist $t_1 = t_2$ eine Formel
- sind $t_1, \ldots, t_n$ Terme und P ein n-stelliges Relationssymbol, dann ist $P(t_1, \ldots, t_n)$ eine Formel

} Atome

- wenn φ und ψ Formeln sind, dann auch $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$
- wenn φ eine Formel ist und $x \in$ VAR, dann sind $\exists x\, \varphi$ und $\forall x\, \varphi$ Formeln

Die Menge aller Formeln über einer Signatur τ bezeichnen wir mit FO(τ).

Beispiele: $x = c$ $\quad (P(x) \wedge Q(x)) \vee P(y) \quad \forall x\, \exists y\, P(x, f(y))$

$$\forall x\ \big(\ \exists y\, \mathsf{neben}(y, x) \vee \exists y\, \mathsf{auf}(y, x)\ \big)$$

$$\exists y\ \big(\ \mathsf{Film}(x, y, \mathsf{Hitchcock}) \wedge \mathsf{Schauspieler}(\mathsf{Connery}, x)\ \big)$$

Sprechweisen und Konventionen

- Statt $\neg(t = t')$ schreiben wir auch $t \neq t'$
- $\rightarrow$ und $\leftrightarrow$ sind analog zur AL definiert
- Klammern werden weggelassen, wenn das Resultat eindeutig ist, wobei $\neg$, $\exists$, $\forall$ stärker binden als $\wedge$, $\vee$ und $\wedge$, $\vee$ stärker binden als $\rightarrow$, $\leftrightarrow$

Also z. B. $\exists x\, P(x) \vee Q(x)$ für $(\exists x\, P(x)) \vee Q(x)$,

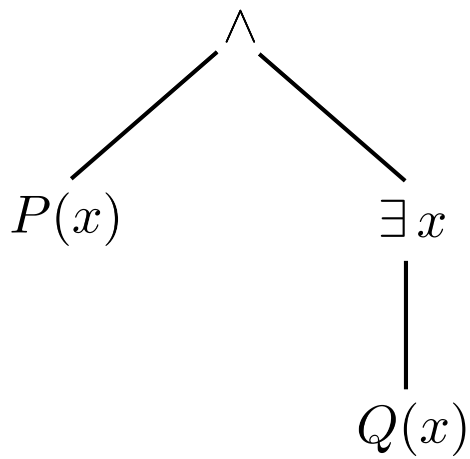
nicht für $\exists x\, (P(x) \vee Q(x))$

Freie und gebundene Variablen

Ein Vorkommen einer Variable in einer Formel kann durch einen Quantor gebunden sein oder nicht (dann ist die Variable frei)

Beispiel:

$$\varphi = P(\underset{\text{frei}}{x}) \wedge \exists x\, Q(\underset{\text{gebunden}}{x})$$



Einige Konventionen:

- Wenn wir eine Formel mit $\varphi(x_1, \ldots, x_n)$ bezeichnen, so sind $x_1, \ldots, x_n$ die freien Variablen in φ; für obige Formel: $\varphi(x)$
- Formeln ohne freie Variablen heißen Satz

Freie und gebundene Variablen

Präzise definiert man die Menge der freien Variablen wie folgt.

Definition 2.5 (Freie Variable)

Sei φ eine Formel. Die Menge $\mathsf{Frei}(\varphi)$ der freien Variablen von φ ist induktiv wie folgt definiert:

- Für atomare Formeln φ ist $\mathsf{Frei}(\varphi)$ die Menge aller Variablen in φ
- $\mathsf{Frei}(\neg\varphi) = \mathsf{Frei}(\varphi)$
- $\mathsf{Frei}(\varphi \wedge \psi) = \mathsf{Frei}(\varphi \vee \psi) = \mathsf{Frei}(\varphi) \cup \mathsf{Frei}(\psi)$
- $\mathsf{Frei}(\exists x\, \varphi) = \mathsf{Frei}(\forall x\, \varphi) = \mathsf{Frei}(\varphi) \setminus \{x\}$

Semantik (Schritt 1)

Struktur interpretiert nur Symbole, aber keine Variablen – dafür Zuweisung:

Definition 2.6 (Zuweisung)

Sei $\mathfrak{A}$ eine Struktur. Eine Zuweisung in $\mathfrak{A}$ ist eine Abbildung $\beta : \text{VAR} \to A$.

Man erweitert β wie folgt induktiv auf Terme:

- wenn $t = f(t_1, \dots, t_k)$, dann $\beta(t) = f^{\mathfrak{A}}(\beta(t_1), \dots, \beta(t_k))$

Ein Paar $(\mathfrak{A}, \beta)$ mit β Zuweisung in $\mathfrak{A}$ heißt *Interpretation*.

Beachte: der implizite Induktionsanfang ist:

- wenn $t = x \in \text{VAR}$, dann $\beta(t) = \beta(x)$
- wenn $t = c$ Konstante, dann $\beta(t) = c^{\mathfrak{A}}$

T2.1

Schreibweise:

$\beta[x/a]$ bezeichnet Zuweisung β modifiziert so dass $x \mapsto a$

Semantik (Schritt 2)

Definition 2.7 (Semantik von FO)

Wir definieren Erfülltheitsrelation $\models$ zwischen Interpretationen $(\mathfrak{A}, \beta)$ und FO-Formeln induktiv wie folgt:

- $\mathfrak{A}, \beta \models t = t'$ gdw. $\beta(t) = \beta(t')$
- $\mathfrak{A}, \beta \models P(t_1, \ldots, t_n)$ gdw. $(\beta(t_1), \ldots, \beta(t_n)) \in P^{\mathfrak{A}}$
- $\mathfrak{A}, \beta \models \neg\varphi$ gdw. $\mathfrak{A}, \beta \not\models \varphi$
- $\mathfrak{A}, \beta \models \varphi \wedge \psi$ gdw. $\mathfrak{A}, \beta \models \varphi$ und $\mathfrak{A}, \beta \models \psi$
- $\mathfrak{A}, \beta \models \varphi \vee \psi$ gdw. $\mathfrak{A}, \beta \models \varphi$ oder $\mathfrak{A}, \beta \models \psi$
- $\mathfrak{A}, \beta \models \exists x\, \varphi$ gdw. ein $a \in A$ existiert mit $\mathfrak{A}, \overbrace{\beta[x/a]}^{\text{Wie } \beta\text{, außer } x \mapsto a} \models \varphi$
- $\mathfrak{A}, \beta \models \forall x\, \varphi$ gdw. für alle $a \in A$ gilt, dass $\mathfrak{A}, \beta[x/a] \models \varphi$

Wenn $\mathfrak{A}, \beta \models \varphi$, dann ist $(\mathfrak{A}, \beta)$ ein Modell für φ.

Semantik (Schritt 2)

Man sieht leicht:

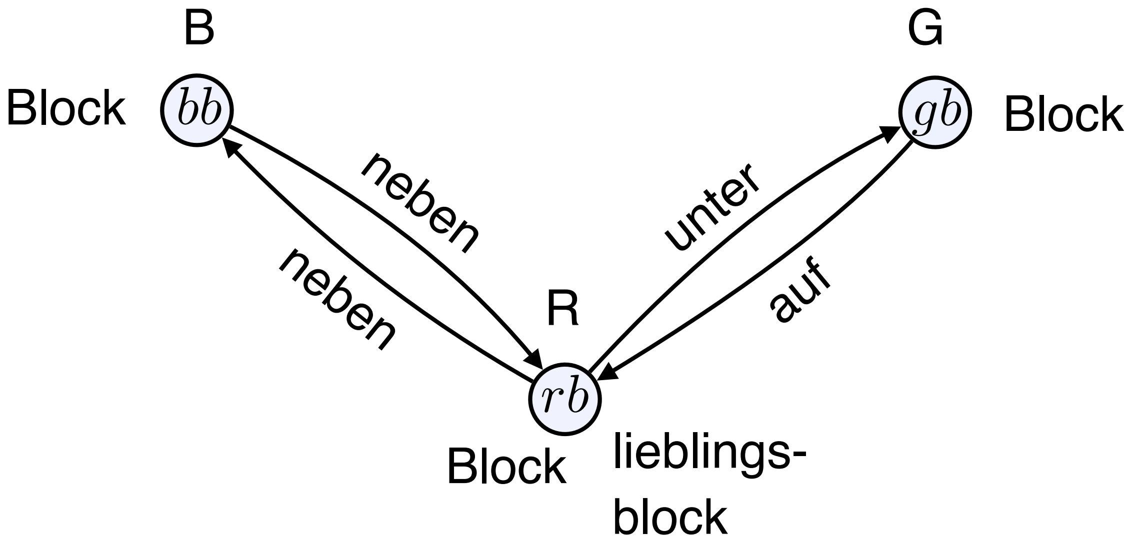
Wenn φ Satz, dann ist $\mathfrak{A}, \beta \models \varphi$ unabhängig von β

d.h.: $\mathfrak{A}, \beta \models \varphi$ gdw. $\mathfrak{A}, \beta' \models \varphi$ für beliebiges β'

Für Sätze φ schreiben wir darum statt $\mathfrak{A}, \beta \models \varphi$ nur $\mathfrak{A} \models \varphi$.

Beispiel 1

Struktur $\mathfrak{A}$:



Dann $\mathfrak{A} \models \exists x\, R(x) \land \exists x\, G(x) \land \exists x\, B(x)$

denn $\mathfrak{A} \models \exists x\, R(x)$ und $\mathfrak{A} \models \exists x\, G(x)$ und $\mathfrak{A} \models \exists x\, B(x)$

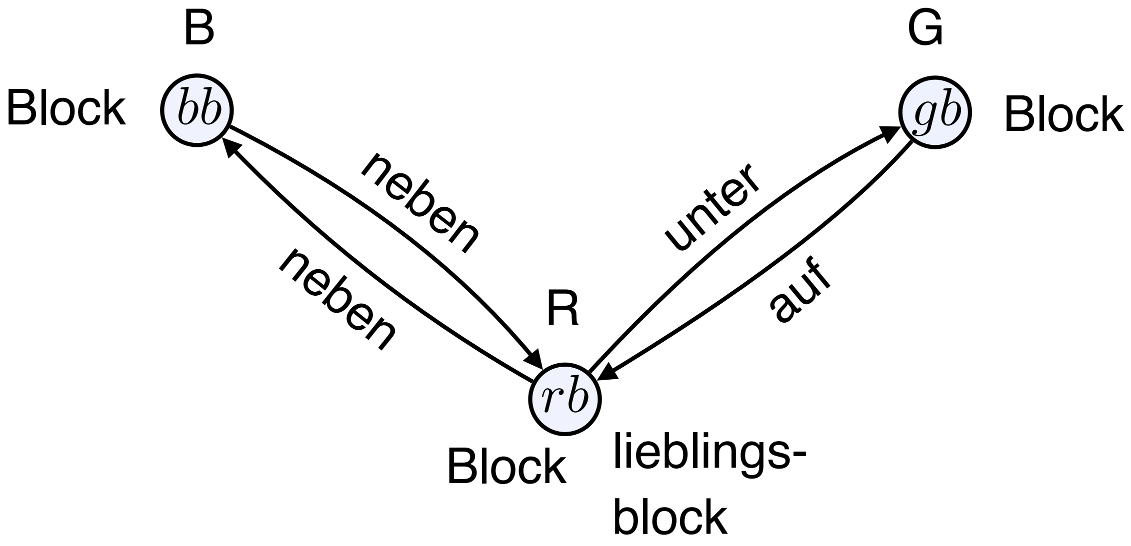
$\mathfrak{A} \models \exists x\, \text{neben}(x, x)$?

$\mathfrak{A} \models \exists x\, (R(x) \land \forall y(\text{auf}(y, x) \to G(y)))$?

$\mathfrak{A} \models \forall x\, ((R(x) \land B(x)) \to G(x))$?

Beispiel 1

Struktur $\mathfrak{A}$:



Betrachte β mit $\beta(x) = bb$, $\beta(y) = gb$, $\beta(z) = gb$

$\mathfrak{A}, \beta \models x \neq \text{lieblingsblock}$?

$\mathfrak{A}, \beta \models G(z) \wedge \exists z\,(\text{neben}(x, z) \wedge \text{unter}(z, y))$?

Beispiel 2

$\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$

$\mathfrak{N} \models \forall x \forall y\, (x + y = y + x)$

$\mathfrak{N}, \beta \models \exists z\, (z \neq 0 \wedge x + z = y)$ gdw $\beta(y) > \beta(x)$

Abkürzung für diese Formel: $y > x$

$\mathfrak{N}, \beta \models$ **?**

gdw $\beta(x)$ eine Primzahl ist

Abkürzung für diese Formel: $\mathsf{prim}(x)$

$\mathfrak{N} \models \forall x\, (\mathsf{prim}(x) \rightarrow \exists y\, (y > x \wedge \mathsf{prim}(y)))$?

$\mathfrak{N} \models \forall x \exists y\, (y > x \wedge \mathsf{prim}(y) \wedge \mathsf{prim}(y + 1 + 1))$?

Beispiel 3

FO kann Eigenschaften von (hier: ungerichteten) Graphen ausdrücken, die bekannten algorithmischen Problemen aus der Informatik entsprechen

G enthält eine k-Clique, für ein festes $k \geq 1$:

(eine Menge M von k Knoten, so dass jeder Knoten in M mit jedem Knoten in M verbunden ist)

$$\exists x_1 \cdots \exists x_k \bigwedge_{1 \leq i < j \leq k} (E(x_i, x_j) \wedge x_i \neq x_j)$$

G enthält ein Dominating Set der Grösse $\leq k$, für ein festes $k \geq 1$:

(eine Menge M von $\leq k$ Knoten, so dass jeder Knoten in M oder adjazent zu einem Knoten in M ist)

$$\exists x_1 \cdots \exists x_k \forall y \, (\bigvee_{1 \leq i \leq k} (y = x_i \vee E(y, x_i)))$$

Wir werden später sehen: es gibt auch viele natürliche Graphprobleme, die nicht in FO ausgedrückt werden können.

Kurze Erinnerung

Syntax der Prädikatenlogik

Konst.

Terme: $t: \quad x \mid c \mid f(t_1, \ldots, t_n)$

Var. $\quad$ *n*-stell. Funktionssymbol angewendet auf *n* Terme

Formeln: $\varphi: \quad t_1 = t_2 \mid P(t_1, \ldots, t_n) \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \exists x\, \varphi \mid \forall x\, \varphi$

Atome $\quad$ Boolesche Operatoren $\quad$ Quantoren

Sätze: Formeln ohne freie Variablen

Vorkommen nicht durch Quantor gebunden

Semantik der Prädikatenlogik

Strukturen: $\mathfrak{A} = (A, P_1^{\mathfrak{A}}, P_2^{\mathfrak{A}}, \ldots, f_1^{\mathfrak{A}}, f_2^{\mathfrak{A}}, \ldots)$

nicht leeres Universum

Interpretation der Relations- und Funktionssymbole aus Signatur τ

Interpretationen $(\mathfrak{A}, \beta)$ mit β : VAR $\to A$ Zuweisung

Koinzidenzlemma

Analog zur Aussagenlogik: $\mathfrak{A}, \beta \models \varphi$ ist unabhängig von Interpretation der Symbole und Variablen, die in φ nicht (bzw. nicht frei) vorkommen.

sig(φ) bezeichne die Signatur der Formel φ, also die Menge der in φ vorkommenden Relations- und Funktionssymbole

Lemma 2.8 (Koinzidenzlemma)

Sei φ eine FO-Formel und $(\mathfrak{A}, \beta)$, $(\mathfrak{A}', \beta')$ Interpretationen, so dass

- $A = A'$
- $S^{\mathfrak{A}} = S^{\mathfrak{A}'}$ für alle $S \in$ sig(φ)
- für alle $x \in$ Frei(φ) gilt: $\beta(x) = \beta'(x)$

T2.2

Dann $\mathfrak{A}, \beta \models \varphi$ gdw. $\mathfrak{A}', \beta' \models \varphi$

Beweis per Induktion über den Aufbau von φ.

Koinzidenzlemma

Wenn wir mit einer Formel φ arbeiten, so erlaubt uns das Koinzidenz-lemma, in Zuweisungen nur die Variablen Frei(φ) zu betrachten.

Das erlaubt insbesondere folgende Notation:

Für eine Formel $\varphi(x_1, \ldots, x_k)$ schreiben wir

$$\mathfrak{A} \models \varphi[a_1, \ldots, a_k]$$

wenn $\mathfrak{A}, \beta \models \varphi$, wobei $\beta(x_i) = a_i$ für $1 \leq i \leq k$

Isomorphismus

Intuitiv: es existiert ein Isomorphismus zwischen zwei Strukturen wenn sie sich nur durch Umbenennen der Elemente des Universums unterscheiden.

Definition 2.9 (Isomorphismus)

Seien $\mathfrak{A}$ und $\mathfrak{B}$ Strukturen. Bijektion $\pi : A \to B$ ist Isomorphismus, wenn folgende Bedingungen erfüllt sind:

1. Für jedes n-stellige Relationssymbol P und alle $a_1, \ldots, a_n \in A^n$:
$$(a_1, \ldots, a_n) \in P^{\mathfrak{A}} \text{ gdw. } (\pi(a_1), \ldots, \pi(a_n)) \in P^{\mathfrak{B}}$$
2. Für jedes n-stellige Funktionssymbol f und alle $a_1, \ldots, a_n \in A^n$:
$$\pi(f^{\mathfrak{A}}(a_1, \ldots, a_n)) = f^{\mathfrak{B}}(\pi(a_1), \ldots, \pi(a_n))$$
(für Konstanten c ergibt sich: $\pi(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$)

$\mathfrak{A}$ und $\mathfrak{B}$ sind isomorph wenn Isomorphismus zwischen $\mathfrak{A}$ und $\mathfrak{B}$ existiert.

T2.3

Isomorphismus

Sei f zweistelliges Funktionssymbol und c Konstantensymbol

Betrachte Strukturen

- $\mathfrak{A} = (A, f^{\mathfrak{A}}, c^{\mathfrak{A}})$ mit

  $A = \mathbb{N}$ Menge der natürlichen Zahlen

  $f^{\mathfrak{A}}(i, j) = i + j$ für alle $i, j \in \mathbb{N}$

  $c^{\mathfrak{A}} = 0$

- $\mathfrak{B} = (B, f^{\mathfrak{B}}, c^{\mathfrak{B}})$ mit

  $B = \{2^i \mid i \in \mathbb{N}\}$ Menge aller Zweierpotenzen

  $f^{\mathfrak{B}}(i, j) = i \cdot j$ für alle $i, j \in B$

  $c^{\mathfrak{B}} = 1$

$\mathfrak{A}$ und $\mathfrak{B}$ sind isomorph, $\pi : A \to B$ mit $\pi(i) = 2^i$ ist Isomorphismus

Isomorphielemma

Lemma 2.10 (Isomorphielemma)

Seien $\mathfrak{A}$, $\mathfrak{B}$ isomorphe Strukturen und φ ein FO-Satz. Dann gilt:

$$\mathfrak{A} \models \varphi \text{ gdw. } \mathfrak{B} \models \varphi$$

Intuitiv:

Die Namen der Elemente des Universums sind irrelevant für FO

Wir wollen Lemma 2.10 per Induktion über den Aufbau von φ beweisen

Dabei ergeben sich jedoch Formeln mit freien Variablen, was nicht zur Formulierung von Lemma 2.10 passt (das nur über Sätze spricht)

Wir müssen das Lemma daher zunächst geeignet umformulieren

Isomorphielemma

Lemma 2.10 (Isomorphielemma)

Seien $\mathfrak{A}$, $\mathfrak{B}$ isomorphe Strukturen und φ ein FO-Satz. Dann gilt:

$$\mathfrak{A} \models \varphi \text{ gdw. } \mathfrak{B} \models \varphi$$

Lemma 2.10b (Isomorphielemma - generalisierte Version)

Seien $\mathfrak{A}$, $\mathfrak{B}$ Strukturen, $\pi : A \to B$ ein Isomorphismus, φ eine FO-Formel.
Seien zudem $\mathfrak{I}_{\mathfrak{A}} = (\mathfrak{A}, \alpha)$ und $\mathfrak{I}_{\mathfrak{B}} = (\mathfrak{B}, \beta)$ Interpretationen so dass

$$\beta(x) = \pi(\alpha(x)) \text{ für alle Variablen } x.$$

Dann gilt: $$(*)\ \mathfrak{I}_{\mathfrak{A}} \models \varphi \text{ gdw. } \mathfrak{I}_{\mathfrak{B}} \models \varphi.$$

Isomorphielemma

Lemma 2.10b (Isomorphielemma - generalisierte Version)

Seien $\mathfrak{A}$, $\mathfrak{B}$ Strukturen, $\pi : A \to B$ ein Isomorphismus, φ eine FO-Formel.
Seien zudem $\mathfrak{I}_{\mathfrak{A}} = (\mathfrak{A}, \alpha)$ und $\mathfrak{I}_{\mathfrak{B}} = (\mathfrak{B}, \beta)$ Interpretationen so dass

$\beta(x) = \pi(\alpha(x))$ für alle Variablen x.

Dann gilt: $(*)\ \mathfrak{I}_{\mathfrak{A}} \models \varphi$ gdw. $\mathfrak{I}_{\mathfrak{B}} \models \varphi$.

Beweis: per Induktion über den Aufbau von φ

Induktionsbeweise in FO folgen i.d.R. der Zweiteilung Terme / Formeln
d.h. man beweist erst geeignete Aussage über Terme, dann über Formeln

Hier: $(**)\ \beta(t) = \pi(\alpha(t))$ für alle Terme t

Induktionsanfang:

$t = x$ Variable — Per Annahme (siehe Lemma)

$t = c$ Konstante — Bed. 2 Isomorphismus liefert $\beta(c) = \pi(\alpha(c))$

Isomorphielemma

Lemma 2.10b (Isomorphielemma - generalisierte Version)

Seien $\mathfrak{A}$, $\mathfrak{B}$ Strukturen, $\pi : A \to B$ ein Isomorphismus, φ eine FO-Formel.

Seien zudem $\mathfrak{I}_\mathfrak{A} = (\mathfrak{A}, \alpha)$ und $\mathfrak{I}_\mathfrak{B} = (\mathfrak{B}, \beta)$ Interpretationen so dass

$$\beta(x) = \pi(\alpha(x)) \text{ für alle Variablen } x.$$

Dann gilt: $$(*)\ \mathfrak{I}_\mathfrak{A} \models \varphi \text{ gdw. } \mathfrak{I}_\mathfrak{B} \models \varphi.$$

Beweis: per Induktion über den Aufbau von φ

Induktionsbeweise in FO folgen i.d.R. der Zweiteilung Terme / Formeln

d.h. man beweist erst geeignete Aussage über Terme, dann über Formeln

Hier: $(**)\ \beta(t) = \pi(\alpha(t))$ für alle Terme t

Induktionsschritt: $t = f(t_1, \dots, t_n)$

$$\begin{aligned}
\beta(f(t_1,\dots,t_n)) &= f^\mathfrak{B}(\beta(t_1),\dots,\beta(t_n)) && \text{(Erw. } \beta\text{)}\\
&= f^\mathfrak{B}(\pi(\alpha(t_1)),\dots,\pi(\alpha(t_n))) && \text{(IV)}\\
&= \pi(f^\mathfrak{A}(\alpha(t_1),\dots,\alpha(t_n))) && \text{(Bed. 2. Isom.)}\\
&= \pi(\alpha(f(t_1,\dots,t_n))) && \text{(Erw. } \alpha\text{)}
\end{aligned}$$

Isomorphielemma

Lemma 2.10b (Isomorphielemma - generalisierte Version)

Seien $\mathfrak{A}$, $\mathfrak{B}$ Strukturen, $\pi : A \to B$ ein Isomorphismus, φ eine FO-Formel.
Seien zudem $\mathfrak{I}_{\mathfrak{A}} = (\mathfrak{A}, \alpha)$ und $\mathfrak{I}_{\mathfrak{B}} = (\mathfrak{B}, \beta)$ Interpretationen so dass

$$\beta(x) = \pi(\alpha(x)) \text{ für alle Variablen } x.$$

Dann gilt: $(*)\ \mathfrak{I}_{\mathfrak{A}} \models \varphi$ gdw. $\mathfrak{I}_{\mathfrak{B}} \models \varphi$.

Beweis: per Induktion über den Aufbau von φ

$$(**)\ \beta(t) = \pi(\alpha(t)) \text{ für alle Terme } t$$

Für den Beweis von $(*)$ Fallunterscheidung gemäß Form von φ.

Induktionsanfang: $t_1 = t_2$ und $P(t_1, \ldots, t_n)$

Induktionsschritt: Fälle $\underbrace{\neg\psi,\ \psi_1 \wedge \psi_2,\ \psi_1 \vee \psi_2}_{\text{als Übung}}$, $\exists x\, \psi$, $\forall x\, \psi$

T2.4

Endliche Modelle und Isomorphie

Umgekehrt:
kann man nicht-isomorphe Strukturen stets durch FO-Sätze unterscheiden?

Für endliche Strukturen ist das der Fall:

Lemma 2.11

Für jede endliche Struktur $\mathfrak{A}$ gibt es einen FO-Satz $\varphi_{\mathfrak{A}}$ so dass

für alle Strukturen $\mathfrak{B}$: $\mathfrak{B} \models \varphi_{\mathfrak{A}}$ gdw. $\mathfrak{B}$ isomorph ist zu $\mathfrak{A}$

Beweis: hier nur für die Signatur von Graphen $\tau = \{E\}$

Sei $\mathfrak{A}$ endliche Struktur und $A = \{a_1, \dots, a_n\}$.

$$\varphi_{\mathfrak{A}} = \exists x_1 \cdots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \bigvee_{1 \leq i \leq n} y = x_i \wedge$$

$$\bigwedge_{(a_i,a_j) \in E^{\mathfrak{A}}} E(x_i, x_j) \wedge \bigwedge_{(a_i,a_j) \notin E^{\mathfrak{A}}} \neg E(x_i, x_j)$$

❑

Prädikatenlogik

Auswertung

Definition 2.12 (Auswertungsproblem)

Das Auswertungsproblem der Prädikatenlogik ist:

Gegeben: FO-Formel $\varphi(x_1, \ldots, x_n)$, endliche Interpretation $(\mathfrak{A}, \beta)$ mit β Zuweisung für $x_1, \ldots, x_n$

Frage: Gilt $\mathfrak{A}, \beta \models \varphi$?

Zusammenhang zu vorherigen Beispielen:

Da wir *k*-Clique und *k*-Dominating Set in FO ausdrücken können, sind diese Probleme ein Spezialfall des Auswertungsproblems für FO

Wir können aber nicht die Frage von unendlich vielen Primzahlzwillingen durch Verwendung des Auswertungsproblems lösen

Denn die dafür relevante Struktur $(\mathbb{N}, +, \cdot, 0, 1)$ ist nicht endlich

Auswertung

Definition 2.12 (Auswertungsproblem)

Das Auswertungsproblem der Prädikatenlogik ist:

Gegeben: FO-Formel $\varphi(x_1, \ldots, x_n)$, endliche Interpretation $(\mathfrak{A}, \beta)$ mit β Zuweisung für $x_1, \ldots, x_n$

Frage: Gilt $\mathfrak{A}, \beta \models \varphi$?

Theorem 2.13

Das Auswertungsproblem der Prädikatenlogik erster Stufe ist entscheidbar in Zeit $n^{\mathcal{O}(k)}$, wobei

- n die Größe der Eingabestruktur $\mathfrak{A}$ ist und
- k die Größe der Eingabeformel φ.

Also exponentielle Laufzeit im Ggs. zu linearer Laufzeit bei Aussagenlogik

Das lässt sich vermutlich auch nicht verhindern

Auswertung

ausw$(\mathfrak{A}, \beta, \varphi)$

case

$\varphi = (t = t')$: return 1 if $\beta(t) = \beta(t')$, else return 0

$\varphi = P(t_1, \ldots, t_k)$: return 1 if $(\beta(t_1), \ldots, \beta(t_k)) \in P^{\mathfrak{A}}$, else return 0

$\varphi = \neg\psi$: return $1-$ausw$(\mathfrak{A}, \beta, \psi)$

$\varphi = \psi \wedge \vartheta$: return min{ausw$(\mathfrak{A}, \beta, \psi)$, ausw$(\mathfrak{A}, \beta, \vartheta)$}

$\varphi = \psi \vee \vartheta$: return max{ausw$(\mathfrak{A}, \beta, \psi)$, ausw$(\mathfrak{A}, \beta, \vartheta)$}

$\varphi = \exists x\, \psi$:

rufe ausw$(\mathfrak{A}, \beta[x/a], \psi)$ für alle $a \in A$

return 1 if ein Ruf erfolgreich, else return 0

$\varphi = \forall x\, \psi$:

rufe ausw$(\mathfrak{A}, \beta[x/a], \psi)$ für alle $a \in A$

return 1 if alle Rufe erfolgreich, else return 0

endcase

T2.5

Auswertung

ausw$(\mathfrak{A}, \beta, \varphi)$

case

$\varphi = (t = t')$: return 1 if $\beta(t) = \beta(t')$, else return 0

$\varphi = P(t_1, \ldots, t_k)$: return 1 if $(\beta(t_1), \ldots, \beta(t_k)) \in P^{\mathfrak{A}}$, else return 0

$\varphi = \neg\psi$: return $1-$a

$\varphi = \psi \wedge \vartheta$: return m

$\varphi = \psi \vee \vartheta$: return max{ausw$(\mathfrak{A}, \beta, \psi)$, ausw$(\mathfrak{A}, \beta, \vartheta)$}

$\varphi = \exists x\, \psi$:

rufe ausw$(\mathfrak{A}, \beta[x/a], \psi)$ für alle $a \in A$

return 1 if ein Ruf erfolgreich, else return 0

$\varphi = \forall x\, \psi$:

rufe ausw$(\mathfrak{A}, \beta[x/a], \psi)$ für alle $a \in A$

return 1 if alle Rufe erfolgreich, else return 0

endcase

Darin steckt nochmal ein (sehr einfacher) rekursiver Algorithmus (Übung!)

T2.5

Auswertung

Lemma 2.14

Der Algorithmus `ausw`

1. ist korrekt: $\texttt{ausw}(\mathfrak{A}, \beta, \varphi) = 1$ gdw. $\mathfrak{A}, \beta \models \varphi$
2. benötigt Zeit $|\mathfrak{A}|^{\mathcal{O}(|\varphi|)}$.

Beweis: 1. Per Induktion über den Aufbau von φ (Übung)

Für 2.:

Die Schachtelungstiefe st(φ) einer Formel φ ist induktiv definiert wie folgt:

- $\mathrm{st}(t = t') \;=\; \mathrm{st}(P(t_1, \ldots, t_k)) \;=\; 0$
- $\mathrm{st}(\neg\varphi) \;=\; \mathrm{st}(\exists x\, \varphi) \;=\; \mathrm{st}(\forall x\, \varphi) \;=\; \mathrm{st}(\varphi) + 1$
- $\mathrm{st}(\varphi \wedge \psi) \;=\; \mathrm{st}(\varphi \vee \psi) \;=\; \max\{\mathrm{st}(\varphi), \mathrm{st}(\psi)\} + 1$

Leicht per Induktion zu zeigen: $\mathrm{st}(\varphi) \leq |\varphi|$ ($|\varphi|$ ist Größe von φ)

Auswertung

Lemma 2.14

Der Algorithmus `ausw`

1. ist korrekt: $\texttt{ausw}(\mathfrak{A}, \beta, \varphi) = 1$ gdw. $\mathfrak{A}, \beta \models \varphi$
2. benötigt Zeit $|\mathfrak{A}|^{\mathcal{O}(|\varphi|)}$.

Beweis: 1. Einfache Induktion über den Aufbau von φ

2. Tiefe Rekursionsbaum beschränkt durch $\mathsf{st}(\varphi)$

Verzweigung Rekursionsbaum beschränkt durch $\max\{|A|, 2\}$

Anzahl Knoten also $\leq |A|^{|\varphi|+1} - 1$

Prüfen ob ein Tupel in $P^{\mathfrak{A}}$ ist

Jeder einzelne Aufruf braucht Zeit $\leq \mathcal{O}(|\mathfrak{A}|) + \mathcal{O}(|\varphi|^2)$

Berechnen von $\beta(t)$

Eine einfache Rechnung zeigt:
insgesamt ist der Zeitaufwand durch $|\mathfrak{A}|^{\mathcal{O}(|\varphi|)}$ beschränkt.

Reflexion

Theorem 2.13

Das Auswertungsproblem der Prädikatenlogik erster Stufe ist entscheidbar in Zeit $|\mathfrak{A}|^{\mathcal{O}(|\varphi|)}$.

Etwas genauer hingeschaut: die Laufzeit ist

- exponentiell in $|\varphi|$ ($|\mathfrak{A}|$ „festhalten“ liefert Funktion $c^{\mathcal{O}(|\varphi|)}$)
- aber nur polynomiell in $|\mathfrak{A}|$ ($|\varphi|$ „festhalten“ liefert Funktion $|\mathfrak{A}|^c$)

Das sind gute Nachrichten, denn

- $|\varphi|$ ist oft klein (z.B. Anfrage, zu verifizierende Eigenschaft)
- $|\mathfrak{A}|$ ist oft groß (z.B. Datenbank, zu verifizierendes System)

Wir werden später darauf zurückkommen

FO und Datenbanken

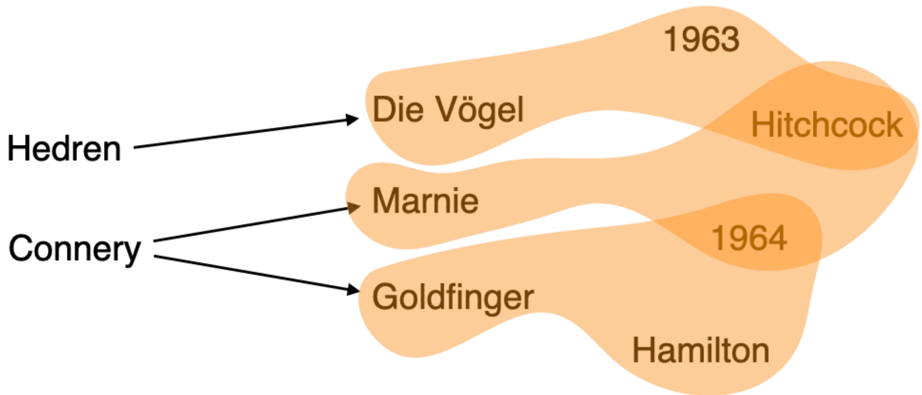
Schon gesehen: Datenbankinstanz $\approx$ endliche relationale Struktur

Film:

Titel	Jahr	Regisseur
Die Vögel	1963	Hitchcock
Marnie	1964	Hitchcock
Goldfinger	1964	Hamilton

Schauspieler:

Name	Filmtitel
Connery	Marnie
Connery	Goldfinger
Hedren	Die Vögel



Dazu passend kann man FO-Formel φ als Datenbankanfrage auffassen

Antworten auf $\varphi(x_1, \ldots, x_n)$ bzgl. Struktur (= Datenbankinstanz) $\mathfrak{A}$:

$$\text{ans}(\mathfrak{A}, \varphi) = \{(a_1, \ldots, a_n) \in A^n \mid \mathfrak{A} \models \varphi[a_1, \ldots, a_n]\}$$

FO und Datenbanken

Film:

Titel	Jahr	Regisseur
Die Vögel	1963	Hitchcock
Marnie	1964	Hitchcock
Goldfinger	1964	Hamilton

Schauspieler:

Name	Filmtitel
Connery	Marnie
Connery	Goldfinger
Hedren	Die Vögel

$$\varphi(x) = \exists y\, \mathsf{Film}(\underline{x}, y, \mathsf{Hitchcock})$$

„Titel aller Hitchcock-Filme“

$$\mathsf{ans}(\mathfrak{A}, \varphi) = \{\mathsf{Die\ Vögel}, \mathsf{Marnie}\}$$

Für Spitzfindige:

Wir verwenden ein Element des Universums als Konstante: Hitchcock

Das ist im allgemeinen nicht zulässig

Im Zshg von “FO als Anfragesprache” nimmt man aber stets an, dass alle Elemente auch Konstanten sind und für alle Konstanten c gilt: $c^{\mathfrak{A}} = c$.

FO und Datenbanken

Film:

Titel	Jahr	Regisseur
Die Vögel	1963	Hitchcock
Marnie	1964	Hitchcock
Goldfinger	1964	Hamilton

Schauspieler:

Name	Filmtitel
Connery	Marnie
Connery	Goldfinger
Hedren	Die Vögel

$$\varphi(x) = \exists y\, \text{Film}(\underline{x}, y, \text{Hitchcock})$$

„Titel aller Hitchcock-Filme“

$$\text{ans}(\mathfrak{A}, \varphi) = \{\text{Die Vögel}, \text{Marnie}\}$$

$$\varphi(x) = \exists y \Big(\text{Film}(\underline{x}, y, \text{Hitchcock}) \ \wedge \ \text{Schauspieler}(\text{Connery}, \underline{x})\Big)$$

$$\text{ans}(\mathfrak{A}, \varphi) = \{\text{Marnie}\}$$

„Titel aller Hitchcock-Filme, in denen Connery mitspielt“

$$\varphi(x, y) = \exists z \exists z' \Big(\text{Schauspieler}(\underline{x}, z) \wedge \text{Film}(z, \underline{y}, z')\Big)$$

$$\text{ans}(\mathfrak{A}, \varphi) = \{(\text{Connery}, 1964), (\text{Hedren}, 1963)\}$$

„Schauspieler mit Jahren, in denen sie gespielt haben“

FO und Datenbanken

Diese Anfragen lassen sich auch in SQL ausdrücken, z.B.:

Beispiele:

„Titel aller Hitchcock-Filme" $\varphi(x) = \exists y \, \mathsf{Film}(\underline{x}, y, \mathsf{Hitchcock})$

```
SELECT Titel FROM Film WHERE Regisseur = Hitchcock
```

„Schauspieler mit Jahren, in denen sie gespielt haben"

$$\varphi(x, y) = \exists z \exists z' \left(\mathsf{Schauspieler}(\underline{x}, z) \wedge \mathsf{Film}(z, \underline{y}, z')\right)$$

```
SELECT Jahr,Name FROM Film, Schauspieler
                WHERE Film.Titel = Schauspieler.Filmtitel
```

FO und Datenbanken

FO als Anfragesprache ist im Wesentlichen dasselbe wie SQL!

Theorem 2.15 (Codd's Theorem 1970)

Jede FO-Anfrage ist äquivalent zu einer SQL-Anfrage und umgekehrt.

Das ist so nicht ganz präzise:

- nur sogenannte domänenunabhängige FO-Formeln sind äquivalent zu SQL-Anfragen (eine unwesentliche Einschränkung)
- Es bezieht sich auf das ursprüngliche SQL 1.0 - mittlerweile wurde SQL stark erweitert und geht teilweise über FO hinaus.

Codd entwickelte bei IBM die Grundlagen für SQL-Datenbanken und implementierte die erste SQL-Datenbank „System R“ - Turingaward 1981

Das obige Resultat ist kein Zufall sondern “by design” (of SQL)

Äquivalenz

Definition 2.16 (Äquivalenz)

Zwei FO-Formeln φ und ψ mit $\mathsf{Frei}(\varphi) = \mathsf{Frei}(\psi)$ sind äquivalent, wenn für alle Interpretationen $(\mathfrak{A}, \beta)$ gilt: $\mathfrak{A}, \beta \models \varphi$ gdw. $\mathfrak{A}, \beta \models \psi$.
Wir schreiben dann: $\varphi \equiv \psi$

Der Begriff einer Teilformel einer FO-Formel kann auf die offensichtliche Weise induktiv definiert werden, analog zur Aussagenlogik.

Auch in FO sind äquivalente Formeln austauschbar:

Lemma 2.17 (Ersetzungslemma)

Seien φ und ψ äquivalente FO-Formeln, ϑ eine Formel mit $\varphi \in \mathsf{TF}(\vartheta)$ und ϑ' eine Formel, die sich aus ϑ ergibt, indem ein beliebiges Vorkommen von φ durch ψ ersetzt wird. Dann gilt $\vartheta \equiv \vartheta'$.

Beweis per Induktion über die Struktur von ϑ.

Äquivalenz

Alle Äquivalenzen aus der Aussagenlogik gelten auch in FO, z. B.:

$$\varphi \land \psi \equiv \neg(\neg\varphi \lor \neg\psi) \qquad \text{für beliebige FO-Formeln } \varphi, \psi$$

Natürlich gibt es auch interessante FO-spezifische Äquivalenzen, z. B.:

- $\forall x\, \varphi \equiv \neg\exists x\, \neg\varphi$ (Dualität von $\exists$ und $\forall$)
- $\exists x\, (\varphi \lor \psi) \equiv \exists x\, \varphi \lor \exists x\, \psi$ ($\exists$ distribuiert über $\lor$)
- $\forall x\, (\varphi \land \psi) \equiv \forall x\, \varphi \land \forall x\, \psi$ ($\forall$ distribuiert über $\land$)
- $\exists x\, \exists y\, \varphi \equiv \exists y\, \exists x\, \varphi$
- $\forall x\, \forall y\, \varphi \equiv \forall y\, \forall x\, \varphi$

Beweisen kann man diese Äquivalenzen durch Verwendung der Semantik

Reduzierte Formeln

Eine FO-Formel heißt reduziert wenn sie nur $\neg, \wedge$ und $\exists$ verwendet, aber nicht $\vee$ und $\forall$

Lemma 2.18

Jede FO-Formel kann in Linearzeit in eine äquivalente reduzierte FO-Formel gewandelt werden.

Beweis: Erschöpfendes Anwenden der Äquivalenzen

$$\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$$

$$\forall x\, \varphi \equiv \neg\exists x\, \neg\varphi$$

❑

Daraus folgt:

In Induktionsbeweisen genügt es meist, nur $\neg, \wedge, \exists$ zu betrachten.

Erfüllbarkeit, Gültigkeit, Konsequenz

Folgende Begriffe sind exakt analog zur Aussagenlogik:

Definition 2.19 (Erfüllbarkeit, Gültigkeit, Konsequenz)

Ein Satz φ heißt

- erfüllbar, wenn er ein Modell hat (Struktur, die ihn wahr macht)
- gültig oder Tautologie, wenn jede Struktur ein Modell von φ ist
- Konsequenz von Satz ψ, wenn für alle Strukturen $\mathfrak{A}$ mit $\mathfrak{A} \models \psi$ auch $\mathfrak{A} \models \varphi$ gilt (wir schreiben dann $\psi \models \varphi$)

Man kann diese Begriffe auch für Formeln mit freien Variablen definieren; verwendet dann Interpretationen statt Strukturen.

Erfüllbarkeit, Gültigkeit, Konsequenz

Folgender Satz ist gültig:

$$\big(\, \forall x \exists y\, R(x,y) \land \qquad \text{„}R\text{ ist total“}$$

$$\forall x \forall y\, (R(x,y) \to R(y,x)) \land \qquad \text{„}R\text{ ist symmetrisch“}$$

$$\forall x \forall y \forall z\, (R(x,y) \land R(y,z) \to R(x,z))\, \big) \qquad \text{„}R\text{ ist transitiv“}$$

$$\to \forall x\; R(x,x) \qquad \text{„}R\text{ ist reflexiv“}$$

Folgende Sätze sind ebenfalls gültig:

$$\forall x \exists y\, (y = f(x)) \qquad \forall x (f(x) = x \to f(f(x)) = x)$$

Weitere gültige Sätze liefern die gezeigten Äquivalenzen, z.B.:

$$\exists x\, P(x) \leftrightarrow \neg \forall x\, \neg P(x)$$

Erfüllbarkeit, Gültigkeit, Konsequenz

Beachte: Gültigkeit bezieht sich stets auf alle (wirklich ALLE) Strukturen

Folgender Satz in Signatur $\tau = \{+, \cdot, 0, 1\}$ ist z.B. nicht gültig:

$$\varphi = \forall x \, (x \cdot x = x \rightarrow (x = 0 \vee x = 1))$$

Ist wahr in der einen Stuktur $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$, die unsere Intuition bestimmt

Modifizieren wir $\mathfrak{N}$ durch Setzen von $\cdot^{\mathfrak{N}}(2, 2) = 2$ so ist das resultierende $\mathfrak{N}'$ ebenfalls eine (seltsame) τ-Stuktur! Darin ist φ aber falsch!

Folgender Satz ist erfüllbar, aber nur in unendlichen Modellen:

$\forall x \exists y \, P(x, y) \;\wedge$	„*P* ist total“
$\forall x \forall y \forall z \, (P(x, y) \wedge P(y, z) \rightarrow P(x, z)) \;\wedge$	„*P* ist transitiv“
$\neg \exists x P(x, x)$	„*P* ist irreflexiv“

T2.6

Pränex-Normalform

Definition 2.20 (Pränex-Normalform)

Eine FO-Formel φ ist in Pränex-Normalform (PNF), wenn sie die Form

$$Q_1 x_1 \cdots Q_n x_n \, \varphi$$

hat und bereinigt ist, wobei $Q_i \in \{\exists, \forall\}$ und φ quantorenfrei ist.

FO-Formel φ ist bereinigt, wenn

- keine Variable in φ sowohl frei als auch gebunden auftritt
- keine Variable mehr als einmal quantifiziert wird

Jede Formel kann leicht durch Umbenennung quantifizierter Variablen bereinigt werden, z. B.:

$$\exists y \, (P(\underline{x}, y) \wedge \forall x \, Q(x, y)) \quad \text{äquivalent zu} \quad \exists y \, (P(\underline{x}, y) \wedge \forall z \, Q(z, y))$$

Pränex-Normalform

Theorem 2.21

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

Die Umwandlung ist in Linearzeit möglich.

Für den Beweis benötigen wir folgende Äquivalenzen:

Falls x nicht frei in φ vorkommt, gilt:

$$\varphi \lor \exists x\, \psi \equiv \exists x\, (\varphi \lor \psi)$$

$$\varphi \land \exists x\, \psi \equiv \exists x\, (\varphi \land \psi)$$

$$\varphi \lor \forall x\, \psi \equiv \forall x\, (\varphi \lor \psi)$$

$$\varphi \land \forall x\, \psi \equiv \forall x\, (\varphi \land \psi)$$

T2.7

Pränex-Normalform

Theorem 2.21

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

Die Umwandlung ist in Linearzeit möglich.

Beweis von Theorem 2.21 per Induktion über die Struktur von φ:

(1) Wenn φ quantorenfrei, dann φ in PNF nach Bereinigung (Induktionsanfang)

(2) Sei $\varphi = \neg\psi$.

IV auf ψ liefert PNF-Formel $\psi' = Q_1 x_1 \cdots Q_n x_n \vartheta$ mit $\psi \equiv \psi'$

Also $\varphi \equiv \neg Q_1 x_1 \cdots Q_n x_n \vartheta$ und es genügt, letzteres in PNF zu wandeln

Dualität von $\exists$ und $\forall$ liefert

$$\varphi \equiv \overline{Q}_1 x_1 \cdots \overline{Q}_n x_n \neg\vartheta$$

wobei $\overline{\exists} = \forall$ und $\overline{\forall} = \exists$

in PNF

Pränex-Normalform

(3) Sei $\varphi = \psi_1 \circ \psi_2$ mit $\circ \in \{\wedge, \vee\}$

IV liefert PNF-Formeln ψ'_1, ψ'_2 mit $\psi_1 \equiv \psi'_1$ und $\psi_2 \equiv \psi'_2$

Also ist φ äquivalent zu $\psi'_1 \circ \psi'_2$

Durch Variablenumbenennung erreichen wir, dass

$$\psi'_1 = Q_1 x_1 \cdots Q_n x_n \, \vartheta_1$$

$$\psi'_2 = Q'_1 y_1 \cdots Q'_m y_m \, \vartheta_2$$

wobei $x_1, \ldots, x_n$ nicht in ψ'_2 vorkommen und $y_1, \ldots, y_m$ nicht in ψ'_1,

weder frei noch gebunden

$n + m$-maliges Anwenden der Äquivalenzen auf $\psi'_1 \circ \psi'_2$ liefert

$$Q_1 x_1 \cdots Q_n x_n Q'_1 y_1 \cdots Q'_m y_m \, (\vartheta_1 \circ \vartheta_2) \quad \text{in PNF}$$

(nur möglich weil $x_1, \ldots, x_n$ nicht in ψ'_2 und $y_1, \ldots, y_m$ nicht in ψ'_1)

Pränex-Normalform

(4) Sei $\varphi = Qx\, \psi$ mit $Q \in \{\exists, \forall\}$

IV liefert PNF-Formel $\psi' = Q_1 x_1 \cdots Q_n x_n\, \vartheta$ mit $\psi \equiv \psi'$.

Durch Umbenennen eines x_i erreichen wir $x \notin \{x_1, \ldots, x_n\}$

Dann ist $Qx\, \psi'$ äquivalent zu φ und in PNF ❏

(das Umbenennen dient nur der Bereinigung)

Beispiel: **T2.8**

Skolem-Normalform

Definition 2.22 (Skolem-Normalform)

Eine FO-Formel φ ist in Skolem-Normalform, wenn sie in PNF ist und ausschließlich universelle Quantoren enthält.

Theorem 2.23

Jede FO-Formel kann in Linearzeit in eine erfüllbarkeitsäquivalente Formel in Skolem Normalform gewandelt werden.

Das Wandeln führt zusätzliche Funktionssymbole ein, darum ist die resultierende Formel nicht äquivalent

T2.9

Skolem-Normalform

Beweis:

Wandle erschöpfend

$$\forall x_1 \cdots \forall x_{i-1} \exists x_i \, Q_{i+1} x_{i+1} \cdots Q_k \, x_k \, \psi$$

in $\forall x_1 \cdots \forall x_{i-1} \, Q_{i+1} x_{i+1} \cdots Q_k x_k \, \psi'$

wobei man ψ' aus ψ durch Ersetzen von x_i durch $f_i(x_1, \ldots, x_{i-1})$ erhält,

f_i frisches $i-1$-stelliges Funktionssymbol (“Skolemisierung”)

Beispiel:

$$\forall x_1 \exists x_2 \forall x_3 \exists x_4 \left(R(x_1, x_3) \to P(x_2) \wedge Q(x_4)\right)$$

$$\forall x_1 \forall x_3 \exists x_4 \left(R(x_1, x_3) \to P(f_2(x_1)) \wedge Q(x_4)\right)$$

$$\forall x_1 \forall x_3 \left(R(x_1, x_3) \to P(f_2(x_1)) \wedge Q(f_4(x_1, x_3))\right)$$

Es genügt, zu zeigen: jeder einzelne Schritt ist erfüllbarkeitserhaltend

Skolem-Normalform

Wandle erschöpfend

$$\varphi = \forall x_1 \cdots \forall x_{i-1}\, \exists x_i\, \psi$$

in $\varphi' = \forall x_1 \cdots \forall x_{i-1}\, \psi'$

wobei man ψ' aus ψ durch Ersetzen von x_i durch $f_i(x_1, \ldots, x_{i-1})$ erhält,

„⇒“: Sei φ erfüllbar und $\mathfrak{A}$ Struktur mit $\mathfrak{A} \models \varphi$.

Semantik ∀ / ∃: dann gilt für alle Zuweisungen β für $x_1, \ldots, x_{i-1}$:

es gibt $a_\beta \in A$: $\mathfrak{A}, \beta[x_i/a_\beta] \models \psi$

Sei $\mathfrak{A}'$ wie $\mathfrak{A}$ außer dass $f_i^{\mathfrak{A}'}(\beta(x_1), \ldots, \beta(x_{i-1})) = a_\beta$ für alle β

Das Funktionssymbol „verhält“ sich also wie der Existenzquantor

quasi dieselbe Aussage

Nun gilt für alle Zuweisungen β für $x_1, \ldots, x_{i-1}$: $\mathfrak{A}', \beta \models \psi'$

Also per Semantik $\mathfrak{A}' \models \forall x_1 \cdots \forall x_{i-1}\, \psi'$, also φ' erfüllbar

Skolem-Normalform

Wandle erschöpfend

$$\varphi = \forall x_1 \cdots \forall x_{i-1} \exists x_i \, \psi$$

in $\varphi' = \forall x_1 \cdots \forall x_{i-1} \, \psi'$

wobei man ψ' aus ψ durch Ersetzen von x_i durch $f_i(x_1, \ldots, x_{i-1})$ erhält,

„$\Leftarrow$“: Sei φ' erfüllbar und $\mathfrak{A}$ Struktur mit $\mathfrak{A} \models \psi'$.

Semantik $\forall$: dann gilt für alle Zuweisungen β für $x_1, \ldots, x_{i-1}$: $\mathfrak{A}, \beta \models \psi'$

Es gilt $\mathfrak{A}, \beta[x_i / f_i^{\mathfrak{A}}(\beta(x_1), \ldots, \beta(x_{i-1}))] \models \psi$

quasi
dieselbe
Aussage

Also per Semantik $\mathfrak{A} \models \exists x_i \psi$

Und damit („alle Zuweisungen“) auch $\mathfrak{A} \models \varphi$, also ist φ erfüllbar ❏

Klauseln in FO

Satz in Skolem Normalform: $\forall x_1 \cdots \forall x_n \, \psi$ mit ψ quantorenfrei

Solche Formeln kann man als Klauselmenge sehen:

- Quantoren nur implizit (jede Variable universell quantifiziert)
- ψ in KNF bringen (Atome $t = t'$ und $P(t_1, \dots, t_n)$ statt Variablen)
- KNF wie in AL als Klauselmenge betrachten

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 \, (\, P(x_1, c) \vee Q(f(x_1), x_2) \,) \wedge (\, \neg P(x_1, c) \vee R(x_3, g(x_4)) \,)$$

wird beispielsweise

$$\{ \, P(x_1, c), \; Q(f(x_1), x_2) \, \}, \; \{ \, \neg P(x_1, c), \; R(x_3, g(x_4)) \, \}$$

Dies ist der Startpunkt für Resolution in FO

Resolventenbildung ist dann ähnlich definiert wie in AL, allerdings mit einer wesentlichen Erweiterung (Unifikation von Termen) - siehe z.B. Schöning

Prädikatenlogik

2.1 Strukturen

2.2 Syntax und Semantik der Prädikatenlogik

2.3 Auswertungsproblem

2.4 Äquivalenz, Erfüllbarkeit, Gültigkeit

2.5 Pränex-Normalform und Skolemform

Next

2.6 Unentscheidbarkeit

2.7 Theorien

Erfüllbarkeits / Gültigkeitsproblem

Wir interessieren uns nun für Algorithmen und die Komplexität des Erfüllbarkeit- / Gültigkeitsproblems in FO

Situation bzgl. Algorithmen im Überblick:

	AL	FO
Auswertung	In Linearzeit	In Zeit $\lvert\mathfrak{A}\rvert^{O(\lvert\varphi\rvert)}$ *
Erfüllbarkeit/ Tautologie	In Zeit 2^n *	? ? ?

* und vermutlich nicht in polynomieller Zeit möglich

Unentscheidbarkeit

Bis in die 1930er hofften viele Mathematiker, dass ein Algorithmus für Gültigkeit in der Prädikatenlogik und ähnlich starken Logiken existiert

Man sagt dann: das Problem ist entscheidbar

Besonders prominent ist Hilbert (1928):
Lösung des Entscheidungsproblems der Logik eines der wichtigsten offenen Probleme der Mathematik (Mathematikerkongress 1900)

Die Idee war:
viele manuelle mathematische Beweise wären durch automatische ersetzbar.

Oder gar alles (philosophische) Schließen und Argumentieren (Gottfried Wilhelm Leibniz: “Calculemus!” - 17. Jh)

Unentscheidbarkeit

Aber das wäre dann doch zu schön, um wahr zu sein …

Theorem 2.24 (Church 1936)

In FO sind Gültigkeit und Erfüllbarkeit unentscheidbar.

Das bedeutet:

es existiert kein Algorithmus, der diese Probleme löst (gar keiner, auch kein ineffizienter Algorithmus)

Mehr zum Thema Unentscheidbarkeit in VL „Berechenbarkeit“

Zur Erinnerung:

- Satz φ ist erfüllbar gdw. $\neg\varphi$ nicht gültig
- Satz φ ist gültig gdw. $\neg\varphi$ nicht erfüllbar

Es können also nur beide Probleme entscheidbar sein oder beide unentscheidbar.

Lesetipp


LOGICOMIX
EINE EPISCHE SUCHE NACH WAHRHEIT
APOSTOLOS DOXIADIS UND CHRISTOS H. PAPADIMITRIOU
GRAFIK VON ALECOS PAPADATOS UND ANNIE DI DONNA
ÜBERSETZT VON EBI NAUMANN
ATRIUM

Endliche Modelle

Ein Unterschied zwischen Aussagenlogik und Prädikatenlogik:

- In AL gibt es nur endlich viele Belegungen für jede Formel
- In FO gibt es nur unendlich viele Strukturen für jede Formel

  (und die dürfen sogar unendlich groß sein)

Vielleicht hilft es, nur endlich große Strukturen zuzulassen?

Für die Informatik sind die ohnehin viel relevanter (z.B. Datenbanken)!

Zur Erinnerung: Satz

$$\begin{aligned}\varphi = {} & \forall x \exists y\, P(x,y) \ \wedge \\ & \forall x \forall y \forall z\, (P(x,y) \wedge P(y,z) \rightarrow P(x,z)) \ \wedge \\ & \neg \exists x P(x,x)\end{aligned}$$

ist erfüllbar, aber nicht endlich erfüllbar

Unentscheidbarkeit bzgl. endlicher Modelle

Leider ändert auch das nichts an der Unentscheidbarkeit

Theorem 2.25 (Trakhtenbrot 1950)

Folgende Probleme sind unentscheidbar:

- Endliche Gültigkeit:
  Ist ein FO-Satz in allen endlichen Interpretationen erfüllt?
- Endliche Erfüllbarkeit:
  Hat ein FO-Satz ein endliches Modell?

Erfüllbarkeit und Gültigkeit sind also sehr schwierige Probleme,

in endlichen wie in unendlichen Strukturen

Theorien

Zur Erinnerung: der FO-Satz

$$\forall x\,(x \cdot x = x \rightarrow (x = 0 \vee x = 1))$$

ist nicht gültig, weil wir ihn per Definition in allen τ-Strukturen interpretieren, für die Signatur $\tau = \{+, \cdot, 0, 1\}$.

Manche Strukturen haben eine besondere Bedeutung, z. B.:

Arithmetik der natürlichen Zahlen $(\mathbb{N}, +, \cdot, 0, 1)$

Die in dieser Struktur erfüllten FO-Sätze sind mathematisch von großer Bedeutung.

Zum Beispiel Goldbachsche Vermutung

$$\varphi_{\mathsf{G}} = \forall x \Big(x > 2 \wedge \mathsf{Even}(x) \;\rightarrow\; \exists y \exists y' \Big(\mathsf{Prim}(y) \wedge \mathsf{Prim}(y') \wedge x = y + y' \Big)\Big)$$

wobei $\mathsf{Even}(x) \;=\; \exists y\,(x = y + y)$ etc.

FO-Theorien

Eine Theorie ist eine „kohärente“ Menge Γ von FO-Sätzen, die von besonderem Interesse ist.

Eine wichtige Art, Theorien zu definieren:
die Menge Γ aller Sätze, die in (interessanter) Struktur $\mathfrak{A}$ wahr sind

Z.B. $\mathfrak{A} = (\mathbb{N}, +, \cdot, 0, 1)$:
φ_{G} ist in Theorie dieser Struktur gdw. Goldbachsche Vermutung wahr!

Interessante Strukturen $\mathfrak{A}$ sind meist unendlich
Algorithmus für das Auswertungsproblem also nicht verwendbar.

In der Tat sind viele interessante Theorien Γ ebenfalls unentscheidbar
Also die Frage: gegeben Satz φ, ist $\varphi \in \Gamma$?

FO-Theorien

Grundbegriffe für Formelmengen Γ (endlich oder unendlich):

- Struktur $\mathfrak{A}$ ist Modell für Γ ($\mathfrak{A} \models \Gamma$), wenn $\mathfrak{A} \models \varphi$ für alle $\varphi \in \Gamma$.
- Γ ist erfüllbar, wenn Γ ein Modell hat.
- FO-Satz ψ folgt aus Γ ($\Gamma \models \psi$), wenn für alle $\mathfrak{A} \models \Gamma$ auch $\mathfrak{A} \models \psi$ gilt.

Für die folgende Definition nehmen wir (implizit) eine feste Signatur τ an, über der alle Formeln gebildet werden.

Definition 2.26 (FO-Theorie)

Eine FO-Theorie ist eine Menge Γ von FO-Sätzen, die erfüllbar und unter Konsequenz abgeschlossen ist:

$$\Gamma \models \varphi \quad \text{impliziert} \quad \varphi \in \Gamma \qquad \text{für alle Sätze } \varphi$$

Γ heißt vollständig, wenn für alle Sätze φ gilt: $\varphi \in \Gamma$ oder $\neg\varphi \in \Gamma$

Beispiele für FO-Theorien

1. Menge aller Tautologien $\text{Taut}(\tau)$ (in einer fixen Signatur τ) ist FO-Theorie; enthalten in allen anderen Theorien, nicht vollständig

2. Sei $\mathfrak{A}$ eine τ-Struktur. Dann ist

$$\text{Th}(\mathfrak{A}) = \{\varphi \text{ ist } \tau\text{-Satz} \mid \mathfrak{A} \models \varphi\}$$

   eine vollständige FO-Theorie.

3. Wenn Γ erfüllbare Menge von FO-Sätzen, dann ist

$$\text{Abschluss}(\Gamma) = \{\varphi \text{ ist } \tau\text{-Satz} \mid \Gamma \models \varphi\}$$

   FO-Theorie (im Allgemeinen nicht vollständig)

4. Sei $\mathcal{K}$ eine nicht-leere Klasse von τ-Strukturen. Dann ist

$$\text{Th}(\mathcal{K}) = \bigcap_{\mathfrak{A} \in \mathcal{K}} \text{Th}(\mathfrak{A})$$

   eine FO-Theorie (im Allgemeinen nicht vollständig).

T2.10

Zu Vollständigen Theorien

Interessanterweise hängt der Begriff der Vollständigkeit sehr eng mit der Definition von Theorien durch Strukturen zusammen.

Lemma 2.27

Sei Γ eine FO-Theorie. Dann sind die folgenden Aussagen äquivalent:

1. Γ ist vollständig
2. $\Gamma = \mathsf{Th}(\mathfrak{A})$ für eine Struktur $\mathfrak{A}$.

Da „2 $\Rightarrow$ 1“ offensichtlich ist, zeigen wir nur „1 $\Rightarrow$ 2“

T2.11

Aus dem Beweis folgt: Alle Modelle einer vollständigen Theorie Γ erfüllen dieselben Formeln (nämlich die aus Γ)

Sie sind jedoch nicht unbedingt isomorph, z.B.: $\mathsf{Th}(\mathbb{Q}, <)$ hat Modell $(\mathbb{R}, <)$

Einige wichtige FO-Theorien

Arithmetik der natürlichen Zahlen: $\mathsf{Th}(\mathbb{N}, +, \cdot, 0, 1)$

Unentscheidbar
(das ist Gödels berühmter 1. Unvollständigkeitssatz)

Presburger-Arithmetik: $\mathsf{Th}(\mathbb{N}, +, 0, 1)$

z.B. $\forall x\,((x + x = x) \to x = 0)$

Entscheidbar

Zu schwach, um wirklich interessante mathematische Probleme auszudrücken, aber wichtige Anwendungen in der Informatik!

Skolem-Arithmetik: $\mathsf{Th}(\mathbb{N}, \cdot, 0, 1)$

Entscheidbar

Einige wichtige FO-Theorien

Arithmetik der reellen Zahlen: Th$(\mathbb{R}, +, \cdot, 0, 1)$

z. B. $\forall x \forall y \forall z \Big(\big(\underbrace{x = y \cdot y}_{y = \sqrt{x}} \;\wedge\; \underbrace{x = z \cdot z}_{z = \sqrt{x}} \big) \;\rightarrow\; \big(y = z \;\vee\; \underbrace{y = z - (2 \cdot z)}_{y = -z} \big) \Big)$

Entscheidbar

Man vergrößert hier also den Zahlenbereich und bekommt dadurch bessere Berechnungseigenschaften.

Aus der Unentscheidbarkeit von Th$(\mathbb{N}, +, \cdot, 0, 1)$ folgt aber, dass man keine FO-Formel $\varphi(x)$ finden kann, die $\mathbb{N}$ in $(\mathbb{R}, +, \cdot, 0, 1)$ definiert, also so dass gilt: $(\mathbb{R}, +, \cdot, 0, 1) \models \varphi[a]$ gdw. $a \in \mathbb{N}$.

(und auch Goldbach's Vermutung etc sind deshalb nicht ausdrückbar)

Axiomatisierung

Die Definition einer Theorie über eine Struktur verrät nicht viel über die enthaltenen Sätze:

Welche Sätze enthält Th$(\mathbb{Q}, <)$?

Die Definition über Abschluss(Π) ist viel aufschlussreicher, z.B.

$$\Pi = \{\ \forall x\, \neg(x < x),\quad \forall x \forall y\, (x < y \ \rightarrow\ \neg(y < x)),\quad \forall x \forall y \forall z\, (x < y\ \wedge\ y < z\ \rightarrow\ x < z),$$

strikte partielle Ordnung

$$\forall x \forall y\, (x < y\ \vee\ y < x\ \vee\ x = y),$$

total

$$\forall x \exists y\, (x < y), \quad \forall x \exists y\, (y < x),$$

beidseitig unbeschränkt

$$\forall x \forall y\, (x < y\ \rightarrow\ \exists z\, (x < z < y))\ \}$$

dicht

Ohne Beweis: Es gilt Th$(\mathbb{Q}, <) =$ Abschluss(Π) !

Axiomatisierung

Definition 2.28 (Axiomatisierung)

Sei Γ FO-Theorie. Eine Menge Π von Sätzen heißt Axiomatisierung von Γ wenn $\Gamma = \mathsf{Abschluss}(\Pi)$, also

$$\Gamma = \{\varphi \text{ ist } \tau\text{-Satz} \mid \Pi \models \varphi\}.$$

Eine Axiomatisierung liefert einem gewissermaßen “alles, was man über die Theorie wissen muss”.

Hauptsächlich interessiert man sich für endliche Axiomatisierungen wie im Fall von $\mathsf{Th}(\mathbb{Q}, <)$.

Unendliche Axiomatisierungen können ebenfalls aufschlussreich sein, das ist aber nicht in jedem Fall so.

Die Axiomatisierung $\Pi = \Gamma$ ist beispielsweise uninteressant

Axiomatisierung

Es gibt einen Zusammenhang zwischen endlicher Axiomatisierbarkeit und Entscheidbarkeit:

Theorem 2.29

Jede vollständige Theorie Γ, die endlich axiomatisierbar ist, ist entscheidbar.

Unentscheidbare (vollständige) Theorien wie $\mathsf{Th}(\mathbb{N}, +, \cdot, 0, 1)$ sind also nicht endlich axiomatisierbar.

Die entscheidbaren Theorien $\mathsf{Th}(\mathbb{N}, +, 0, 1)$ und $\mathsf{Th}(\mathbb{R}, +, \cdot, 0, 1)$ ebenfalls nicht, haben aber “aufschlussreiche” unendliche Axiomatisierungen

Axiomatisierung

Es gibt einen Zusammenhang zwischen endlicher Axiomatisierbarkeit und Entscheidbarkeit:

Theorem 2.29

Jede vollständige Theorie Γ, die endlich axiomatisierbar ist, ist entscheidbar.

Beweis:

Im folgenden Abschnitt der VL werden wir sehen, dass es einen Aufzählalgorithmus der folgenden Art gibt:

Eingabe: endliche Menge von FO-Sätzen Π

Ausgabe: alle FO-Sätze φ mit $\Pi \models \varphi$, einer nach dem anderen

(unendlich viele, ohne Terminierung)

Axiomatisierung

Es gibt einen Zusammenhang zwischen endlicher Axiomatisierbarkeit und Entscheidbarkeit:

Theorem 2.29

Jede vollständige Theorie Γ, die endlich axiomatisierbar ist, ist entscheidbar.

Beweis:

Sei nun $\Gamma = \text{Abschluss}(\Pi)$ eine vollständige Theorie, Π endlich.

Gegeben φ entscheiden wir ob $\varphi \in \Gamma$ mit folgendem Algorithmus:

- starte den erwähnten Aufzählalgorithmus auf Π
- erzeugt werden genau die Sätze in Γ
- da Γ vollständig ist, wird früher oder später φ oder $\neg\varphi$ erzeugt
- antworte entsprechend “ja” oder “nein”