Notizen zur Logik erster Stufe

Inhaltsverzeichnis

Notizen zur Logik erster Stufe

Formeln der Logik erster Stufe, FO (englisch: first-order logic), sprechen über Strukturen: Bereiche von Elementen über denen vorgegebene Funktionen und Relationen (Prädikate) interpretiert sind. Einer Formel wird ein Wahrheitswert an einer Stelle (an einem Tupel von Elementen) in einer solchen Struktur zugewiesen. Der einfachste Fall ist das Zutreffen oder Nichtzutreffen einer Relationsbeziehung (eines Prädikats) auf ein Tupel – daher auch Prädikatenlogik.

Interessant wird die Logik erster Stufe durch die Möglichkeit über Elemente zu quantifizieren (Allaussagen und Existenzaussagen zu treffen).

Kontext: Strukturen und FO-Formeln bieten ein universelles Format für die Modellierung mathematischer und informatischer Gegenstandsbereiche. Die Verwendungen von Syntax und Semantik von FO reichen von den Grundlagen der Mathematik bis zu Abfragesprachen für relationale Datenbanken.

Wegen der komplexeren Ausdrucksmöglichkeiten sind die Definition der Semantik und die Auswertung von Formeln, und erst recht Erfüllbarkeit und Allgemeingültigkeit, nicht-trivial.

Im allgemeinen sind Erfüllbarkeit und Allgemeingültigkeit von FO unentscheidbar.

Auch für die Logik erster Stufe gibt es aber noch korrekte und vollständige Beweiskalküle. Wir behandeln wiederum zwei derartige Kalküle unterschiedlichen Charakters: Resolution (Widerlegungskalkül, Unerfüllbarkeitsbeweise) und einen Sequenzenkalkül (Deduktionskalkül, Allgemeingültigkeitsbeweise).

1 Strukturen und Belegungen

Symbole

$x, y, z, \ldots, x_1, x_2, \ldots\ldots$	Variablen (für Elemente)
$c, d, e, \ldots$	Konstantensymbole
$f, g, \ldots$	Funktionssymbole (von geg. Stelligkeiten)
$P, Q, R, U, W, \ldots$	Relationsymbole (von geg. Stelligkeiten)

Eine *Signatur* S ist eine Menge von Konstanten-, Funktions- und Relationssymbolen, mit angegebenen Stelligkeiten.

Spezialfälle: S ohne Funktionssymbole : relationale Signatur;
S ohne Relationssymbole : funktionale Signatur.

1.1 Strukturen

Definition 1.1 [S-Strukturen] Für Signatur S:
Eine *S-Struktur* $\mathcal{A} = (A, c^{\mathcal{A}}, \ldots, f^{\mathcal{A}}, \ldots, R^{\mathcal{A}}, \ldots)$ besteht aus ihrer Trägermenge $A \neq \emptyset$ zusammen mit einer *Interpretation* der Symbole in S, d.h.,

für jedes Konstantensymbol $c \in S$: ein ausgezeichnetes Element $c^{\mathcal{A}} \in A$.

für jedes n-stellige Funktionssymbol $f \in S$: eine n-stellige Funktion $f^{\mathcal{A}}\colon A^n \to A$.

für jedes n-stellige Relationssymbol $R \in S$: eine n-stellige Relation $R^{\mathcal{A}} \subseteq A^n$.

Beispiele (vgl. auch: FG I; Datentypen; Standardstrukturen der Mathematik.)

Σ-*Wörter/Wortstrukturen* über der Signatur $S = \{<\} \cup \{P_a\colon a \in \Sigma\}$ mit 2-stelligem Relationssymbol $<$ und 1-stelligen Relationssymbolen P_a. Assoziiere Σ-Wort $w = a_1 \ldots a_n$

mit der Wortstruktur

$$\mathcal{W} = \big(\{1,\ldots,n\}, <^{\mathcal{W}}, (P_a^{\mathcal{W}})_{a\in\Sigma}\big),$$

wo $<^{\mathcal{W}}$ die übliche Ordnung auf $\{1,\ldots,n\}$ ist und $P_a^{\mathcal{W}} = \{i\colon a_i = a\}$.

Wortmonoid über der Signatur $S = \{\circ, e\}$ mit 2-stelligem Funktionssymbol $\circ$ und Konstantensymbol e. Für Alphabet Σ ist das Wortmonoid die S-Struktur $\mathcal{A} = \big(\Sigma^*, \circ^{\mathcal{A}}, e^{\mathcal{A}}\big)$ wobei $\circ^{\mathcal{A}}$ die Konkatenationsoperation auf Σ^* und $e^{\mathcal{A}} = \varepsilon$ das leere Σ-Wort ist.

Graphen über der Signatur $S = \{E\}$ mit einem 2-stelligen Relationssymbol. Eine S-Struktur $\mathcal{G} = (V, E^{\mathcal{G}})$ heißt Graph mit Knotenmenge V und Kantenrelation $E^{\mathcal{G}}$.

Transitionssysteme zum Alphabet Σ über der Signatur $S = \{E_a\colon a \in \Sigma\}$ mit 2-stelligen Relationssymbolen E_a. So kann man ein Transitionssystem (Σ, Q, Δ) als S-Struktur $\mathcal{A} = \big(Q, (E_a^{\mathcal{A}})_{a\in\Sigma}\big)$ beschreiben, wobei $E_a^{\mathcal{A}} = \{(q,q')\colon (q,a,q') \in \Delta\}$ (a-beschriftete Kanten). Für deterministische Transitionssysteme (Σ, Q, δ) kann man alternativ auch 1-stellige Funktionssysmbole $(f_a)_{a\in\Sigma}$ verwenden, die als $f_a^{\mathcal{A}}(q) := \delta(q,a)$ interpretiert werden.

Relationale Datenbanken lassen sich als relationale Strukturen modellieren. Als Trägermenge dient die disjunkte Vereinigung aller möglichen Sorten (Attribute), die in Datentupeln auftreten können (mehrsortige Strukturen); jede dieser Sorten wird durch ein 1-stelliges Prädikat gekennzeichnet; Dateneinträge sind dann Tupel in enstsprechende Relationen. Z.B. könnte eine rudimentäre Immatrikulationssdatenbank aus Sorten für die Matrikelnummer $n \in \{0,\ldots,N\}$, Startsemester $s \in \{\mathrm{WS}, \mathrm{SS}\}$ und Jahr $j \in \{1950,\ldots,2050\}$ bestehen. Zur relationalen Signatur $\{M, S, J, I\}$ mit Relationssymbolen M, S, J (1-stellig) und I (3-stellig) kann man eine Instanz dieser Datenbank dann als Struktur über der Trägermenge $\{0,\ldots,N\} \cup \{\mathrm{WS},\mathrm{SS}\} \cup \{1950,\ldots,2050\}$ modellieren, in der M, S, J durch die entsprechenden Teilmengen der Trägermenge interpretiert sind und die Relation I genau aus allen Tupeln (n,s,j) besteht, die zu Einträgen in der Immatrikulationstabelle gehören.

Boolesche Algebren (vgl. FG I) Boolesche Algebren sind bestimmte S-Strukturen zur funktionalen Signatur $S = \{\cdot, +, ', 0, 1\}$ mit 2-stelligen Funktionssymbolen $\cdot$ und $+$, einstelligem Funktionssymbol $'$ und Konstantensymbolen 0 und 1. Z.B. kann man die Standard-BA als S-Struktur mit Trägermenge $\mathbb{B} = \{0,1\}$ und der Interpretation von $\cdot$, $+$, $'$ durch die Booleschen Operationen $\wedge$, $\vee$, $\neg$ und von den Konstanten 0 und 1 durch die entsprechenden Elemente von $\mathbb{B}$ auffassen.

Arithmetik Die Standardstruktur der Arithmetik ist für $S = \{+, \cdot, <, 0, 1\}$ die S-Struktur $\mathcal{N} = \big(\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, <^{\mathbb{N}}, 0, 1\big)$ mit den üblichen arithmetischen Operationen als Interpretation für die 2-stelligen Funktionssysmbole $+$ und $\cdot$, mit der natürlichen linearen Ordnung auf $\mathbb{N}$ als Interpretation für das 2-stellige Relationssymbol $<$ und mit den üblichen Interpretationen der Konstantensymbole 0 und 1 durch die entsprechenden Elemente des Trägers $\mathbb{N}$.

Übung 1.2 Man schlage Signaturen S und natürliche Modellierungen als S-Strukturen vor z.B. für: den Datentyp M-wertiger Listen (über fester Menge M); Σ-NFA bzw. Σ-DFA; den Konfigurationsraum eines gegebenen Σ-PDA.

1.2 Terme

Sei S eine Signatur. Wir interessieren uns hier nur für die Funktions- und Konstantensymbole in S, also den funktionalen Anteil $S_{\mathsf{F}} \subseteq S$. Terme sind korrekt geschachtelte

Funktions-Ausdrücke aus Variablen, Konstanten und Funktionssymbolen, die zur Benennung bestimmter Elemente von Strukturen dienen. Variablensymbole dienen dabei als vorübergehend vereinbarte Namen für Elemente; die 'vorübergehende Vereinbarung' wird durch eine Belegung der Variablen durch Elemente spezifiziert.

Standardvariablenmengen $\mathrm{V} := \{x_1, x_2, \ldots\}$, und $\mathrm{V}_n := \{x_1, \ldots, x_n\} \subseteq \mathrm{V}$ für $n \in \mathbb{N}$. Konvention (zur besseren Lesbarkeit): auch x, y oder z anstelle von entsprechenden x_i.

Definition 1.3 [S-Terme]
Die Menge der *S-Terme*, $T(S)$ (mit Variablenmenge V) ist induktiv erzeugt wie folgt:

- $x \in T(S)$ für jede Variable $x \in \mathrm{V}$.
- $c \in T(S)$ für jedes Konstantensymbol $c \in S$.
- ist $f \in S$ ein n-stelliges Funktionssymbol, und sind $t_1, \ldots, t_n \in T(S)$, so ist auch $ft_1 \ldots t_n \in T(S)$.

$T_n(S) \subseteq T(S)$: die Mengen der Terme, in denen nur Variablensymbole aus $\mathrm{V}_n = \{x_1, \ldots, x_n\}$ vorkommen.

Speziell steht $T_0(S)$ für die Menge der Variablen-freien Terme ($= \emptyset$ wenn S keine Konstanten hat).

Schreibweisen: bei 2-stelligen Funktionen alternativ oft auch infixe Notation wie z.B. $(c + d)$ anstelle der Präfixnotation $+cd$; beachte aber, dass dann i.d.R. Klammern nötig sind, um geschachtelte Termen eindeutig lesbar zu machen. Man kann sich überlegen (und exakt beweisen), dass bei Präfixnotation eindeutige Lesbarkeit auch ohne Klammern gegeben ist.

Der induktive Aufbau der S-Terme erlaubt es, Funktionen auf $T(S)$ induktiv zu definieren (vgl. FG I). Z.B. gebe man eine induktive Definition einer Funktion

$$\begin{array}{rcl} \mathrm{var}\colon T(S) & \longrightarrow & \mathcal{P}(\mathrm{V}) \\ t & \longmapsto & \mathrm{var}(t) \end{array}$$

an, sodass $\mathrm{var}(t)$ die Menge der in t vorkommenden Variablensymbole ist.
[Damit ist $T_n(S) = \{t \ \in T(S)\colon \mathrm{var}(t) \subseteq \mathrm{V}_n\}$.]

Übung 1.4 Für feste endliche Signatur und Variablenmenge V_n soll (über einem geeigneten Alphabet) eine Grammatik zur Erzeugung von $T_n(S)$ angegeben werden.

Man überlegt sich dabei, dass $T_n(S)$ schon für relatv einfache S nicht regulär, aber kontextfrei ist.
Wie kann man $T(S)$ sinnvoll als Sprache über einem endlichen Alphabet erfassen?

Termstrukturen Die Menge der S-Terme ist Träger einer S_{F}-Struktur $\mathcal{T} = \mathcal{T}(S)$, der Termstruktur (*Herbrand-Struktur*) zu S, mit der folgenden natürlichen Interpretation der Konstanten- und Funktionssymbole in S:

- für Konstantensymbol $c \in S$: $\quad c^{\mathcal{T}} := c \in T(S)$.
- für n-stelliges Funktionssymbol $f \in S$: $\quad \begin{array}{rcl} f^{\mathcal{T}}\colon T(S)^n & \longrightarrow & T(S) \\ (t_1, \ldots, t_n) & \longmapsto & ft_1 \ldots t_n. \end{array}$

Wenn S Konstantensymbole hat, ist auch $T_0(S)$ Träger einer entsprechenden Termstruktur $\mathcal{T}_0(S)$ (eine Substruktur von $\mathcal{T}(S)$).

1.3 Belegungen

Variablenfreie S-Terme haben in jeder S-Struktur $\mathcal{A}$ eine eindeutige Interpretation (als Namen von Elementen, die man durch Auswertung des Terms i.S.d. Interpretation von Konstanten und Funktionen in $\mathcal{A}$ bestimmt). Für Terme mit Variablen braucht man zusätzlich eine Interpretation der Variablen, sogenannte *Belegungen*.

Definition 1.5 [Belegungen und Interpretationen]
Eine Funktion $\beta\colon \mathrm{V} \to A$ heißt *Belegung* (für die $x \in \mathrm{V}$) in der S-Struktur $\mathcal{A} = (A, \ldots)$. Eine S-Struktur $\mathcal{A}$ und Belegung β zusammen bilden eine *S-Interpretation* $\mathfrak{I} = (\mathcal{A}, \beta)$.

Semantik von Termen Induktiv über den Aufbau der S-Terme definieren wir für eine gegebene S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$ als *Interpretation von $t \in T(S)$* das von t bezeichnete Element $t^{\mathfrak{I}} \in A$:

- Für $t = x$ ($x \in \mathrm{V}$ Variable): $\quad t^{\mathfrak{I}} := \beta(x)$.
- Für $t = c$ ($c \in S$ Konstantensymbol): $\quad t^{\mathfrak{I}} := c^{\mathcal{A}}$.
- Für $t = ft_1 \ldots t_n$, mit n-stelligem Funktionssymbol $f \in S$: $\quad t^{\mathfrak{I}} := f^{\mathcal{A}}\big(t_1^{\mathfrak{I}}, \ldots, t_n^{\mathfrak{I}}\big)$.

Übung 1.6 Man formuliere und beweise den folgenden (offensichtlichen) Sachverhalt exakt: Die Interpretation $t^{\mathfrak{I}}$ hängt nur ab von $\mathcal{A}$ und den Belegungen $\beta(x)$ für die $x \in \mathrm{var}(t)$.

Wir schreiben $t = t(x_1, \ldots, x_n)$ wenn $\mathrm{var}(t) \subseteq \mathrm{V}_n$. Dann sei

$$t^{\mathcal{A}}[a_1, \ldots, a_n] := t^{\mathfrak{I}} \quad \text{für } \mathfrak{I} = (\mathcal{A}, \beta) \text{ mit } \beta(x_i) = a_i \text{ für } i = 1, \ldots, n.$$

Übung 1.7 (vgl. FG I) Man zeige, dass für jede S_{F}-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$ die Abbildung

$$\begin{array}{rcl} h\colon T(S) & \longrightarrow & A \\ t & \longmapsto & t^{\mathfrak{I}} \end{array}$$

ein Homomorphismus von der Termstruktur $\mathcal{T}(S)$ nach $\mathcal{A}$ ist.

Schreibweisen für Belegungen und Interpretationen Zu $\beta\colon \mathrm{V} \to A$ bezeichnet $\beta[x \mapsto a]$ die abgeänderte Belegung β' mit

$$\beta'(y) = \begin{cases} a & \text{für } y = x \\ \beta(y) & \text{sonst.} \end{cases}$$

Analog bei Interpretationen $\mathfrak{I} = (\mathcal{A}, \beta)$: $\quad \mathfrak{I}[x \mapsto a]$ steht für die Variante $(\mathcal{A}, \beta[x \mapsto a])$.

2 Syntax und Semantik von FO

Bem.: Wir behandeln in diesem Teil die volle Logik erster Stufe, *mit Gleichheit*. Wenn in anderen Kapiteln die eingeschränkte Variante von FO ohne die Gleichheitsrelation behandelt wird, wird explizit darauf hingewiesen.

2.1 Syntax

Für FO(S), bei gegebener Signatur S:

Symbole

$c, \ldots, f, \ldots, R, \ldots$	Symbole der Signatur S
$x \in \mathrm{V}$	Variablensymbole (gemäß obigen Konventionen)
$\neg, \wedge, \vee$	Junktoren, wie in AL
$\rightarrow, \leftrightarrow, \ldots$	weitere, definierte Junktoren, wie in AL
$=$	Gleichheitssymbol
$\forall, \exists$	All- und Existenzquantoren
$(,)$	

Definition 2.1 [Syntax von FO(S)]
Die Menge FO(S) der Formeln der Logik erster Stufe zur Signatur S wird induktiv erzeugt wie folgt

- (atomare Formeln)
  (Gleichheit) für $t_1, t_2 \in T(S)$: $t_1 = t_2 \in \mathrm{FO}(S)$.
  (n-st. Relationssymbol $R \in S$) für $t_1, \ldots, t_n \in T(S)$: $Rt_1 \ldots t_n \in \mathrm{FO}(S)$.
- (Negation) für $\varphi \in \mathrm{FO}(S)$ ist $\neg\varphi \in \mathrm{FO}(S)$.
- (Konjunktion, Disjunktion) für $\varphi, \psi \in \mathrm{FO}(S)$ sind $(\varphi \wedge \psi), (\varphi \vee \psi) \in \mathrm{FO}(S)$.
- (Quantoren) für $\varphi \in \mathrm{FO}(S)$ und $x \in \mathrm{V}$ sind
  $\exists x\varphi \in \mathrm{FO}(S)$ (existentielle Quantifizierung, Existenzformel),
  $\forall x\varphi \in \mathrm{FO}(S)$ (universelle Quantifizierung, Allformel).

Für gleichheitsfreie Logik erster Stufe, $\mathrm{FO}^{\neq}$, entfallen die atomaren Formeln vom Typ $t_1 = t_2$.

Die existenzielle/universelle Quantifizierung $\exists x\varphi$ bzw. $\forall x\varphi$ *bindet* die Variable x. Variablen können in Formeln gebunden oder frei auftreten.

Freie Variablen und Quantorenrang (Schachtelungstiefe von Quantoren) einer Formel werden als Funktionen induktiv anhand des Aufbaus der Formeln definiert:

Definition 2.2 [freie Variablen]
Induktive Definition der Menge der *freien Variablen*, $\mathrm{frei}(\varphi) \subseteq \mathrm{V}$, für $\varphi \in \mathrm{FO}(S)$:
$\mathrm{frei}(t_1 = t_2) := \mathrm{var}(t_1) \cup \mathrm{var}(t_2)$.
$\mathrm{frei}(Rt_1 \ldots t_n) := \mathrm{var}(t_1) \cup \ldots \cup \mathrm{var}(t_n)$.
$\mathrm{frei}(\neg\varphi) := \mathrm{frei}(\varphi)$.
$\mathrm{frei}(\varphi \wedge \psi) = \mathrm{frei}(\varphi \vee \psi) := \mathrm{frei}(\varphi) \cup \mathrm{frei}(\psi)$.
$\mathrm{frei}(\exists x\varphi) = \mathrm{frei}(\forall x\varphi) := \mathrm{frei}(\varphi) \setminus \{x\}$.
Formeln ohne freie Variablen heißen *Sätze*.

Schreibweisen: $\mathrm{FO}_n(S) := \{\varphi \in \mathrm{FO}(S) \colon \mathrm{frei}(\varphi) \subseteq \mathrm{V}_n\}$. Für $\varphi \in \mathrm{FO}_n(S)$ schreiben wir auch $\varphi = \varphi(x_1, \ldots, x_n)$ um die möglicherweise freien Variablen explizit anzudeuten.

Definition 2.3 [Quantorenrang]
Induktive Definition des *Quantorenrangs*, $\mathrm{qr}(\varphi) \in \mathbb{N}$, für $\varphi \in \mathrm{FO}(S)$:
$\mathrm{qr}(\varphi) = 0$ für atomares φ.
$\mathrm{qr}(\neg\varphi) := \mathrm{qr}(\varphi)$.
$\mathrm{qr}(\varphi \wedge \psi) = \mathrm{qr}(\varphi \vee \psi) := \max(\mathrm{qr}(\varphi), \mathrm{qr}(\psi))$.
$\mathrm{qr}(\exists x\varphi) = \mathrm{qr}(\forall x\varphi) := \mathrm{qr}(\varphi) + 1$.
Formeln von Quantorenrang 0 heißen *quantorenfrei*.

2.2 Semantik

Jeder FO(S)-Formel wird bezüglich einer gegebenen S-Interpretation $\mathfrak{I}$ ein Wahrheitswert $\varphi^{\mathfrak{I}} \in \mathbb{B}$ zugewiesen.

D.h., die Semantik beruht auf einer *Modellbeziehung* zwischen FO(S)-Formeln φ und S-Interpretationen $\mathfrak{I} = (\mathcal{A}, \beta)$ (S-Strukturen mit Belegungen der Variablen!): $\mathfrak{I}$ ist ein Modell von φ, $\mathfrak{I} \models \varphi$, gdw. $\varphi^{\mathfrak{I}} = 1$. Die Funktion

$$\begin{array}{rccc} {}^{\mathfrak{I}}\colon \mathrm{FO}(S) & \longrightarrow & \mathbb{B} \\ \varphi & \longmapsto & \varphi^{\mathfrak{I}}, \end{array}$$

wird induktiv über den Aufbau der Formeln φ definiert. Für atomare Formeln wird die Interpretation $t^{\mathfrak{I}}$ für Terme $t \in T(S)$ verwendet.

- (atomare Formeln): $(t_1 = t_2)^{\mathfrak{I}} = 1$ gdw. $t_1^{\mathfrak{I}} = t_2^{\mathfrak{I}}$.
  $(Rt_1 \dots t_n)^{\mathfrak{I}} = 1$ gdw. $(t_1^{\mathfrak{I}}, \dots, t_n^{\mathfrak{I}}) \in R^{\mathcal{A}}$.
- (Negation): $(\neg\varphi)^{\mathfrak{I}} := 1 - \varphi^{\mathfrak{I}}$.
- (Konjunktion): $(\varphi \wedge \psi)^{\mathfrak{I}} := \min(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.
- (Disjunktion): $(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.
- (Quantoren): $(\exists x\varphi)^{\mathfrak{I}} = \max\big(\varphi^{\mathfrak{I}[x\mapsto a]}\colon a \in A\big)$.
  $(\forall x\varphi)^{\mathfrak{I}} = \min\big(\varphi^{\mathfrak{I}[x\mapsto a]}\colon a \in A\big)$.

Bem.: Die min/max Konstrukte für die Wahrheitswerte von $\forall/\exists$-Formeln sind analog zu (i.d.R. unendlichen) Konjunktionen/Disjunktionen über *alle* an der Stelle x abgeänderten Belegungen gebildet. $(\exists x\varphi)^{\mathfrak{I}} = \max\big(\varphi^{\mathfrak{I}[x\mapsto a]}\colon a \in A\big)$ z.B. bedeutet dass $\exists x\varphi$ unter $\mathfrak{I}$ wahr ist gdw. φ unter mindestens einer der $\mathfrak{I}[x \mapsto a] = (\mathcal{A}, \beta[x \mapsto a])$ wahr ist (wobei alle Elemente a des Trägers von $\mathcal{A}$ als Belegungen von x zugelassen sind).

Definition 2.4 [Semantik]
Für S-Interpretation $\mathfrak{I} = (\mathcal{A}, \beta)$ und $\varphi \in \mathrm{FO}(S)$:
$\mathfrak{I}$ *erfüllt* φ gdw. $\varphi^{\mathfrak{I}} = 1$. Schreibweise: $\mathfrak{I} \models \varphi$.
Für Formelmengen $\Phi \subseteq \mathrm{AL}(\mathcal{V})$ entsprechend: $\mathfrak{I} \models \Phi$ gdw. $\mathfrak{I} \models \varphi$ für alle $\varphi \in \Phi$.

Sprechweisen für $\mathfrak{I} \models \varphi$: "$\mathfrak{I}$ *erfüllt* φ",
"$\mathfrak{I}$ *ist Modell von* φ",
"φ *ist wahr unter* $\mathfrak{I}$".
Die Relation $\models$ heißt *Modellbeziehung*.

Beispiele Wir geben einige Beispiele für FO-Formalisierungen an (vgl. auch FG I). Dabei verwenden wir die üblichen AL-Abkürzungen mittels Junktoren $\rightarrow$, und sparen Klammern, wo das aus AL-Äquivalenzen (die sich alle übertragen) gerechtfertigt ist.

Als Übung empfohlen: ein paar Beispiele explizit anhand der offiziellen Definition der Semantik auszuwerten.

Äquivalenzrelationen: $S = \{E\}$, E 2-stelliges Relationssymbol. $E^{\mathcal{A}}$ ist eine Äquivalenzrelation auf A, gdw. $\mathcal{A} = (A, E^{\mathcal{A}}) \models \varphi$ für den FO(E)-Satz

$$\varphi = \forall xExx \wedge \forall x\forall y(Exy \rightarrow Eyx) \wedge \forall x\forall y\forall z((Exy \wedge Eyz) \rightarrow Exz).$$

Eigenschaften von Funktionen: Sei f ein 1-stelliges Funktionssymbol in S. Dann wird z.B. Injektivität von f formalisiert durch

$$\forall x \forall y (fx = fy \to x = y).$$

Beachte, dass z.B. $\forall x \exists y fx = y$ in jeder Interpretation gilt, da $f^{\mathcal{A}}$ stets als Funktion mit Definitionsbereich A interpretiert wird. Man kann aber z.B. auch für 1-Stellige Relationssymbole $U, W \in S$ ausdrücken, dass die Einschränkung von f auf den Definitionsbereich U eine Funktion mit Bild W ist:

$$\forall x (Ux \to Wfx) \wedge \forall y (Wy \to \exists x (Ux \wedge fx = y)).$$

Das Bild von $f^{\mathcal{A}}$ besteht allgemein aus denjenigen Belegungen für die Variable x, die über $\mathcal{A}$ die Formel $\exists y\, fy{=}x$ wahr machen.

Lineare Ordnungen: $S = \{<\}$, $<$ 2-stelliges Relationssymbol (das wir infix schreiben: $x < y$ statt $< xy$). $<^{\mathcal{A}}$ ist eine lineare Ordnung auf A, gdw. $\mathcal{A} = (A, <^{\mathcal{A}}) \models \varphi$ für den FO($<$)-Satz

$$\varphi = \forall x \neg x < x \wedge \forall x \forall y (\neg x = y \to (x < y \vee y < x)) \wedge \forall x \forall y \forall z ((x < y \wedge y < z) \to x < z).$$

In Graphen: $S = \{E\}$, E 2-stelliges Relationssymbol. $\mathcal{A} = (A, E^{\mathcal{A}})$ ist ein symmetrischer (ungerichteter) Graph ohne Schlaufen und ohne isolierte Knoten, gdw. der folgende Satz erfüllt ist:

$$\forall x \forall y (Exy \leftrightarrow Eyx) \wedge \forall x (\neg Exx \wedge \exists y Exy).$$

In relationalen Datenbanken: (project/join Abfrage; vgl. "select-from-where" in SQL) Seien $I, P \in S$ zwei 3-stellige Relationssymbole zur Modellierung einer Immatrikulationsrelation I von Tupeln (Matrikel-Nr,Imm.-Semester,Imm.-Jahr) und Prüfungsanmeldungsrelation P von Tupeln (Matrikel-Nr,Prüfungsfach-Nr,Jahr). Dann erhält man als Antwort auf die Abfrage nach Matr.-Nummern von Studenten, die sich bereits im Kalenderjahr ihrer Immatrikulation zu einer Prüfung gemeldet haben, diejenigen Belegungen der Variablen x für die die folgende Formel wahr gemacht wird:

$$\varphi(x) = \exists z \exists y_1 \exists y_2 (Ixy_1z \wedge Pxy_2z).$$

Dies ist ein Beispiel einer "conjunctive query", eine wichtige Klasse von Datenbankabfragen; die Kernformel $Ixy_1z \wedge Pxy_2z$ beschreibt einen sogenannten "relational join", der zwei gegebene Relationen über bestimmte gemeinsame Attribute (Stellen, Variablen) verknüpft.

Arithmetik: Für $S = \{+, \cdot, 0, 1\}$ sind die folgenden Axiome der Peano-Arithmetik im Standardmodell $\mathcal{N} = (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, 0, 1)$ erfüllt (aber nicht nur in diesem):

$\forall x\ \neg x + 1 = 0$ $\qquad$ $\forall x\ x + 0 = x$ $\qquad$ $\forall x \forall y\ x + (y + 1) = (x + y) + 1$

$\forall x (\neg x = 0 \to \exists y x = y + 1)$ $\qquad$ $\forall x\ x \cdot 0 = 0$ $\qquad$ $\forall x \forall y\ x \cdot (y + 1) = (x \cdot y) + x$

$\forall x \forall y (x + 1 = y + 1 \to x = y)$

Die Rolle der Belegungen Man zeigt (durch Induktion über die Formeln φ), dass $\varphi^{\mathfrak{I}}$ für $\mathfrak{I} = (\mathcal{A}, \beta)$ nur von $\mathcal{A}$ und den Belegungen $\beta(x)$ für $x \in \mathrm{frei}(\varphi)$ abhängt. Präzise:

$$\big(\beta(x) = \beta'(x) \text{ für alle } x \in \mathrm{frei}(\varphi)\big) \quad \Rightarrow \quad \big((\mathcal{A}, \beta) \models \varphi \;\Leftrightarrow\; (\mathcal{A}, \beta') \models \varphi\big).$$

Sei $\varphi = \varphi(x_1, \ldots, x_n)$, d.h. φ mit $\mathrm{frei}(\varphi) \subseteq \mathrm{V}_n$. Dann reicht es also die Belegung β auf V_n zu kennen.

Eine Belegung für $\mathrm{V}_n \subseteq \mathrm{V}$ wird durch das n-Tupel $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$ mit $a_i = \beta(x_i)$ vollständig spezifiziert. Man definiert daher

$$\mathcal{A} \models \varphi[a_1, \ldots, a_n] \quad \text{gdw.} \left[\begin{array}{l} (\mathcal{A}, \beta) \models \varphi \text{ für ein/alle } \beta \text{ mit} \\ \beta(x_i) = a_i \text{ für } i = 1, \ldots n \end{array}\right].$$

2.3 Semantische Grundbegriffe

Begriffe von *Folgerung*, *Erfüllbarkeit*, *Allgemeingültigkeit*, *logischer Äquivalenz* übertragen sich sofort auf FO.

Definition 2.5 [Folgerungsbeziehung, $\varphi \models \psi$ bzw. $\Phi \models \psi$.]
Für $\varphi, \psi \in \mathrm{FO}(S)$:
ψ ist eine *logische Folgerung* von φ, oder ψ *folgt aus* φ, in Symbolen $\varphi \models \psi$, gdw. für alle S-Interpretationen $\mathfrak{I}$ gilt: $\mathfrak{I} \models \varphi \;\Rightarrow\; \mathfrak{I} \models \psi$.
Entsprechend ist $\Phi \models \psi$ für Formelmengen Φ definiert (ψ *folgt aus* Φ).

Definition 2.6 [Allgemeingültigkeit]
Eine Formel $\varphi \in \mathrm{FO}(S)$ heißt *allgemeingültig* gdw. für alle S-Interpretationen $\mathfrak{I}$ gilt: $\mathfrak{I} \models \varphi$.

Definition 2.7 [logische Äquivalenz]
Zwei Formeln $\varphi, \psi \in \mathrm{FO}(S)$ heißen *(logisch) äquivalent*, gdw. für alle S-Interpretationen $\mathfrak{I}$ gilt: $\mathfrak{I} \models \varphi$ gdw. $\mathfrak{I} \models \psi$. In Symbolen: $\varphi \equiv \psi$.

Bem.: Logische Äquivalenzen der AL übertragen sich auf FO. Hinzu treten charakteristische logische Äquivalenzen im Zusammenhang mit Quantoren.

Z.B. die *Dualität* zwischen $\forall$ und $\exists$, die besagt dass für alle $\varphi \in \mathrm{FO}(S)$:

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

Übung 2.8 Zeigen Sie, dass für beliebige φ und Variablen $x, y \in \mathrm{V}$ zwar stets gilt, dass $\exists x\forall y\varphi \models \forall y\exists x\varphi$, aber i.A. nicht $\exists x\forall y\varphi \equiv \forall y\exists x\varphi$.

Übung 2.9 Eine Formel $\varphi \in \mathrm{FO}(S)$ ist in *Negationsnormalform* (NNF) wenn sie ausgehend von atomaren und negiert atomaren Formeln allein mittels $\wedge, \vee, \exists, \forall$ aufgebaut ist. Man gebe eine induktiv definierte Funktion $\mathrm{NNF}\colon \mathrm{FO}(S) \to \mathrm{FO}(S)$ an, sodass $\mathrm{NNF}(\varphi) \equiv \varphi$ und $\mathrm{NNF}(\varphi)$ in NNF ist.
Hinweis: Am einfachsten definiert man für jedes φ simultan $\mathrm{NNF}(\varphi)$ und $\mathrm{NNF}(\neg\varphi)$.

Bem.: Logische Äquivalenz ist modular und mit allen natürlichen Einsetzungsprozessen verträglich. Ersetzt man z.B. in einer Formel φ eine ihrer Teilformeln ψ durch $\psi' \equiv \psi$, so ist das Ergebnis φ' wieder zu φ äquivalent. Damit kann man z.B. AL-Äquivalenzen im Innern von FO-Formeln auszunutzen.

Die folgende Äquivalenzbeziehung der *Erfüllbarkeitsäquivalenz* ist schwächer als logische Äquivalenz. Offensichtlich sind logisch äquivalente Formeln erfüllungsäquivalent. Wir werden z.B. im Zusammenhang mit der Skolemnormalformen in Abschnitt 3.3 erfüllbarkeitsäquivalente, nicht logisch äquivalente Formlen betrachten.

Definition 2.10 Formeln φ, φ' heißen *erfüllbarkeitsäquivalent* wenn gilt: φ erfüllbar gdw. φ' erfüllbar. Analog wird Erfüllbarkeitsäquivalenz für Formelmengen definiert.

2.4 Zwei Variationen: relationale Algebra, Spielsemantik

Zwei Bemerkungen zur Semantik von FO illustrieren äquivalente, alternative und anschauliche Sichtweisen, die für Verständnis und Anwendungen nützlich sind.

Definierte Relationen; relationale Algebra ($\to$ relationale Datenbanken)
In einer S-Struktur $\mathcal{A}$ kann man einer $\mathrm{FO}_n(S)$-Formel $\varphi = \varphi(x_1, \ldots, x_n)$ als Semantik auch die *von φ definierte n-stellige Relation*

$$[\![\varphi]\!]^{\mathcal{A}} := \big\{\mathbf{a} = (a_1, \ldots, a_n) \in A^n \colon \mathcal{A} \models \varphi[\mathbf{a}]\big\} \subseteq A^n$$

zuweisen. [Vgl. in Datenbanken: das Ergebnis der DB-Abfrage φ.]

Für $\varphi \in \mathrm{FO}_n(S)$ mit Variablen aus V_n (frei oder gebunden) kann man so induktiv die Semantik direkt anhand der Zuordnung $\varphi \mapsto [\![\varphi]\!]^{\mathcal{A}}$ definieren:

- $[\![t_1 = t_2]\!]^{\mathcal{A}} := \{\mathbf{a} \in A^n \colon t_1^{\mathcal{A}}[\mathbf{a}] = t_2^{\mathcal{A}}[\mathbf{a}]\}$.
  $[\![Rt_1 \ldots t_k]\!]^{\mathcal{A}} := \{\mathbf{a} \in A^n \colon (t_1^{\mathcal{A}}[\mathbf{a}], \ldots, t_k^{\mathcal{A}}[\mathbf{a}]) \in R^{\mathcal{A}}\}$.
- $[\![\neg\varphi]\!]^{\mathcal{A}} := A^n \setminus [\![\varphi]\!]^{\mathcal{A}}$.
- $[\![\varphi \wedge \psi]\!]^{\mathcal{A}} := [\![\varphi]\!]^{\mathcal{A}} \cap [\![\psi]\!]^{\mathcal{A}}$.
- $[\![\varphi \vee \psi]\!]^{\mathcal{A}} := [\![\varphi]\!]^{\mathcal{A}} \cup [\![\psi]\!]^{\mathcal{A}}$.
- $[\![\exists x_i \varphi]\!]^{\mathcal{A}} := \big\{\mathbf{a} = (a_1, \ldots, a_n) \in A^n \colon$ ex. $a_i' \in A$ mit $(a_1, \ldots, a_i', \ldots, a_n) \in [\![\varphi]\!]^{\mathcal{A}}\big\}$.
  $[\![\forall x_i \varphi]\!]^{\mathcal{A}} := \big\{\mathbf{a} = (a_1, \ldots, a_n) \in A^n \colon$ f.a. $a_i' \in A$ mit $(a_1, \ldots, a_i', \ldots, a_n) \in [\![\varphi]\!]^{\mathcal{A}}\big\}$.

So entsprechen sich

Negation	—	Komplement
Konjunktion	—	Durchschnitt
Disjunktion	—	Vereinigung

Der existentiellen Quantifizierung entspricht eine Projektion (man kann die abquantifizierte Komponente weglassen anstatt sie wie hier trivial aufzufüllen).

Spielsemantik – Semantikspiele ($\to$ model checking)
Wir betrachten Formeln $\varphi \in \mathrm{FO}_n(S)$ in Negationsnormalform (NNF) mit Variablen aus V_n (frei oder gebunden) über einer festen S-Struktur $\mathcal{A}$. Sei $\mathrm{SF}(\varphi) \subseteq \mathrm{FO}_n(S)$ die Menge aller Subformeln von φ (induktive Definition von $\mathrm{SF}(\varphi)$: Übung!).

Alle relevanten Belegungen über $\mathcal{A}$ (für $\psi \in \mathrm{SF}(\varphi)$) lassen sich als n-Tupel $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$ spezifizieren.

Semantik-Spiel $[\mathcal{A}; \mathrm{SF}(\varphi)]$:

Spieler: **V**erifizierer gegen **F**alsifizierer

Spielpositionen: $(\psi, \mathbf{a}) \in \mathrm{SF}(\varphi) \times A^n$

Züge in Position $(\psi, \mathbf{a})$, $\mathbf{a} = (a_1, \ldots, a_n)$:

$\psi = \psi_1 \wedge \psi_2$	**F** am Zug	zieht nach $(\psi_1, \mathbf{a})$ oder nach $(\psi_2, \mathbf{a})$.
$\psi = \psi_1 \vee \psi_2$	**V** am Zug	zieht nach $(\psi_1, \mathbf{a})$ oder nach $(\psi_2, \mathbf{a})$.
$\psi = \forall x_i \psi_0$	**F** am Zug	zieht nach einem $(\psi_0, \mathbf{a}')$ mit $\mathbf{a}' = (a_1, \ldots, a'_i, \ldots, a_n)$.
$\psi = \exists x_i \psi_0$	**V** am Zug	zieht nach einem $(\psi_0, \mathbf{a}')$ mit $\mathbf{a}' = (a_1, \ldots, a'_i, \ldots, a_n)$.

Spielende: in Positionen $(\psi, \mathbf{a})$, wo ψ atomar oder negiert atomar.

Gewinner: **V** gewinnt in Endposition $(\psi, \mathbf{a})$, wenn $\mathcal{A} \models \psi[\mathbf{a}]$,
F gewinnt in Endposition $(\psi, \mathbf{a})$, wenn $\mathcal{A} \not\models \psi[\mathbf{a}]$,

Spieler **V** hat eine Gewinnstrategie in Position $(\psi, \mathbf{a})$ wenn sie unabhängig von den Zügen von **F** in jeder Partie des Spiels, die in Position $(\psi, \mathbf{a})$ startet, Gewinn erzwingen kann. Dann gilt für alle Positionen $(\psi, \mathbf{a})$:

$$\mathcal{A} \models \psi[\mathbf{a}] \qquad \text{gdw.} \qquad \textbf{V} \text{ hat Gewinnstrategie in Position } (\psi, \mathbf{a}).$$

Bem.: Bei Eingaben $(\varphi, \mathcal{A}, \mathbf{a})$ mit endlicher S-Struktur $\mathcal{A}$ und φ mit Variablen in V_n führt ein geeigneter Suchalgorithmus im Spielgraphen zu einem Auswertungsalgorithmus mit (theoretisch bestmöglicher) polynomialer Laufzeit: effizientes model checking. (Ohne Einschränkung der Variablenzahl: Pspace-vollständig).

Frage: Wie muss das Spiel erweitert werden, damit es auch allgemein Negationen erfasst, d.h., damit man es nicht auf NNF Formeln einschränken muss?

2.5 FO mit und ohne Gleichheit

Definition 2.11 [FO ohne Gleichheit] $\mathrm{FO}^{\neq}(S) \subseteq \mathrm{FO}(S)$ ist aufgebaut wie FO aber ohne Termgleichheiten als atomare Formeln. Die Semantik von FO überträgt sich auf die Teillogik $\mathrm{FO}^{\neq}$.

Anstatt wie in FO (mit Gleichheit) der Gleichheitsrelation eine besondere logische Rolle zu geben, kann man ein 2-stelliges Relationssymbol, etwa $\sim$ (das wir infix schreiben) zur Signatur hinzunehmen, um damit die Gleichheit zu modellieren. Man kann aber zeigen, dass keine $\mathrm{FO}^{\neq}(S \cup \{\sim\})$-Formelmenge in allen ihren Modellen $\mathcal{A}$ erzwingt, dass $\sim^{\mathcal{A}} = \{(a, a) \colon a \in A\}$ (dass also $\sim$ in $\mathcal{A}$ durch die echte Gleichheitsrelation interpretiert wird). Das ist aber für die meisten Zwecke auch nicht nötig. Es reicht, dass $\sim$ eine Äquivalenzrelation ist, axiomatisiert durch

$$\varphi_\sim := \forall x\, x \sim x \wedge \forall x \forall y (x \sim y \to y \sim x) \wedge \forall x \forall y \forall z \big((x \sim y \wedge y \sim z) \to x \sim z\big),$$

und dass die Interpretation aller übrigen Symbole mit der Bildung von $\sim$-Äquivalenzklassen verträglich ist. Für ein 2-stelliges Relationssymbol z.B. ist diese Verträglichkeit durch die Bedingung

$$\varphi^R_\sim := \forall x_1 \forall x_2 \forall y_1 \forall y_2 \big((x_1 \sim y_1 \wedge x_2 \sim y_2) \to (Rx_1x_2 \leftrightarrow Ry_1y_2)\big)$$

formalisiert; für ein 2-stelliges Funktionssymbol f durch

$$\varphi^f_\sim := \forall x_1 \forall x_2 \forall y_1 \forall y_2 \big((x_1 \sim y_1 \wedge x_2 \sim y_2) \to fx_1x_2 \sim fy_1y_2\big).$$

In Modellen derartiger $\mathrm{FO}^{\neq}$-Axiome werden die eigentlich gemeinten Elemente durch $\sim$-Äquivalenzklassen beschrieben. Man kann in solchen Modellen dann zur *Quotientenstruktur* bzgl. der Interpretation von $\sim$ übergehen, um wieder mit der gewöhnlichen Gleichheit zu arbeiten.

Beispiel 2.12 Um die Kommutativität und Assoziativität einer 2-stelligen Operation $\circ$ so im Rahmen von $\mathrm{FO}^{\neq}$ zu erfassen, kann man in $\mathrm{FO}^{\neq}(\{\circ,\sim\})$ formalisieren:

$$\varphi = \varphi_\sim \wedge \varphi_\sim^\circ \wedge \forall x\forall y\big(x\circ y \sim y\circ x\big) \wedge \forall x\forall y\forall z\big((x\circ y)\circ z \sim x\circ(y\circ z)\big).$$

Zu jedem Modell $\mathcal{A} = (A, \sim^{\mathcal{A}}, \circ^{\mathcal{A}}) \models \varphi$ hat man nun eine $\{\circ\}$-Struktur, deren Elemente gerade die $\sim^{\mathcal{A}}$-Äquivalenzklassen $[a]$ der Elemente von $\mathcal{A}$ sind, mit der Interpretation $[a_1]\,\tilde\circ\,[a_2] := [a_1 \circ^{\mathcal{A}} a_2]$ für $\circ$. Man prüft nach, dass die entsprechenden Anteile von φ für dieses $\tilde\circ$ gerade die Kommutativität und Assoziativität beschreiben.

Vergleiche Definition 2.10 zur Erfüllbarkeitsäquivalenz.

Bemerkung 2.13 *Zu jeder Formelmenge $\Phi \subseteq \mathrm{FO}(S)$ erhält man durch eine systematische Übersetzung in eine explizite Modellierung der Gleichheitsrelation durch eine neues Relationssysmbol $\sim$ eine erfüllbarkeitsäquivalente Formelmenge $\Phi_\sim \subseteq \mathrm{FO}^{\neq}(S\cup\{\sim\})$.*

3 Normalformen, Substitution, Skolemisierung

3.1 Pränexe Normalform

Definition 3.1 [pränexe NF]
FO-Formeln in *pränexer Normalform* sind von der Form

$$Q_1 x_{i_1} \ldots Q_k x_{i_k} \psi,$$

wo $k \in \mathbb{N}$, $Q_i \in \{\forall, \exists\}$ und ψ quantorenfrei.
ψ heißt auch *quantorenfreier Kern* der Formel, $Q_1 x_{i_1} \ldots Q_k x_{i_k}$ ihr Quantorenpräfix.

Beispiel 3.2 $S = \{E\}$, E 2-st. Relations-Symbol. Die folgenden Äquivalenzen (unbedingt nachprüfen!) liefern auf der rechten Seite pränexe Formalisierungen:

$$\exists y(Exy \wedge \forall x(Eyx \to x = y)) \equiv \exists y\forall z\big(Exy \wedge (Eyz \to z = y)\big),$$
$$\exists y\forall x Exy \;\vee\; \neg\exists y Exy \equiv \exists y_1\forall y_2\forall y_3\big(Ey_1y_2 \vee \neg Exy_3\big).$$

(Man braucht i.d.R. zusätzliche Variablensymbole!)

Übung 3.3 Sei $x \notin \mathrm{frei}(\varphi)$. Zeigen Sie, dass dann für $Q \in \{\forall,\exists\}$: $\varphi \wedge Qx\psi \equiv Qx(\varphi\wedge\psi)$.
Analog schließe man, dass, sofern $x_1 \notin \mathrm{frei}(\varphi_2)$ und $x_2 \notin \mathrm{frei}(\varphi_1)$ ist, auch

$$Q_1x_1\varphi_1 \wedge Q_2x_2\varphi_2 \equiv Q_1x_1Q_2x_2(\varphi_1\wedge\varphi_2) \equiv Q_2x_2Q_1x_1(\varphi_1\wedge\varphi_2).$$

Satz 3.4 *Jede* FO*-Formel ist äquivalent zu einer Formel in pränexer NF.*

Beweis Induktion über den Aufbau der Formel; mit offiziellen Variablensymbolen in $\mathrm{V} = \{x_1, x_2, \ldots\}$.

Induktionsanfang für atomare (also quantorenfreie) Formeln und die Induktionsschritte für Quantoren sind trivial.

Negation: Mit Dualität von $\exists$ und $\forall$. Sei $\varphi = \neg\varphi_0$, $\varphi_0 \equiv Q_1 x_{i_1} \ldots Q_k x_{i_k} \psi$ mit quantorenfreiem ψ. Dann ist $\varphi \equiv \overline{Q_1} x_{i_1} \ldots \overline{Q_k} x_{i_k} \neg\psi$, wo $\overline{\exists} := \forall$ und $\overline{\forall} := \exists$.

Konjunktion: Sei $\varphi = \varphi_1 \wedge \varphi_2$, $\varphi_1 \equiv Q_1 x_{i_1} \ldots Q_k x_{i_k} \psi_1$, $\varphi_2 \equiv Q'_1 x_{i'_1} \ldots Q'_\ell x_{i'_\ell} \psi_2$, mit quantorenfreien ψ_1, ψ_2. Wir ersetzen die Variablensymbole $x_{i'_1}, \ldots, x_{i'_\ell}$ in ψ_2 durch Variablensymbole $x_{j_1}, \ldots, x_{j_\ell}$, die nicht in $\mathrm{frei}(\varphi) \cup \{x_{i_1}, \ldots, x_{i_k}\}$ sind. Dann ist $\varphi_2 \equiv Q'_1 x_{j_1} \ldots Q'_\ell x_{j_\ell} \psi'_2$, und die x_{i_s} und die x_{j_t} sämtlich verschieden. Wie in der Übung oben ergibt sich daraus dann, dass $\varphi \equiv Q_1 x_{i_1} \ldots Q_k x_{i_k} Q'_1 x_{j_1} \ldots Q'_\ell x_{j_\ell} (\psi_1 \wedge \psi'_2)$ in pränexer NF. Frage: Welche anderen Reihenfolgen der Quantoren $Q_s x_{i_s}$ und $Q'_t x_{j_t}$ führen in dieser besonderen Situation ebenfalls zu äquivalenten Formalisierungen?

Disjunktion: wie Konjunktion, oder durch Reduktion auf Konjunktion und Negation mittels Dualität von $\vee$ und $\wedge$. □

3.2 Substitution

Substitution ist eine syntaktische Operation für das Einsetzen eines Terms für eine freie Variable. Zu $\varphi(x)$ und Term t soll die neue Formel $\varphi(t/x)$ besagen, dass das von t beschriebene Element die Formel φ erfüllt, d.h. man will für alle Interpretationen $\mathfrak{I}$ haben:

$$\mathfrak{I} \models \varphi(t/x) \quad \Leftrightarrow \quad \mathfrak{I}[x \mapsto t^{\mathfrak{I}}] \models \varphi. \qquad (*)$$

Einfache syntaktische Ersetzung von x in φ durch t ist i.d.S. nicht immer korrekt:

– Man darf x nicht an Stellen ersetzen, wo es in φ gebunden auftritt.

Bsp.: In $\varphi(x) = Ux \wedge \exists x \neg Ux$ ist nur das erste x frei, das zweite gebunden. Für $t = c$ (eine Konstante) soll $\varphi(c/x) \equiv Uc \wedge \exists x \neg Ux$ sein.

– t kann selbst Variablen haben, die in φ gebunden werden.

Bsp.: In $\varphi(x) = \exists y Exy$ und für $t = fy$ soll $\varphi(fy/x) \equiv \exists z Efyz$ sein, und nicht etwa $\exists y Efyy$.

Die induktive Definition von $\varphi(t/x)$ umgeht diese Konflikte mit gebundenen Variablen durch systematische Umbenennung. Korrektheit im Sinne von $(*)$ lässt sich anhand dieser Definition induktiv beweisen.

Die Fälle von atomaren (oder allgemein quantorenfreien) φ sowie die Schritte für AL Junktoren sind trivial:

- (quantorenfreie φ, inbes. atomare): einfache Ersetzung jedes Vorkommens des Symbols x in φ durch t tut's.
- (Negation, Konjunktion, Disjunktion): trivial, z.B.:
  $(\neg\varphi)(t/x) := \neg(\varphi(t/x))$; $(\varphi_1 \wedge \varphi_2)(t/x) := \varphi_1(t/x) \wedge \varphi_2(t/x)$.

Es bleibt der Quantorenschritt: $\varphi = Qy\psi$, $Q \in \{\forall, \exists\}$; hier können wir induktiv auf bereits definierte $\xi(t'/x_i)$ für alle x_i, t und für alle ξ mit $\mathrm{qr}(\xi) \leqslant \mathrm{qr}(\psi)$ zurückgreifen!

- (Quantifizierung) $\varphi = Qy\psi$: Sei $i \geqslant 1$ minimal mit $x_i \notin \mathrm{var}(t) \cup \mathrm{var}(\varphi) \cup \{x\}$; sei $\hat{\psi} := \psi(x_i/y)$ (nach Induktionsvoraussetzung zu ψ).
  Wir setzen $\varphi(t/x) := Qx_i\big(\hat{\psi}(t/x)\big)$.

Die vorgeschaltete (innere) Substitution von x_i für y im Quantorenschritt vermeidet Konflikte zwischen der y-Quantifizierung und der Substitution von t für x auch für den Fall, dass $y \in \mathrm{var}(t)$.

Simultane Substitution von mehreren Variablen x_i durch Terme t_i funktioniert analog.

3.3 Skolemisierung

Beispiel 3.5 Der Satz $\psi = \forall x \exists y \varphi(x, y)$ verlangt, dass es zu jeder Belegung von x mindestens eine Belegung von y gibt, die φ wahr macht: ein Existenzbeispiel für y in Abhängigkeit von x. Man kann (in einer erweiterten Signatur) ein neues Funktionssymbol f (hier 1-stellig) dafür reservieren, ein Existenzbeispiel für y in Abhängigkeit von x auszuwählen:

$$\psi = \forall x \exists y \varphi(x, y) \text{ erfüllbar} \quad \Leftrightarrow \quad \psi' := \forall x \varphi(x, fx) \text{ erfüllbar.}$$

$\varphi(x, fx)$ steht für das Substitutionsergebnis $\varphi(fx/y)$. "$\Leftarrow$" ist offensichtlich. Für "$\Rightarrow$" nehmen wir an, dass $\mathcal{A} \models \forall x \exists y \varphi(x, y)$ ist. Sei dann $f^{\mathcal{A}} \colon A \to A$ so, dass für alle $a \in A$ gerade $f^{\mathcal{A}}(a) \in \{a' \in A \colon \mathcal{A} \models \varphi[a, a']\}$ ($\neq \emptyset$!). Dann ist $(\mathcal{A}, f^{\mathcal{A}}) \models \psi'$. Ein so gewähltes $f^{\mathcal{A}}$ heißt *Skolemfunktion*.

Im Falle einer Formel mit weiteren freien Variablen erhöht sich die Stelligkeit der Skolemfunktion entsprechend, da das Existenzbeispiel von der Belegung dieser anderen Variablen auch abhängen darf. Im Falle eines Satzes $\psi = \exists y \varphi(y)$ dagegen kommt man mit einer '0-stelligen Skolemfunktion' aus, d.h. mit einer Konstanten, die durch ein Existenzbeispiel zu interpretieren ist: $\psi = \exists y \varphi(y)$ ist erfüllbar gdw. $\psi' := \varphi(c/y)$ erfüllbar ist, wobei c ein neues, nicht in φ vorkommendes Konstantensymbol ist.

Beachte am Beispiel auch, dass die betrachteten Formeln nicht logisch äquivalent sind, sondern auf eine besondere Weise *erfüllbarkeitsäquivalent*: jedes Modell von ψ lässt sich zu einem Modell von ψ' (durch geeignete Interpretation der neuen Funktionssymbole) erweitern; und jedes Modell von ψ' ist automatisch Modell von ψ, d.h. $\psi' \models \psi$. Hinsichtlich der Definition von Erfüllbarkeitsäquivalenz vergleiche Definition 2.10.

Satz 3.6 (Skolemnormalform) *Jede Formel $\varphi \in \mathrm{FO}$ ist erfüllbarkeitsäquivalent zu einer universell-pränexen Formel*

$$\varphi' = \forall x_{i_1} \ldots \forall x_{i\ell}\, \xi$$

mit quantorenfreiem ξ (in einer erweiterten Signatur). Eine solche Formel φ' in Skolemnormalform *erhält man aus einer zu φ logisch äquivalenten Formel in pränexer Normalform durch Substitution von Skolemfunktionstermen für existentiell abquantifizierte Variablen. Hinsichtlich der Erfüllbarkeitsäquivalenz gilt sogar:*

(i) $\varphi' \models \varphi$.

(ii) *Jedes Modell von φ lässt sich durch geeignete Interpretation der (neuen) Skolemfunktionen zu einem Modell von φ' erweitern.*

Beweis Wir behandeln o.B.d.A. Formeln φ in pränexer Normalform der Gestalt $\varphi = Q_1 x_{i_k} \ldots Q_k x_{i_1}\ \psi(\mathbf{x})$ mit quantorenfreiem ψ. Für $\ell = 0, \ldots, k$ sei φ_ℓ die Subformel $\varphi_\ell := Q_1 x_{i_\ell} \ldots Q_k x_{i_1}\ \psi(\mathbf{x})$ von φ. Wir gehen induktiv von innen nach außen längs des Quantorenpräfixes vor und konstruieren φ'_ℓ zu φ_ℓ wie im Satz gefordert; für $\ell = k$ ist dann $\varphi' = \varphi'_k$ wie gewünscht.

Induktionsanfang, $\ell = 0$. $\varphi_0 = \psi$ ist quantorenfrei. Also tut's $\varphi'_0 := \varphi_0$.

Induktionsschritt von ℓ nach $\ell + 1$.

$\varphi_{\ell+1} = Q_{\ell+1} x_{i_{\ell+1}} \varphi_\ell$, und φ'_ℓ für φ_ℓ bereits wie gefordert. Falls $Q_{\ell+1} = \forall$, sei $\varphi'_{\ell+1} := \forall x_{i_{\ell+1}} \varphi'_\ell$.

Falls $Q_{\ell+1} = \exists$, sei $\varphi'_{\ell+1} := \varphi'_\ell(f\mathbf{x}/x_{i_{\ell+1}})$, wobei $\mathbf{x}$ das Tupel aller in $\varphi_{\ell+1}$ freien Variablen ist und f ein neues Funktionssymbol von dazu passender Stelligkeit. □

Beispiel 3.7 Betrachte in der Signatur $S = \{\circ, e\}$ mit 2-stelligem Funktionssymbol $\circ$ (infix notiert) und Konstantensymbol e eines der Gruppenaxiome, Existenz des Inversen (wenn e das neutrale Element ist):

$$\varphi = \forall x \exists y (x \circ y = e).$$

Eine Skolemfunktion f für "$\exists y \ldots$" führt zum erfüllbarkeitsäquivalenten Satz $\varphi' = \forall x (x \circ fx = e)$.

In einer Gruppe muss man das neue Funktionssymbol als die Operation der Inversenbildung interpretieren, um φ' wahr zu machen, z.B. in der additiven Gruppe der ganzen Zahlen, $\mathcal{Z} = (\mathbb{Z}, +, 0)$, ist $f^{\mathcal{Z}}(m) := -m$ die gewünschte Interpretation. [Man hat in einer Gruppe keine Wahlmöglichkeiten für die Interpretation von f, da die Inversen eindeutig bestimmt sind.] In Modellen von φ, die keine Gruppen sind (φ ist nur eines von mehreren notwendigen Gruppenaxiomen), kann es dagegen viele zulässige Interpretationen für f geben. Betrachte z.B. $\mathcal{A} = (\mathbb{N}, \circ^{\mathcal{A}}, 0)$ wo $\circ^{\mathcal{A}}$ als Multiplikation modulo 2 interpretiert ist. Hier kann man für $f^{\mathcal{A}}$ irgendeine Funktion nehmen, die jeder ungeraden Zahl eine gerade Zahl zuordnet.

Bem.: Im Falle von pränexen Sätzen überlege man sich, dass man Skolemfunktionen für alle existenziell abquantifizierten Variablen so ansetzen kann, dass jede nur abhängig ist von den weiter aussen universell abquantifizierten Variablen (d.h. man kann ggf. mit niedrigeren Stelligkeiten auskommen). Z.B. ist $\psi = \exists x \forall y \exists z \varphi(x, y, z)$ erfüllbarkeitsäquivalent mit $\psi' = \forall y \varphi(c/x, y, f(y)/z)$ für neue Konstante c und 1-stellige Skolemfunktion f (die allerdings dann passend zu c interpretiert werden muss!).

Bem.: Man kann Skolemfunktionen auch in Formeln, die nicht in pränexer Normalform gegeben sind, direkt einführen, und anschließend in pränexe Normalform transformieren. Das ist i.d.R. sogar sparsamer als die umgekehrte Reihenfolge. Warum?

Bem.: Skolemfunktionen entsprechen Anweisungen für $\exists$-Züge von $\mathbf{V}$ im Semantikspiel. Wenn die Formel wahr ist, d.h., wenn $\mathbf{V}$ eine Gewinnstrategie hat, dann kann sie in allen Spielpositionen, in denen sie ein Existenzbeispiel wählen muss, stets den Wert der entsprechenden Skolemfunktion wählen. Umgekehrt entspricht jeder Gewinnstrategie für $\mathbf{V}$ für diese Spielsituationen, die eine eindeutige Auswahl vorgibt, eine Skolemfunktion.

3.4 Satz von Herbrand

Wir behandeln die Erfüllbarkeit von universellen, gleichheitsfreien Sätzen. Aus dem letzten Abschnitt wissen wir, dass wir die Frage nach der Erfüllbarkeit von beliebigen Sätzen und Satzmengen stets auf die Erfüllbarkeit von universell-pränexen Sätzen und Satzmengen reduzieren können (Skolemisierung). Gleichheitsfreiheit lässt sich auf dem Umweg über eine explizite Modellierung durch eine Äquivalenzrelation wie in Bemerkung 2.13 erreichen. Im Kern haben wir also das Erfüllbarkeitsproblem für beliebige Satzmengen im Griff, wenn wir universelle gleichheitsfreie Sätze und Satzmengen behandeln können.

Der *Satz von Herbrand* gibt uns hier Modelle, deren Trägermenge auf besonders einfache Weise durch Terme beschrieben wird. Kurz: Jede erfüllbare Menge von universellen, gleichheitsfreien Sätzen hat ein Modell, das auf der zugehörigen Termstruktur aufgebaut ist (siehe Seite 5), ein *Herbrand-Modell*.

Erinnerung: $\mathrm{FO}^{\neq}$ steht für die Logik erster Stufe ohne Gleichheit. O.B.d.A. enthalte die Signatur S mindestens ein Konstantensymbol. Dann bildet $T_0(S)$, die Menge der variablenfreien S-Terme, eine S_{F}-Struktur $\mathcal{T}_0(S)$ (Termstrukturen: Seite 5). Eine Erweiterung dieser funktionalen Termstruktur zu einer S-Struktur $\mathcal{H} = \big(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R\in S}\big)$ mit Interpretationen $R^{\mathcal{H}}$ für die Relationssymbole R in S heißt *Herbrand-Struktur*.

Definition 3.8 Eine Formel ist *universell* wenn sie aus atomaren und negiert atomaren Formeln allein mittels $\wedge, \vee$ und $\forall$-Quantoren aufgebaut ist.

Übung 3.9 Zeigen Sie: Jede universelle Formel ist logisch äquivalent ist zu einer universell-pränexen Formel (also in Skolemnormalform).

Satz 3.10 (Herbrand) *Sei $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ eine Menge von universellen, gleichheitsfreien Sätzen. Dann sind äquivalent:*

(i) *Φ erfüllbar.*

(ii) *Φ hat ein Herbrand-Modell $\mathcal{H} = \big(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R\in S}\big) \models \Phi$, dessen Trägermenge und Funktions- und Konstanteninterpretationen mit der Termstruktur $\mathcal{T}_0(S)$ übereinstimmen ($\mathcal{H}$ erweitert die S_{F}-Struktur $\mathcal{T}_0(S)$ lediglich um eine geeignete Interpretation der Relationssymbole in S).*

Beweis (ii) $\Rightarrow$ (i) ist offensichtlich. Wir zeigen (i) $\Rightarrow$ (ii).

Sei $\mathcal{A} \models \Phi$ irgendein Modell von Φ. Wir interpretieren Relationssymbole $R \in S$ über $\mathcal{H}$ anhand von $\mathcal{A}$, wie folgt. Ist R n-stellig, so sei

$$R^{\mathcal{H}} := \big\{(t_1, \ldots, t_n) \in (T_0(S))^n \colon (t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}) \in R^{\mathcal{A}}\big\}.$$

[Erinnerung: $t_i^{\mathcal{A}}$ ist die Interpretation von t_i in $\mathcal{A}$; wohldefiniert auch ohne Belegung, da die t_i variablenfrei sind.]

Für die so vollständig definierte Struktur $\mathcal{H} = \big(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R\in S}\big)$ zeigen wir, dass $\mathcal{H} \models \Phi$.

Dafür zeigen wir durch Induktion über den Aufbau beliebiger universeller Formeln $\varphi(x_1, \ldots, x_n) \in \mathrm{FO}^{\neq}(S)$, dass für alle $(t_1, \ldots, t_n) \in (T_0(S))^n$ gilt:

$$\mathcal{A} \models \varphi\big[t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}\big] \quad \Rightarrow \quad \mathcal{H} \models \varphi\big[t_1, \ldots, t_n\big]. \qquad (*)$$

Daraus folgt dann $\mathcal{H} \models \Phi$, da $\mathcal{A} \models \Phi$.

Zum induktiven Beweis von $(*)$:

Induktionsanfang: atomare bzw. negiert atomare (gleichheitsfreie!) Formeln sind von der Gestalt $(\neg)Rt_1 \ldots t_n$ und die Definition der $R^{\mathcal{H}}$ ist gerade so, dass $(*)$ gilt.

Die Induktionsschritte für die AL-Junktoren $\wedge$ und $\vee$ sind trivial.

Es bleibt der universelle Quantorenschritt:

Sei etwa $\varphi(x_1, \ldots, x_n) = \forall x_{n+1}\psi(x_1, \ldots, x_{n+1})$ und die Behauptung gelte für ψ.

Dann gilt

$$\begin{aligned}
& \mathcal{A} \models \varphi\big[t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}\big] \\
\Rightarrow\ & \text{f.a. } t \in T_0(S) \text{ gilt: } \mathcal{A} \models \psi\big[t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}, t^{\mathcal{A}}\big] \\
\Rightarrow\ & \text{f.a. } t \in T_0(S) \text{ gilt: } \mathcal{H} \models \psi\big[t_1, \ldots, t_n, t\big] && \text{(Ind.-Ann. für } \psi) \\
\Rightarrow\ & \mathcal{H} \models \varphi\big[t_1, \ldots, t_n\big]. && \text{(der Träger von } \mathcal{H} \text{ ist } T_0(S))
\end{aligned}$$

□

3.5 Erfüllbarkeit: Reduktion von FO auf AL

Wir reduzieren die Frage ob eine (endliche oder unendliche) Satzmenge erfüllbar ist auf das AL Erfüllbarkeitsproblem. Diese Reduktion liefert insbesondere den Kompaktheitssatz (Endlichkeitssatz) für FO, durch Übertragung des Kompaktheitssatzes für AL.

Betrachten wir zunächst eine beliebige Menge von Formeln $\Phi \subseteq \mathrm{FO}(S)$. Für Erfüllbarkeitsfragen können wir o.B.d.A. annehmen, dass

- $\Phi \subseteq \mathrm{FO}_0(S)$ eine Satzmenge (ohne freie Variablen) ist. Man erhält eine zu einer Formelmenge erfüllbarkeitsäquivalente Satzmenge, indem man neue Konstantensymbole für alle freien Variablen substituiert. (Warum?)
- $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ gleichheitsfrei ist. Eine explizite Modellierung der Gleichheitsrelation durch eine zusätzliche Äquivalenzrelation (siehe Bemerkung 2.13) führt zu erfüllbarkeitsäquivalenten Satzmengen ohne Gleichheit.
- $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ aus universell-pränexen, gleichheitsfreien Sätzen besteht. Skolemisierung liefert eine erfüllbarkeitsäquivalente Satzmenge in universell-pränexer Form.
- S mindestens ein Konstantensymbol enthält, sodass $T_0(S) \neq \emptyset$ ist, und wir uns ggf. auf Herbrand-Modelle von $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ zurückziehen können.

In diesem Sinne o.B.d.A., arbeiten wir im Folgenden mit einer Menge $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ von *universell-pränexen, gleichheitsfreien Sätzen* über einer Symbolmenge mit Konstantensymbolen. Aus dem Satz von Herbrand folgt dann, dass

$$\Phi \text{ erfüllbar} \quad \Leftrightarrow \quad \mathcal{H} \models \Phi \text{ für eine Herbrand-Struktur } \mathcal{H} = \big(\mathcal{T}_0(S), (R^{\mathcal{H}})_{R\in S}\big).$$

Die möglichen Herbrand-Strukturen unterscheiden sich nur hinsichtlich der Interpretationen der verschiedenen Möglichkeiten, jedes einzelne Relationssymbol $R \in S$ als Relation über $T_0(S)$ zu interpretieren.

Das heißt, dass man für jedes n-stellige $R \in S$ bestimmen muss, welche variablenfreien atomaren Formeln (Sätze!) $\alpha = Rt_1 \dots t_n$ wahr sind und welche falsch, für $t_1, \dots, t_n \in T_0(S)$. Man hat daher eine ein-eindeutige Korrespondenz zwischen Herbrand-Strukturen $\mathcal{H}$ und Auswahlen von Wahrheitswerten p_α für sämtliche variablenfreien atomaren α. Mit

$$\mathcal{V} := \{p_\alpha \colon \alpha = Rt_1 \dots t_n; R \in S; t_1, \dots, t_n \in T_0(S) \text{ für } n\text{-stelliges } R\}$$

beschreiben die (aussagenlogischen) $\mathcal{V}$-Interpretationen also genau die zulässigen Herbrand-Strukturen. Zur $\mathcal{V}$-Interpretation $\mathfrak{I}$ gehört die Herbrand-Struktur $\mathcal{H} = \mathcal{H}(\mathfrak{I})$ mit

$$R^{\mathcal{H}} = \big\{(t_1, \dots, t_n) \in T_0(S)^n \colon \mathfrak{I}(p_{\mathtt{Rt_1 \dots t_n}}) = 1\big\}.$$

Umgekehrt erhalten wir als AL-Beschreibung einer gegebenen Herbrand-Struktur $\mathcal{H}$ die $\mathcal{V}$-Interpretation $\mathfrak{I} = \mathfrak{I}(\mathcal{H})$ als

$$\begin{array}{rcl} \mathfrak{I} \colon \mathcal{V} & \longrightarrow & \mathbb{B} \\ p_\alpha & \longmapsto & \begin{cases} 1 & \text{falls } \mathcal{H} \models \alpha, \\ 0 & \text{falls } \mathcal{H} \models \neg\alpha. \end{cases} \end{array}$$

Übung 3.11 Warum ist es für die obige Argumentation wichtig, dass in Φ keine Gleichheiten vorkommen? Was geht sonst schief?

Wann erfüllt $\mathcal{H} = \mathcal{H}(\mathfrak{I})$ den universell-pränexen Satz $\varphi = \forall x_1 \ldots \forall x_k \xi(x_1, \ldots, x_k)$ mit quantorenfreiem ξ? Offenbar genau dann, wenn für jedes k-Tupel von Termen $\mathbf{t} = (t_1, \ldots, t_k) \in T_0(S)^k$ gilt, dass $\mathcal{H} \models \xi(t_1/x_1, \ldots, t_k/x_k)$.

Zu jedem solchen variablenfreien, quantorenfreien $\xi(\mathbf{t}) = \xi(t_1/x_1, t_k/x_k)$ sei $\xi(\mathbf{t})^{\mathrm{AL}}$ die AL($\mathcal{V}$)-Formel, die man aus $\xi(\mathbf{t})$ erhält, indem man jedes relationale Atom $\alpha = R\ldots$ durch die AL-Variable $p_\alpha = p_{\mathtt{R}\ldots}$ ersetzt. Z.B. erhält man so zu

$$\xi = Rxfy \vee (Ufx \to Wxyfz)$$

für die Substitution von Termen (c, fc, d) für (x, y, z) die AL-Formel

$$\xi(c, fc, d)^{\mathrm{AL}} = p_{\mathtt{Rcffc}} \vee (p_{\mathtt{Ufc}} \to p_{\mathtt{Wcfcfd}}).$$

Zu $\varphi = \forall x_1 \ldots \forall x_k \xi(x_1, \ldots, x_k)$ sei dann $[\![\varphi]\!]^{\mathrm{AL}} := \{\xi(\mathbf{t})^{\mathrm{AL}} \colon \mathbf{t} \in T_0(S)^k\}$.
Die Menge $[\![\varphi]\!]^{\mathrm{AL}}$ ist i.d.R. unendlich.
Die Satzmenge Φ übersetzen wir entsprechend in

$$[\![\Phi]\!]^{\mathrm{AL}} := \bigcup_{\varphi \in \Phi} [\![\varphi]\!]^{\mathrm{AL}} \subseteq \mathrm{AL}(\mathcal{V}).$$

Lemma 3.12 *Sei $\Phi \subseteq \mathrm{FO}_0^{\neq}(S)$ eine Menge von universell-pränexen Sätzen. Dann sind äquivalent:*

(i) Φ *erfüllbar.*

(ii) $[\![\Phi]\!]^{\mathrm{AL}}$ *erfüllbar.*

Beweis (i) $\Rightarrow$ (ii). Sei Φ erfüllbar. Dann hat Φ ein Herbrand-Modell $\mathcal{H} \models \Phi$ und die zugehörige $\mathcal{V}$-Interpretation $\mathfrak{I} = \mathfrak{I}(\mathcal{H})$ erfüllt $[\![\Phi]\!]^{\mathrm{AL}}$.

(ii) $\Rightarrow$ (i). Sei $[\![\Phi]\!]^{\mathrm{AL}}$ erfüllbar, also $\mathfrak{I} \models [\![\Phi]\!]^{\mathrm{AL}}$ für eine $\mathcal{V}$-Interpretation $\mathfrak{I}$. Mit $\mathcal{H} = \mathcal{H}(\mathfrak{I})$ haben wir eine Herbrand-Struktur, die für jedes $\varphi = \forall x_1 \ldots \forall x_k \xi(x_1, \ldots, x_k) \in \Phi$ alle zugehörigen $\xi(\mathbf{t})$ erfüllt. Demnach gilt $\mathcal{H} \models \varphi$. Also $\mathcal{H} \models \Phi$. □

Übung 3.13 Warum folgt aus der bewiesenen Reduktion *nicht*, dass das Erfüllbarkeitsproblem (für universell-pränexe, gleichheitsfreie) FO-Sätze entscheidbar wäre?
(Wir werden später sehen, dass SAT(FO) unentscheidbar ist (Abschnitt 7); SAT(AL) aber ist entscheidbar.)

Beispiel 3.14 Wir betrachten zur Signatur $S = \{R, Q, f\}$ mit Relationssymbolen R (2-stellig) und Q (1-stellig) und Funktionssymbol f (1-stellig) die universellen, gleichheitsfreien Sätze

$$\begin{aligned}
\varphi_1 &= \forall x \forall y \big(Rxy \to (Qx \leftrightarrow \neg Qy)\big),\\
\varphi_2 &= \forall x (Rxfx \vee Rfxx),\\
\varphi_3 &= \forall x \forall y \big(\neg Rxy \to Rxffy\big).
\end{aligned}$$

Behauptung: $\Phi = \{\varphi_1, \varphi_2, \varphi_3\}$ ist unerfüllbar. Für die Reduktion auf AL brauchen wir ein Konstantensymbol, und nehmen daher eine Konstante c hinzu, $S_c := S \cup \{c\}$. Die Trägermenge einer Herbrand-Struktur zu S_c ist $T_0(S_c) = \{c, fc, ffc, fffc, \ldots\} = \{f^n c \colon n \in \mathbb{N}\}$, wenn wie wie üblich $f^0 c$ als Schreibweise für den Term c ansehen und induktiv $f^{n+1}c := ff^n c$ definieren. Als AL-Variablen benutzen wir für die Reduktion:

$$\begin{array}{lll}
q_n \quad (= p_{\mathtt{Qf^nc}}) & \text{für die Atome } Qf^n c, & (n \in \mathbb{N}),\\
r_{\ell,m} \quad (= p_{\mathtt{Rf^\ell cf^mc}}) & \text{für die Atome } Rf^\ell c f^m c, & (\ell, m \in \mathbb{N}).
\end{array}$$

Aus den φ_i erhalten wir so die Mengen

$$\begin{aligned}
[\![\varphi_1]\!]^{\mathrm{AL}} &= \big\{r_{\ell,m} \to (q_\ell \leftrightarrow \neg q_m) : \ell, m \in \mathbb{N}\big\},\\
[\![\varphi_2]\!]^{\mathrm{AL}} &= \big\{r_{\ell,\ell+1} \vee r_{\ell+1,\ell} : \ell \in \mathbb{N}\big\},\\
[\![\varphi_3]\!]^{\mathrm{AL}} &= \big\{\neg r_{\ell,m} \to r_{\ell,m+2} : \ell, m \in \mathbb{N}\big\}.
\end{aligned}$$

Bereits die folgende Auswahl aus $[\![\varphi_1]\!]^{\mathrm{AL}} \cup [\![\varphi_2]\!]^{\mathrm{AL}} \cup [\![\varphi_3]\!]^{\mathrm{AL}}$ ist aber nicht simultan erfüllbar (nachprüfen!):

$$\begin{array}{l}
r_{0,0} \to (q_0 \leftrightarrow \neg q_0),\\
r_{0,1} \to (q_0 \leftrightarrow \neg q_1),\\
r_{1,0} \to (q_1 \leftrightarrow \neg q_0),\\
r_{0,2} \to (q_0 \leftrightarrow \neg q_2),\\
r_{1,2} \to (q_1 \leftrightarrow \neg q_2),\ r_{0,1} \vee r_{1,0},\\
\underbrace{r_{2,1} \to (q_2 \leftrightarrow \neg q_1),}_{\in [\![\varphi_1]\!]^{\mathrm{AL}}}\ \underbrace{r_{1,2} \vee r_{2,1},}_{\in [\![\varphi_2]\!]^{\mathrm{AL}}}\ \underbrace{\neg r_{0,0} \to r_{0,2}}_{\in [\![\varphi_3]\!]^{\mathrm{AL}}}.
\end{array}$$

Das Beispiel zeigt, wie sich die Unerfüllbarkeit in einer endlichen Teilmenge der AL-Übersetzung manifestiert. Nach dem Kompaktheitssatz der AL muss das stets so sein. Tatsächlich erhalten wir daraus den Kompaktheitssatz für FO.

4 Kompaktheitssatz (Endlichkeitssatz)

Aus dem Reduktionsansatz des vorigen Abschnitts erhalten wir einen Beweis des wichtigsten modelltheoretischen Satzes über die Logik erster Stufe.

Satz 4.1 (Kompaktheitssatz) *Für jede Formelmenge $\Phi \subseteq \mathrm{FO}$ sind äquivalent:*

(i) Φ *erfüllbar.*

(ii) *Jede endliche Teilemenge $\Phi_0 \subseteq \Phi$ ist erfüllbar.*

Eine äquivalente und nützliche Variante für die Folgerungsbeziehung:

Korollar 4.2 *Für jede Formelmenge $\Phi \subseteq \mathrm{FO}$ und Formel $\psi \in \mathrm{FO}$ sind äquivalent:*

(i) $\Phi \models \psi$.

(ii) *Es existiert eine endliche Teilemenge $\Phi_0 \subseteq \Phi$, sodass $\Phi_0 \models \psi$.*

Das Korollar folgt aus dem Satz über den Zusammenhang (vgl. Übung 4.3 zur AL):

$$\Phi \models \varphi \quad \text{gdw.} \quad \Phi \cup \{\neg\varphi\} \text{ unerfüllbar.}$$

Beweis (des Satzes) (i) $\Rightarrow$ (ii) ist trivial. Die interessante Aussage ist (ii) $\Rightarrow$ (i): Allein aus der Erfüllbarkeit aller endlichen Teilmengen lässt sich schließen, dass die ganze Menge erfüllbar ist.

Im Falle einer universell-pränexen, gleichheitsfreien Satzmenge $\Phi \subseteq \mathrm{FO}_0^{\neq}$, folgt die Aussage des Satzes direkt mit Lemma 3.12 aus dem AL Kompaktheitssatz. Es ist

$$\begin{array}{lll}
& \Phi \text{ erfüllbar} & \\
\Leftrightarrow & [\![\Phi]\!]^{\mathrm{AL}} \text{ erfüllbar} & \text{(Lemma 3.12)}\\
\Leftrightarrow & \text{jede endliche Teilmenge von } [\![\Phi]\!]^{\mathrm{AL}} \text{ ist erfüllbar.} & \text{(AL Kompaktheit)}
\end{array}$$

Ist nun jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar, so sind mit Lemma 3.12 also die zughörigen $[\![\Phi_0]\!]^{\mathrm{AL}}$ erfüllbar. Da jede endliche Teilmenge von $[\![\Phi]\!]^{\mathrm{AL}}$ in einem $[\![\Phi_0]\!]^{\mathrm{AL}}$ für endliches $\Phi_0 \subseteq \Phi$ enthalten ist, folgt mit der obigen Äquivalenz die Erfüllbarkeit von Φ.

Die Verallgemeinerung für FO (mit Gleichheit) ergibt sich mit der Idee aus Abschnitt 2.5.

Die Verallgemeinerung von Satzmengen auf Formelmengen (mit freien Variablen) ergibt sich über eine Reduktion, die die freien Variablen durch neue Konstantensymbole ersetzt. Man überlegt sich, dass dieser Prozess zu einer erfüllbarkeitsäquivalenten Satzmenge führt. □

Bem.: Wir werden einen alternativen (und methodisch interessanteren) Zugang zum Kompaktheitssatz über einen vollständigen Beweiskalkül für FO (Gödelscher Vollständigkeitssatz) kennenlernen.

Konsequenzen des Kompaktheitssatzes Ein Beispiel für die Stärke des Kompaktheitssatzes ist die Existenz sogenannter *Nichtstandardmodelle*. Ein Nichtstandardmodell der Arithmetik z.B. ist eine Struktur $\mathcal{N}^* = (\mathbb{N}^*, +^*, \cdot^*, 0^*, 1^*, <^*)$ die genau dieselben $\mathrm{FO}(\{+, \cdot, 0, 1, <\})$-Sätze erfüllt wie das Standardmodell $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$, aber nicht isomorph dazu ist. D.h., dass $\mathcal{N}^*$ und $\mathcal{N}$ zwar im Rahmen von $\mathrm{FO}(\{+, \cdot, 0, 1, <\})$ völlig ununterscheidbar sind, aber doch wesentlich verschieden. Also sind wesentliche Eigenschaften der Struktur $\mathcal{N}$ nicht in $\mathrm{FO}(\{+, \cdot, 0, 1, <\})$ fassbar. Das gleiche gilt für jede unendliche Struktur, und man macht sich die Existenz etwa von Nichtstandardmodellen zur reellen Arithmetik in der sogenannten Nichtstandardanalysis zunutze. Wir zeigen hier kurz, wie man aus dem Kompaktheitssatz schließt, dass es Nichtstandardmodelle $\mathcal{N}^*$ zu $\mathcal{N}$ gibt.

Beispiel 4.3 Sei $S = \{+, \cdot, 0, 1, <\}$ die übliche Signatur der Arithmetik, $\mathcal{N}$ das Standardmodell der Arithmetik über den natürlichen Zahlen. Man beachte, dass jedes Element der Standardstruktur, also jedes $n \in \mathbb{N}$, gerade die Interpretation eines zugehörigen variablenfreien S-Terms t_n ist. Für $n = 0, 1$ haben wir die Konstantensymbole 0 und 1 als t_0 und t_1; für $n > 1$ sei $t_n := \underbrace{1 + \cdots + 1}_{n\text{-mal}}$.

Sei $\varphi_n(x)$ die $\mathrm{FO}(S)$-Formel $\varphi_n(x) := t_n < x$ und Φ die unendliche Formelmenge

$$\Phi := \big\{\varphi \in \mathrm{FO}_0(S) \colon \mathcal{N} \models \varphi\big\} \cup \big\{\varphi_n < x \colon n \in \mathbb{N}\big\}.$$

Φ ist erfüllbar: Jedes endliche $\Phi_0 \subseteq \Phi$ enthält nur endlich viele der $\varphi_n(x)$ und wir finden im Standardmodell $\mathcal{N}$ eine Belegung für x, die groß genug ist um diese endlich vielen Forderungen wahr zu machen. Also ist Φ erfüllbar (Kompaktheitssatz).

Jedes Modell von Φ muss

(a) alle $\mathrm{FO}(S)$-Sätze erfüllen, die im Standardmodell gelten (also genau dieselben $\mathrm{FO}(S)$-Sätze wie $\mathcal{N}$).

(b) für die Belegung der Variablen x ein Element besitzen, dass im Sinne der Ordnung $<$ größer als alle t_n ist; also so etwas wie eine "unendliche natürliche Zahl".

Aus (b) folgt insbesondere, dass jede so gewonnene S-Struktur nicht zum Standardmodell isomorph sein kann, aber wegen (a) vom Standardmodell bezüglich aller $\mathrm{FO}(S)$-Sätze ununterscheidbar ist.

Bem.: Um unendliche Strukturen wie $\mathcal{N}$ axiomatisch bis auf Isomorphie zu charakterisieren braucht man mehr als $\mathrm{FO}(S)$. In diesem Fall benutzt die natürliche Axiomatisierung,

zusätzlich zu FO(S)-Sätzen, auch eine Aussage über Teilmengen der Trägermenge. Das entscheidende Axiom ist eine Umschreibung des *Induktionsprinzips für* $\mathbb{N}$, etwa in der Fassung, dass jede nicht-leere Teilmenge des Trägers ein kleinstes Element besitzt (vgl. Rechtfertigung von Induktionsbeweisen in FG I). (Man kann sich überlegen, dass keines der oben gewonnenen Nichtstandardmodelle diese Eigenschaft hat). Solche Quantifizierung über Teilmengen ist in der *monadischen Logik zweiter Stufe* MSO möglich (die auch interessante Anwendungen in der Informatik hat).

5 Resolution

Wir verknüpfen die Reduktion von FO nach AL mit dem für AL korrekten und vollständigen Resolutionskalkül. Man erhält einen Refutationskalkül (Unerfüllbarkeitsbeweise), der für Unerfüllbarkeit von *universellen-pränexen, gleichheitsfreien Satzmengen* korrekt und vollständig ist.

Der AL Resolutionskalkül arbeitet mit Klauselmengen; es ist leicht, die Skolemnormalform an dieses Format anzupassen.

Wir arbeiten mit Sätzen und nicht mit Formeln mit freien Variablen. Die Einschränkung ist unproblematisch, da man – bis auf Erfüllbarkeitsäquivalenz – stets neue Konstantensymbole für freie Variablen einsetzen kann.

5.1 Skolemnormalform in Klauselform

Aus Satz 3.6 (Skolemnormalform) erhalten wir zu Sätzen $\varphi \in \mathrm{FO}_0^{\neq}(S)$ erfüllbarkeitsäquivalente Sätze φ' in universell-pränexer Form. Ein typischer universell-pränexer Satz hat die Form

$$\forall x_1 \ldots \forall x_n \, \xi(x_1, \ldots, x_n),$$

wobei $\xi \in \mathrm{FO}_n^{\neq}(S)$ quantorenfrei ist, d.h. eine rein aussagenlogische Kombination von relationalen Atomen $\alpha = R\mathbf{t}$ mit Relationssymbolen $R \in S$ und Tupeln von Termen $t_i \in T_n(S)$ (in Variablen $x_1, \ldots, x_n$). Seien $\alpha_1, \ldots, \alpha_m$ die in ξ auftretenden Atome. Wenn man, wie in Abschnitt 3.5, die α_j wie AL-Variablen behandelt, kann man ξ als Formel in $\mathrm{AL}(\{\alpha_1, \ldots, \alpha_m\})$ auffassen und in logisch äquivalente KNF bzw. Klauselform bringen.

Definition 5.1 Ein $\mathrm{FO}^{\neq}(S)$-*Literal* ist eine atomare oder negiert atomare $\mathrm{FO}^{\neq}(S)$-Formel $\lambda = \alpha$ oder $\lambda = \neg\alpha$, α ein relationales Atom der Form $\alpha = Rt_1 \ldots t_r$ (wobei $R \in S$ und $t_i \in T(S)$ für $i = 1, \ldots, r$ wenn R r-stellig ist).

Eine $\mathrm{FO}^{\neq}(S)$-*Klausel* C ist eine endliche Menge von $\mathrm{FO}^{\neq}(S)$-Literalen, die wir logisch mit der Disjunktion $\bigvee C$ ihrer Literale identifizieren.

Eine $\mathrm{FO}^{\neq}(S)$-*Klauselmenge* K ist eine Menge von $\mathrm{FO}^{\neq}(S)$-Klauseln. Endliche Klauselmengen K identifizieren wir logisch mit der Konjunktion $\bigwedge_{C \in K} \bigvee C$.

Mit einer $\mathrm{FO}^{\neq}(S)$-Klausel C assoziieren wir den *universell-pränexen* $\mathrm{FO}^{\neq}(S)$-*Satz*, den wir aus C durch universelles Abquantifizieren *aller* in $\bigwedge C$ vorkommenden Variablen erhalten ($\mathbf{x}$ sei das Tupel dieser Variablen, $\forall\mathbf{x}$ kurz für den $\forall$-Präfix zu den x in $\mathbf{x}$):

$$C \equiv \forall\mathbf{x} \bigvee C \quad \in \mathrm{FO}_0^{\neq}(S).$$

Mit einer Klauselmenge K assoziieren wir analog die Menge der $\mathrm{FO}^{\neq}(S)$-Sätze, die man als universell pränexe Abquantifizierungen aller Klauseln von K erhält:

$$K \equiv \{\forall\mathbf{x} \bigvee C \colon\ C \in K\} \quad \subseteq \mathrm{FO}_0^{\neq}.$$

In disem Sinne wenden wir logische Begriffe wie *Erfüllbarkeit* auf Klauseln und Klauselmengen an.

Einer endliche Klauselmenge K ist logisch äquivalent zu den $\mathrm{FO}^{\neq}(S)$-Sätzen

$$K \equiv \forall \mathbf{x} \bigwedge_{j=1}^{k} \bigvee C_j \equiv \bigwedge_{j=1}^{k} \forall \mathbf{x} \bigvee C_j \quad \in \mathrm{FO}_0^{\neq}(S).$$

Wir betrachten die endliche Klauselmenge K als eine Darstellung des Satzes φ *in Klauselform* wenn $\varphi \equiv K$. Mit dem, was wir über KNF und Klauselform in AL wissen, ist klar, dass jeder universell-pränexe $\mathrm{FO}^{\neq}(S)$-Satz in Klauselform darstellbar ist.

Beispiel 5.2 Für den universell-pränexen Satz $\varphi = \forall x \forall y \big(Rxy \to (Qx \leftrightarrow \neg Qy)\big)$ (das ist φ_1 aus Beispiel 3.14) sind die relevanten Atome $\alpha = Rxy$, $\beta_1 = Qx$ und $\beta_2 = Qy$.

Eine mögliche KNF-Formalisierung des quantorenfreien Kerns von φ_1 bzgl. dieser Atome ist etwa $(\neg\alpha \vee \beta_1 \vee \neg\beta_1) \wedge (\neg\alpha \vee \beta_1 \vee \beta_2) \wedge (\neg\alpha \vee \neg\beta_2 \vee \neg\beta_1) \wedge (\neg\alpha \vee \neg\beta_2 \vee \beta_2)$, wobei man das erste und das letzte Konjunktionsglied weglassen kann, da beide allgemeingültig sind. In Klauselform entspricht das Ergebnis der Klauselmenge

$$K(\varphi) = \big\{\{\neg\alpha, \beta_1, \beta_2\}, \{\neg\alpha, \neg\beta_1, \neg\beta_2\}\big\} = \big\{\{\neg Rxy, Qx, Qy\}, \{\neg Rxy, \neg Qy, \neg Qx\}\big\}.$$

5.2 Grundinstanzen-Resolution

S sei eine Signatur mit mindestens einem Konstantensymbol, sodass $T_0(S) \neq \emptyset$.

Man erhält eine *Grundinstanz* (GI) einer $\mathrm{FO}^{\neq}(S)$-Klausel C indem man simultan in allen Literalen $\lambda \in C$ jede vorkommende Variable x_i durch einen *variablenfreien* Term $t_i \in T_0(S)$ ersetzt (jedes Vorkommen von x_i durch denselben Term t_i, aber beliebige Wahl der $t_i \in T_0(S)$).

Definition 5.3 Zu einer $\mathrm{FO}^{\neq}(S)$-Klausel C über Literalen $\lambda \in \mathrm{FO}_n^{\neq}(S)$ (d.h. mit Variablen unter $x_1, \ldots, x_n$) und variablenfreien Termen $t_1, \ldots, t_n \in T_0(S)$ ist

$$C(t_1/x_1, \ldots, t_n/x_n) := \{\lambda(t_1/x_1, \ldots, t_n/x_n) \colon \lambda \in C\}$$

eine *Grundinstanz* (GI) von C. Zu einer Klauselmenge K erhält man die Menge aller ihrer Grundinstanzen indem man alle Grundinstanzen aller Klauseln $C \in K$ zusammenfasst:

$$\mathrm{GI}(K) := \big\{C(t_1/x_1, \ldots) \colon C \in K, t_i \in T_0(S)\big\}.$$

Beobachtung 5.4 Offenbar ist $K \models \mathrm{GI}(K)$, da eine universell-pränexe Formel jede Substitutionsinstanz ihres quantorenfreien Kerns impliziert. Andererseits liefert jedes Modell von $\mathrm{GI}(K)$ ein Herbrand-Modell für K. K und $\mathrm{GI}(K)$ sind erfüllbarkeitsäquivalent.

GI-Resolution ist ganz analog zur AL-Resolution definiert, nur dass anstelle der Literale der AL (AL-Variabeln und negierte AL-Variablen) jetzt die variablenfreien $\mathrm{FO}^{\neq}(S)$-Literale treten. Wir schreiben $\overline{\lambda}$ für das Literal, das zu $\neg\lambda$ logisch äquivalent ist.

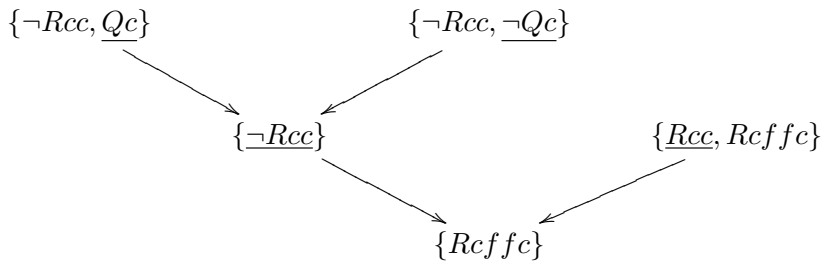
Definition 5.5 [GI-Resolution] Für Klauseln C_1, C_2, C von variablenfreien $\mathrm{FO}^{\neq}(S)$-Literalen ist C eine *Resolvente* von C_1 und C_2 bezüglich des Literals λ, wenn

$$\lambda \in C_1, \quad \overline{\lambda} \in C_2, \quad \text{und } C = (C_1 \setminus \{\lambda\}) \cup (C_2 \setminus \{\overline{\lambda}\}).$$

Wir sagen, dass C aus C_1 und C_2 in einem Resolutionsschritt ableitbar ist.

Für eine Klauselmenge K über variablenfreien $\mathrm{FO}^{\neq}(S)$-Literalen sei $\mathrm{Res}^*(K)$ der Abschluß von K unter Hinzunahme von Resolventen (d.h. K zusammen mit allen Klauseln, die man aus Klauseln in K durch iterierte Resolutionsschritte gewinnen kann).

Zwei typische Resolutionsschritte in diesem Sinne, über Klauseln aus der Menge der Grundinstanzen von $\{\neg Rxy, Qx, Qy\}$, $\{\neg Rxy, \neg Qx, \neg Qy\}$ und $\{Rxx, Rxfffx\}$:



Man überlegt sich, dass tatsächlich gilt

$$\left.\begin{array}{c}\forall x\forall y\big(\neg Rxy \vee Qx \vee Qy\big)\\ \forall x\forall y\big(\neg Rxy \vee \neg Qx \vee \neg Qy\big)\\ \forall x\big(Rxx \vee Rxfffx\big)\end{array}\right\} \models Rcfffc.$$

Der folgende Satz zeigt *Korrektheit* und *Vollständigkeit* von GI-Resolution für die Unerfüllbarkeit von universell-pränexen $\mathrm{FO}^{\neq}(S)$-Sätzen in Klauselform:

Korrektheit: Ist die leere Klausel $\Box$ durch GI-Resolution aus $\mathrm{GI}(K)$ ableitbar, $\Box \in \mathrm{Res}^*(\mathrm{GI}(K))$, so ist K unerfüllbar.

Vollständigkeit: Ist K unerfüllbar, so kann man aus $\mathrm{GI}(K)$ durch GI-Resolution die leere Klausel $\Box$ ableiten: $\Box \in \mathrm{Res}^*(\mathrm{GI}(K))$.

Für die Korrektheit hat man das folgende Lemma, das man genau wie für AL beweist.

Lemma 5.6 *Ist C eine Resolvente von C_1 und C_2, so gilt $C_1 \wedge C_2 \models C$. Daraus folgt weiter, dass $\mathrm{GI}(K) \models C$ und also auch $K \models C$ für jede Klausel C, die durch GI-Resolution aus $\mathrm{GI}(K)$ ableitbar ist. Demnach gilt $K \models \mathrm{Res}^*(\mathrm{GI}(K))$.*

Satz 5.7 (Resolutionssatz für GI-Resolution)
Für $\mathrm{FO}^{\neq}(S)$-Klauselmengen K sind äquivalent:

(i) *K unerfüllbar.*
(ii) *$\mathrm{GI}(K)$ unerfüllbar.*
(iii) $\Box \in \mathrm{Res}^*(\mathrm{GI}(K))$.

Beweis (Skizze)
(iii) $\Rightarrow$ (i) folgt mit dem Lemma, da $\Box \equiv 0$ unerfüllbar ist.
(i) $\Leftrightarrow$ (ii) folgt aus Beobachtung 5.4.
(ii) $\Rightarrow$ (iii) folgt aus der Vollständigkeit der AL Resolution, zusammen mit der Reduktion von FO auf AL gemäß Abschnitt 3.5. $\Box$

Übung 5.8 Man gebe einen Resolutionsbeweis für die Unerfüllbarkeit der Satzmenge in Beispiel 3.14. Dazu muss man zunächst die betrachteten Sätze in Klauselform bringen, was wir teilweise in Beispiel 5.2 durchgeführt haben.

Übung 5.9 Erneut die Frage, warum wir so nicht ein algorithmisches Entscheidungsverfahren für die Erfüllbarkeit von (universell-pränexen, gleichheitsfreien) FO-Sätzen erhalten?

5.3 Allgemeinere Resolutionsverfahren

Die Beschränkung der Resolutionsschritte auf Grundinstanzen zieht i.d.R. große Redundanzen nach sich, da Ableitungen für jede neue Grundinstanz repliziert werden müssen. Man würde lieber z.B. direkt aus den Klauseln $\{\neg Rxy, Qx, Qy\}$, $\{\neg Rxy, \neg Qx, \neg Qy\}$ und $\{Rxx, Rxfffx\}$ die Klausel $\{Rxfffx\}$ gewinnen können. Das wäre hier korrekt, da wirklich

$$\left.\begin{array}{c} \forall x\forall y\big(\neg Rxy \vee Qx \vee Qy\big) \\ \forall x\forall y\big(\neg Rxy \vee \neg Qx \vee \neg Qy\big) \\ \forall x\big(Rxx \vee Rxfffx\big) \end{array}\right\} \models \forall x Rxfffx.$$

Für eine korrekte Verallgemeinerung des Resolutionskalküls auf Klauseln mit Variablen muss man die Situationen in den Griff bekommen, in denen GI-Resolutionsschritte für beliebige Grundinstanzen bestimmter Terme durchführbar wäre. Um solche Situationen und geeignete Terme aufzuspüren, muss man erkennen, wann genau verschiedene Terme durch geeignete Substitutionen (von Termen, die selbst wieder Variablen erhalten können) syntaktisch gleich gemacht werden können (*Unifizierbarkeit*).

Im Beispiel: Aus den Klauseln $\{\neg Rxy, Qx, Qy\}$ und $\{\neg Rxx, \neg Qx, \neg Qy\}$ erhält man durch Substitution von x für y (sozusagen als Spezialfälle, die aber noch nicht Grundinstanzen sind) die Klauseln $\{\neg Rxx, Qx\}$ und $\{\neg Rxx, \neg Qx\}$, aus denen ein Resolutionsschritt die Klausel $\{\neg Rxx\}$ liefert. Sinngemäß wäre dieser Resolutionsschritt für jede mögliche Grundinstanz für x in GI-Resolution korrekt; die konkrete Grundinstanz $\{\neg Rcc\}$ haben wir oben durch GI-Resolution aus Grundinstanzen der gegebenen Klauseln gewonnen. Man kann nun weiter aus $\{\neg Rxx\}$ zusammen mit der Klausel $\{Rxx, Rxfffx\}$ in einem nächsten Resolutionsschritt die gewünschte Zielklausel $\{Rxfffx\}$ bekommen.

Resolution mit Unifikation spielt in automatischen Beweisern und in der logischen Programmierung (z.B. Prolog) eine wichtige Rolle.

Im folgenden schreiben wir $\sigma = (t_1, \ldots, t_n) \in T(S)^n$ für die Operation der (simultanen) Subsitution von S-Termen $t_1, \ldots, t_n$ für die Variablen $x_1, \ldots, x_n$. Wir schreiben $\lambda^\sigma := \lambda(t_1/x_1, \ldots, t_n/x_n)$ für die *σ-Substitutionsinstanz* des Literals λ, und $C^\sigma := \{\lambda_1^\sigma : \lambda \in C\}$ für die *σ-Substitutionsinstanz* der Klausel C. Die folgende Definition verallgemeinert den GI-Resulutionschritt aus Definition 5.5 auf Klauseln, die Variablen haben dürfen.

Definition 5.10 Für Klauseln C_1, C_2, C von $\mathrm{FO}^{\neq}(S)$-Literalen ist C eine *Resolvente* von C_1 und C_2 bezüglich des Literals λ, wenn für geeignete Substitutionen σ_1 und σ_2 gilt:

$$\lambda \in C_1^{\sigma_1}, \quad \overline{\lambda} \in C_2^{\sigma_2}, \quad \text{und } C = (C_1^{\sigma_1} \setminus \{\lambda\}) \cup (C_2^{\sigma_2} \setminus \{\overline{\lambda}\}).$$

Auf der Basis solcher Resolutionsschritte erhält man einen Resolutionskalkül, der nicht dazu zwingt, jeweils zu Grundinstanzen abzusteigen. Hier wird nun $\mathrm{Res}^*(K)$ als der Abschluß von K unter Hinzunahme von Resolventen (im verallgemeinerten Sinne der Definition oben) definiert.

Da $C \models C^\sigma$ für alle Substitutionsinstanzen einer Klausel C gilt (vgl. Beobachtung 5.4), ergibt sich, dass wieder $C_1 \wedge C_2 \models C$ wenn C eine Resolvente von C_1, C_2

ist. Man hat daraus, analog zu Lemma 5.6, $K \models \mathrm{Res}^*(K)$, womit auch der erweiterte Kalkül korrekt ist. Ebenso bleibt die Erweiterung natürlich vollständig. Man erhält so das allgemeinere Analogon des Resolutionssatzes Satz 5.7 für Klauselmengen mit Variablen.

Satz 5.11 (Resolutionssatz)
Für $\mathrm{FO}^{\neq}(S)$*-Klauselmengen* K *gilt:* K *unerfüllbar gdw.* $\Box \in \mathrm{Res}^*(K)$.

Bem.: Für algorithmische Realisierungen von Resolutionsverfahren spielt u.a. der zugrundeliegende Unifikationsalgorithmus eine große Rolle. Dabei nutzt man *allgemeinste unifizierende Substitutionen* (engl.: *most general unifiers*) für eine gegebene Menge von Literalen, um jeweils logisch stärkste Resolventen zu bekommen. Dies dient dazu, nicht durch übermäßig spezielle Resolventen (wie im Extremfall der GI-Resolution) den Arbeitsaufwand unnötig zu vergrößern.

6 Sequenzenkalküle

Wie in der AL, so ist auch für FO der Sequenzenkalkül ein Kalkül für das formale, syntaktische Beweisen von Folgerungsbeziehungen bzw. Allgemeingültigkeit. Sequenzen, Allgemeingültigkeit, und die Korrektheit von Regeln für das Ableiten neuer Sequenzen aus bereits abgeleiteten Sequenzen sind ganz analog zum Fall von AL definiert. Die Regeln des Sequenzenkalküls für FO bestehen aus den von der AL bekannten Regeln und zusätzlichen Regeln, die den zusätzlichen Elementen in FO Formeln Rechnung tragen (Regeln für Quantoren und für Gleichheit).

Man erhält so einen vollständigen und korrekten formalen (syntaktischen) Beweiskalkül für die Logik erster Stufe (*Gödelscher Vollständigkeitssatz*).

Die wichtigsten Konsequenzen des Vollständigkeitssatzes: ein alternativer Beweis des Kompaktheitssatzes für FO, und das Ergebnis, dass die Menge der allgemeingültigen FO Formeln rekursiv aufzählbar (semi-entscheidbar) ist. Im Gegensatz zu AL sind Allgemeingültigkeit und Erfüllbarkeit für FO jedoch *nicht entscheidbar*, da die Suche nach möglichen formalen Beweisen – anders als im Falle der AL – im Allgemeinen nicht terminierend gestaltet werden kann.

6.1 Sequenzen, Regeln, Ableitbarkeit

Wir beschränken uns (o.B.d.A.) wieder auf die Behandlung von Sätzen und Satzmengen.

Definition 6.1 [Sequenzen]
Eine FO-*Sequenz* ist ein Paar von endlichen FO-Satzmengen, (Γ, Δ), $\Gamma, \Delta \subseteq \mathrm{FO}_0(S)$; auch als $\Gamma \vdash \Delta$ notiert. Eine Sequenz $\Gamma \vdash \Delta$ heißt *allgemeingültig*, wenn $\bigwedge \Gamma \models \bigvee \Delta$ gilt.

Wie bei AL wird die linke Seite einer Sequenz als eine Konjunktion gelesen, die rechte Seite als eine Disjunktion. In einer allgemeingültigen Sequenz ist die rechte Seite (als Disjunktion gelesen) eine Folgerung aus der linken Seite (als Konjuntion von Voraussetzungen gelesen). Schreibweisen: Γ, φ anstelle von $\Gamma \cup \{\varphi\}$; φ anstelle von $\{\varphi\}$, usw.; wir fassen die Satzmengen in Sequenzen auch als Listen (mit beliebiger Reihenfolge der Elemente) auf.

Beispiel 6.2 Die Sequenz $\emptyset \vdash \{\varphi\}$ ist allgemeingültig, gdw. φ allgemeingültig ist; die Sequenz $\Gamma \vdash \emptyset$ ist allgemeingültig, gdw. Γ unerfüllbar ist.

Wie bei AL, erlauben Sequenzenregeln die Erzeugung (Ableitung) neuer Sequenzen aus bereits erzeugten oder gegebenen Sequenzen. Erinnerung (siehe AL): allgemeines Format von Sequenzenregeln mit Prämissen (über dem Balken) und Konklusion (unter dem Balken); Konklusionen von Regeln ohne Prämisssen werden als Axiome aufgefasst.

Definition 6.3 [Ableitbarkeit]
Eine Sequenz heißt *ableitbar* im Sequenzenkalkül, falls sie (in endlich vielen Schritten) durch Anwendung von Sequenzenregeln (ausgehend von Axiomen, d.h. Regeln ohne Prämissen) als Konklusion gewonnen werden kann.

Die *Korrektheit* des Sequenzenkalküls besagt:

Korrektheit: jede ableitbare Sequenz ist allgemeingültig.

Die Korrektheit des Sequenzenkalküls folgt aus der Korrektheit der einzelnen Regeln, d.h., daraus, dass:

(a) die Axiome allgemeingültige Sequenzen sind.

(b) für alle Regeln mit Prämissen gilt: sind die Prämissen allgemeingültig, so auch die Konklusion.

Wir behandeln den Nachweis der Bedingung (b) jeweils exemplarisch zusammen mit der Einführung der neuen Regeln.

Der FO Sequenzenkalkül $\mathcal{SK}$ hat drei Gruppen von Regeln:

- aussagenlogische Regeln (die Regeln des AL-Sequenzenkalküls, jetzt für die aussagenlogischen Junktoren in FO-Formeln).
- Quantorenregeln, für die Einführung von $\forall$ oder $\exists$ in Formeln auf der linken oder rechten Seite von Sequenzen: Regeln ($\forall$L), ($\forall$R), ($\exists$L), und ($\exists$R).
- Gleichheitsregeln, die die Verwendung trivialer Term-Gleichheiten $t = t$ erlauben (Regel (=)), bzw. unter Voraussetzung der Termgleichheiten $t = t'$ oder $t' = t$ die Substitution von Termen t' anstelle von t erlauben: Regeln (Sub-L) und (Sub-R).

Die Quantorenregeln bilden zusammen mit den AL-Regeln einen vollständigen Beweiskalkül $\mathcal{SK}^{\neq}$ für $\mathrm{FO}^{\neq}$. Mit Hinzunahme der Gleichheitsregeln ergibt sich insgesamt ein vollständiger Beweiskalkül $\mathcal{SK}$ für FO.

Wie im Falle der AL ist es für manche Zwecke nützlich, für die Vollständigkeit aber nicht erforderlich, eine Schnittregel für die Schlussfigur des *modus ponens* (Kettenschlussregel), sowie eine daraus ableitbare Widerspruchsregel für die Schlussfigur des indirekten Beweises hinzuzunehmen.

Quantorenregeln Die folgenden Regeln gelten jeweils für beliebige Satzmengen $\Gamma, \Delta \subseteq \mathrm{FO}_0(S)$, Formeln $\varphi(x) \in \mathrm{FO}(S)$, in denen allenfalls x frei ist, Terme $t \in T_0(S)$, und Konstanten $c \in S$ (mit expliziten Einschränkungen hinsichtlich des Vorkommens wie angegeben). Erinnerung: $\varphi(c/x)$ steht für das Ergebnis der Substitution von c für die freie Variable x in $\varphi(x)$.

$$(\forall\mathrm{L})\quad \frac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, \forall x\varphi(x) \vdash \Delta} \qquad (\forall\mathrm{R})\quad \frac{\Gamma \vdash \Delta, \varphi(c/x)}{\Gamma \vdash \Delta, \forall x\varphi(x)}$$
falls c nicht in $\Gamma, \Delta, \varphi(x)$

$$(\exists\mathrm{L})\quad \frac{\Gamma, \varphi(c/x) \vdash \Delta}{\Gamma, \exists x\varphi(x) \vdash \Delta} \qquad (\exists\mathrm{R})\quad \frac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma \vdash \Delta, \exists x\varphi(x)}$$
falls c nicht in $\Gamma, \Delta, \varphi(x)$

Korrektheit Wir behandeln exemplarisch den Fall der beiden $\forall$-Regeln indem wir Bedingung (b) überprüfen; die Argumente für die $\exists$-Regeln sind streng analog.

Regel ($\forall$L). Sei $\Gamma, \varphi(t/x) \vdash \Delta$ allgemeingültig, also $\Gamma \cup \{\varphi(t/x)\} \models \delta$, wo $\delta := \bigvee \Delta$. Zu zeigen ist die Allgemeingültigkeit von $\Gamma, \forall x\varphi(x) \vdash \Delta$, also, dass auch $\Gamma \cup \{\forall x\varphi(x)\} \models \delta$. Sei also $\mathcal{A} \models \Gamma \cup \{\forall x\varphi(x)\}$; dann folgt aus $\mathcal{A} \models \forall x\varphi(x)$ insbesondere, dass $\mathcal{A} \models \varphi[t^{\mathcal{A}}]$, also $\mathcal{A} \models \varphi(t/x)$, und damit folgt $\mathcal{A} \models \delta$ mit $\Gamma \cup \{\varphi(t/x)\} \models \delta$.

Regel ($\forall$R). Sei $\Gamma \vdash \Delta, \varphi(c/x)$ allgemeingültig, c nicht in $\Gamma, \Delta, \varphi(x)$. Sei $\delta := \bigvee \Delta$. Zu zeigen ist die Allgemeingültigkeit von $\Gamma \vdash \Delta, \forall x\varphi(x)$. Sei $\mathcal{A} \models \Gamma$. Falls $\mathcal{A} \models \delta$, ist nichts zu zeigen; wir nehmen also an, dass $\mathcal{A} \not\models \delta$. Sei $a \in A$; wir müssen zeigen, dass $\mathcal{A} \models \varphi[a]$. $\mathcal{A}'$ entstehe aus $\mathcal{A}$, indem wir $c^{\mathcal{A}'} := a$ setzen. Dann ist $\mathcal{A}' \models \Gamma$ und $\mathcal{A}' \not\models \delta$, da c weder in Γ noch in Δ vorkommt. Wegen $\mathcal{A}' \models \Gamma$, und aus der Allgemeingültigkeit von $\Gamma \vdash \Delta, \varphi(c/x)$ folgt, dass $\mathcal{A}' \models \delta \vee \varphi(c/x)$; da $\mathcal{A}' \not\models \delta$ muss also $\mathcal{A}' \models \varphi(c/x)$ sein, d.h. $\mathcal{A}' \models \varphi[a]$ und demnach $\mathcal{A} \models \varphi[a]$. Da dies für jedes $a \in A$ gilt, folgt also $\mathcal{A} \models \forall x\varphi(x)$.

Beispiel 6.4 Die Sequenz $Pc \vdash Pc$ ist allgemeingültig, nicht aber die Sequenz $Pc \vdash \forall xPx$, die man wie in ($\forall$R) mit $\varphi(x) = Px$ aus $Pc \vdash Pc$ ableiten könnte, wenn die Bedingung "c nicht in $\Gamma, \Delta, \varphi(x)$" nicht wäre.

Die bisher behandelten Regeln bilden einen Sequenzenkalkül $\mathcal{SK}^{\neq}$ für $\mathrm{FO}^{\neq}$. Der Sequenzenkalkül $\mathcal{SK}$ für FO hat zusätzlich folgende Gleichheitsregeln.

Gleichheitsregeln Die Regeln verstehen sich wieder für beliebige Satzmengen $\Gamma, \Delta \subseteq \mathrm{FO}_0(S)$, Formeln $\varphi(x) \in \mathrm{FO}(S)$, in denen allenfalls x frei ist, Terme $t, t' \in T_0(S)$. Die Sätze $\varphi(t/x)$ und $\varphi(t'/x)$ sind das Ergebnis der Substitution von t bzw. von t' für x in $\varphi(x)$.

$$(=)\quad \frac{\Gamma, t = t \vdash \Delta}{\Gamma \vdash \Delta}$$

$$(\text{Sub-L})\quad \frac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, t = t', \varphi(t'/x) \vdash \Delta} \qquad (\text{Sub-R})\quad \frac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma, t = t' \vdash \Delta, \varphi(t'/x)}$$
und analoge Regeln mit $t' = t$ statt $t = t'$

Korrektheit Bedingung (b) (Seite 27) ist offensichtlich für die Regel (=). Wir prüfen (b) exemplarisch für die Regel (Sub-L) nach. Sei $\delta := \bigvee \Delta$, und betrachte $\mathcal{A} \models \Gamma \cup \{t = t', \varphi(t'/x)\}$; wir müssen zeigen, dass $\mathcal{A} \models \delta$. $\mathcal{A} \models \varphi(t'/x)$ bedeutet, dass $\mathcal{A} \models \varphi[t'^{\mathcal{A}}]$; da $\mathcal{A} \models t = t'$ gilt $t^{\mathcal{A}} = t'^{\mathcal{A}}$ und demnach auch $\mathcal{A} \models \varphi[t^{\mathcal{A}}]$, also $\mathcal{A} \models \varphi(t/x)$. Aus der Korrektheit der Prämisse folgt nun wegen $\mathcal{A} \models \Gamma \cup \{\varphi(t/x)\}$, dass $\mathcal{A} \models \delta$.

Optional: Schnittregeln Die Schnittregel modus ponens und die daraus ihrerseits ableitbare Widerspruchsregel sind genau wie im AL Sequenzenkalkül gebaut, wobei aber hier natürlich Γ, Γ' und φ beliebige Sequenzen bzw. Sätze in FO sind. Ihre Korrektheit lässt sich direkt nachprüfen. Wir betrachten auch hier wieder eine Erweiterung des Sequenzenkalküls $\mathcal{SK}$ zu $\mathcal{SK}^+$, weil die zusätzlichen Regeln

- naheliegenden und häufig verwendeten Schlussfiguren in natürlichen mathematischen Beweisen entsprechen (Kettenschlüsse nach *modus ponens* und indirekte Beweise nach der *Widerspruchsregel*).
- man für den so erweiterten Sequenzenkalkül einen etwas vereinfachten Vollständigkeitsbeweis führen kann.

Erinnerung: Charakteristisch an Schnittregeln ist, dass sie Formeln (im Beweis: Zwischenbehauptungen bzw. den Widerspruch) schlucken.

$$\text{(modus ponens)}\quad \frac{\Gamma \vdash \varphi \qquad \Gamma', \varphi \vdash \Delta}{\Gamma, \Gamma' \vdash \Delta} \qquad \text{(Kontr)}\quad \frac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \neg\varphi}{\Gamma, \Gamma' \vdash \emptyset}$$

Wie in AL lässt auch hier die Verwendung der Widerspruchsregel (Kontr) lokal durch modus ponens und die übrigen Regeln eliminieren.

Wir schreiben $\mathcal{SK}$ bzw. $\mathcal{SK}^{\neq}$ für die sparsameren *schnittfreien* Sequenzenkalküle (mit und ohne Gleichheit) und $\mathcal{SK}^+$ für den um die Schnittregel(n) erweiterten Sequenzenkalkül $\mathcal{SK}$.

Die Regeln des Sequenzenkalküls $\mathcal{SK}$ ($\mathcal{SK}^{\neq}$ besteht aus den Teilen AL und $\forall/\exists$):

(Ax) $\dfrac{}{\Gamma, \varphi \vdash \Delta, \varphi}$

($\neg$L) $\dfrac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}$ ($\neg$R) $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$

($\vee$L) $\dfrac{\Gamma, \varphi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}$ ($\vee$R) $\dfrac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}$

($\wedge$L) $\dfrac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}$ ($\wedge$R) $\dfrac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}$

} AL

($\forall$L) $\dfrac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, \forall x\varphi(x) \vdash \Delta}$ ($\forall$R) $\dfrac{\Gamma \vdash \Delta, \varphi(c/x)}{\Gamma \vdash \Delta, \forall x\varphi(x)}$ falls c nicht in $\Gamma, \Delta, \varphi(x)$

($\exists$L) $\dfrac{\Gamma, \varphi(c/x) \vdash \Delta}{\Gamma, \exists x\varphi(x) \vdash \Delta}$ falls c nicht in $\Gamma, \Delta, \varphi(x)$ ($\exists$R) $\dfrac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma \vdash \Delta, \exists x\varphi(x)}$

} $\forall/\exists$

(=) $\dfrac{\Gamma, t = t \vdash \Delta}{\Gamma \vdash \Delta}$

(Sub-L) $\dfrac{\Gamma, \varphi(t/x) \vdash \Delta}{\Gamma, t = t', \varphi(t'/x) \vdash \Delta}$ (Sub-R) $\dfrac{\Gamma \vdash \Delta, \varphi(t/x)}{\Gamma, t = t' \vdash \Delta, \varphi(t'/x)}$

und analoge Regeln mit $t' = t$ statt $t = t'$

} =/Sub

6.2 Der Gödelsche Vollständigkeitssatz

Betrachtet man den Sequenzenkalkül als Kalkül für formale, syntaktische Beweise im Rahmen der Logik erster Stufe, so ist man auch an einem Begriff der Ableitbarkeit interessiert, der beliebige (auch unendliche) Mengen von Voraussetzungen zulässt. Z.B. will man von der Ableitbarkeit (formalen Beweisbarkeit) im Rahmen einer gegebenen in FO formalisierten Theorie sprechen können.

Definition 6.5 [Ableitbarkeit und formale Beweisbarkeit in Theorien, Konsistenz]
Sei $\Phi \subseteq \mathrm{FO}_0(S)$ eine Satzmenge (FO Theorie):

$\varphi \in \mathrm{FO}_0(S)$ heißt *im Sequenzenkalkül ableitbar (beweisbar) aus* Φ, wenn eine Sequenz $\Gamma_0 \vdash \varphi$ mit $\Gamma_0 \subseteq \Phi$ im Sequenzenkalkül ableitbar ist. In Symbolen: $\Phi \vdash \varphi$.

Eine Sequenz $\Gamma \vdash \Delta$ ist *im Sequenzenkalkül ableitbar (beweisbar) aus* Φ, wenn eine Sequenz $\Gamma_0, \Gamma \vdash \Delta$ mit $\Gamma_0 \subseteq \Phi$ im Sequenzenkalkül ableitbar ist.

Φ heißt *konsistent*, wenn für kein $\Gamma_0 \subseteq \Phi$ die Sequenz $\Gamma_0 \vdash \emptyset$ ableitbar ist.

Die Korrektheit des Sequenzenkalküls ist damit äquivalent zu jeder der Aussagen:

- für alle $\Phi \subseteq \mathrm{FO}_0(S)$, $\varphi \in \mathrm{FO}_0(S)$: $\quad \Phi \vdash \varphi \quad \Rightarrow \quad \Phi \models \varphi$.
- für alle $\Phi \subseteq \mathrm{FO}_0(S)$: $\quad \Phi$ erfüllbar $\Rightarrow$ Φ konsistent.

Übung 6.6 Zeigen Sie die Äquivalenz der obigen Bedingungen zur Korrektheitsbedingung, die besagt, dass jede ableitbare Sequenz allgemeingültig ist.

Der Gödelsche Vollständigkeitssatz besagt, dass der Sequenzenkalkül in dem starken Sinne vollständig ist, dass man die genaue Umkehrung der beiden Korrektheitsaussagen hat. Korrektheit und Vollständigkeit zusammen liefern also gerade die völlige Entsprechung zwischen syntaktischer Beweisbarkeit und der semantischen Folgerungsbeziehung, bzw. zwischen Konsistenz und Erfüllbarkeit.

Ableitbarkeit $\Phi \vdash \varphi$	$\longleftrightarrow$	Folgerung $\Phi \models \varphi$
Konsistenz	$\longleftrightarrow$	Erfüllbarkeit

Die Begriffe auf der linken Seite sind syntaktischer Natur, die auf der rechten Seite semantischer Natur. Für die erste Äquivalenz steckt die Vollständigkeit in der Implikation von rechts nach links; für die zweite in der Implikation von links nach rechts. Korrektheit steckt in der jeweils anderen Implikation.

Satz 6.7 (Gödelscher Vollständigkeitssatz)
Für jede Satzmenge $\Phi \subseteq \mathrm{FO}_0(S)$ *und jeden Satz* $\varphi \in \mathrm{FO}_0(S)$ *gelten:*

(i) $\Phi \models \varphi$ *gdw.* $\Phi \vdash \varphi$.

(ii) Φ *erfüllbar gdw.* Φ *konsistent.*

Folgerung 1: Kompaktheit
Für die Ableitbarkeitsbeziehung gilt offensichtlich (per Definition) die Endlichkeitsaussage

$$\Phi \vdash \varphi \quad \text{gdw.} \quad \Phi_0 \vdash \varphi \text{ für eine endliche Teilmenge } \Phi_0 \subseteq \Phi.$$

Aus der Korrespondenz zwischen Ableitbarkeit und Folgerungsbeziehung erhalten wir so den Kompaktheitssatz als Korollar aus dem Vollständigkeitssatz:

$$\Phi \models \varphi \quad \text{gdw.} \quad \Phi_0 \models \varphi \text{ für eine endliche Teilmenge } \Phi_0 \subseteq \Phi.$$

Übung 6.8 Folgern Sie entsprechend, direkt aus dem Vollständigkeitssatz, dass Φ erfüllbar ist gdw. jede endliche Teilmenge $\Phi_0 \subseteq \Phi$ erfüllbar ist.

Folgerung 2: Allgemeingültigkeit ist rekursiv aufzählbar
Die Menge aller ableitbaren Sequenzen $\Gamma \vdash \varphi$ über $\mathrm{FO}_0(S)$ ist für jede feste endliche (oder rekursiv aufzählbare) Signatur S rekursiv aufzählbar: man kann systematisch alle endlichen Kombinationen von Regelanwendungen so durchprobieren, dass man jede tatsächlich ableitbare Sequenz schließlich erreicht. Insbesondere ist also die Menge aller ableitbaren Sequenzen der Form $\emptyset \vdash \varphi$ rekursiv aufzählbar. Nach dem Vollständigkeitssatz entspricht dies gerade der Menge der φ mit $\emptyset \models \varphi$, also der Menge der allgemeingültigen φ.
Entsprechend ist die Menge aller aus einer rekursiv aufzählbaren Satzmenge Φ ableitbaren Sätze rekursiv aufzählbar – z.B. die Menge aller wahren Sätze der Gruppentheorie.

6.3 Exkurs: Vollständigkeitsbeweise

Wir skizzieren die groben Züge zweier wichtiger Vollständigkeitsbeweise. Der erste, über sogenannte *Hintikka-Mengen*, liefert die (stärkeren) Vollständigkeitsaussagen für die Sequenzenkalküle ohne Schnittregeln ($\mathcal{SK}$, bzw. $\mathcal{SK}^{\neq}$ in der gleichheitsfreien Version); wir konzentrieren uns hierbei den gleichheitsfreien Fall. Der zweite, über eine sogenannte *Henkin-Konstruktion*, liefert einen etwas einfacheren Zugang zur (schwächeren) Vollständigkeitsaussage für den Sequenzenkalkül $\mathcal{SK}^{+}$ mit Schnittregeln.

Eine Hintikka-Konstruktion Wir argumentieren für die Sequenzenkalküle $\mathcal{SK}$ bzw. $\mathcal{SK}^{\neq}$. Die Vollständigkeitsaussage ist hier die folgende:

Ist die Sequenz $\Gamma \vdash \Delta$ *nicht* aus Φ ableitbar, so ist $\Phi \cup \Gamma \cup \Delta^{\neg}$ erfüllbar (wobei $\Delta^{\neg} = \{\neg\varphi \colon \varphi \in \Delta\}$); also gilt *nicht* $\Phi \models \bigwedge \Gamma \to \bigvee \Delta$.

Lemma 6.9 *Für Ableitbarkeit/Beweisbarkeit aus einer Satzmenge Φ:*
Ist die Sequenz $\Gamma \vdash \Delta$ nicht aus Φ ableitbar, so ist $\Phi \cup \Gamma \cup \Delta^{\neg}$ erfüllbar.

Der Beweis basiert auf folgenden Schritten. Zur Illustration betrachten wir die Variante für $\mathcal{SK}^{\neq}$ (ohne Gleichheit) über einer höchstens abzählbaren Signatur S_0.

Wir erweitern S_0 um eine unendlichen Folge neuer Konstantensymbole $(c_i)_{i\in\mathbb{N}}$. Wir wollen zu der gegebenen, nicht aus Φ ableitbaren Sequenz $\Gamma \vdash \Delta$ eine Herbrand-Struktur $\mathcal{H}$ über den variablenfreien Termen $T_0(S)$ gewinnen, die ein Modell von $\Phi \cup \Gamma \cup \Delta^{\neg}$ ist.

Man konstruiert induktiv Folgen von endlichen Satzmengen

$$\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \cdots$$
$$\Delta = \Delta_0 \subseteq \Delta_1 \subseteq \Delta_2 \subseteq \cdots$$

derart, dass für jedes $n \in \mathbb{N}$ gilt, dass $\Gamma_n \vdash \Delta_n$ nicht aus Φ ableitbar ist.

Die Information in der nicht ableitbaren Sequenz $\Gamma_0 \vdash \Delta_0$ wird dabei schrittweise induktiv angereichert. Das Ziel dabei ist, dass die atomaren Sätze auf der linken Seite ($\bigcup_{n\in\mathbb{N}} \Gamma_n$, positive Information) zusammen mit den Negationen der Sätze auf der rechten Seite ($\bigcup_{n\in\mathbb{N}} \Delta_n$: negative Information) schließlich eine Spezifikation der gewünschten Herbrand-Struktur $\mathcal{H}$ liefern. Dafür, dass $\mathcal{H}$ auch die nicht-atomaren Sätze auf der linken Seite und die Negate derjenigen auf der rechten Seite erfüllt, sorgen die Abschlussforderungen, die die induktive Anreicherung dieser Satzmengen steuern. Für die unendlichen Satzmengen $\hat{\Gamma} := \bigcup_{n\in\mathbb{N}} \Gamma_n$ und $\hat{\Delta} := \bigcup_{n\in\mathbb{N}} \Delta_n$ soll $\hat{\Phi} := \Phi \cup \hat{\Gamma} \cup \hat{\Delta}^{\neg}$ folgende Abschlusseigenschaften haben (man nennt solche Satzmengen auch *Hintikka-Mengen*):

(i) für kein φ ist $\varphi \in \hat{\Phi}$ und $\neg\varphi \in \hat{\Phi}$. (Konsistenzbedingung)
(ii) ist $\varphi \in \hat{\Phi}$, $\varphi = \varphi_1 \vee \varphi_2$, so ist $\varphi_i \in \hat{\Phi}$ für mindestens eines von $i = 1$ oder $i = 2$.
(iii) ist $\varphi \in \hat{\Phi}$, $\varphi = \varphi_1 \wedge \varphi_2$, so ist $\varphi_i \in \hat{\Phi}$ für $i = 1$ und $i = 2$.
(iv) ist $\varphi \in \hat{\Phi}$, $\varphi = \exists x\psi(x)$, so ex. $c \in S$, sodass $\psi(c/x) \in \hat{\Phi}$. (Existenzbeispiele)
(v) ist $\varphi \in \hat{\Phi}$, $\varphi = \forall x\psi(x)$, so ist $\psi(t/x) \in \hat{\Phi}$ für jeden Term $t \in T_0(S)$.

Satz 6.10 (über Hintikka-Mengen) *$\hat{\Phi} \subseteq \mathrm{FO}^{\neq}(S)$ erfülle die Bedingungen (i)–(v) (Hintikka-Menge). Sei $\mathcal{H} = \mathcal{H}(\hat{\Phi})$ die Herbrand-Struktur mit Trägermenge $T_0(S)$, mit folgender Interpretation der Relationssymbole: für n-stelliges $R \in S$ sei*

$$R^{\mathcal{H}} := \big\{(t_1, \ldots, t_n) \in T_0(S)^n \colon Rt_1 \ldots t_n \in \hat{\Phi}\big\}.$$

Dann ist $\mathcal{H} \models \hat{\Phi}$, d.h. es gilt für alle $\varphi \in \hat{\Phi}$: $\mathcal{H} \models \varphi$.

Übung 6.11 Man beweise die Aussage des Satzes durch Induktion über den Aufbau der Sätze $\varphi \in \Phi$ anhand der Abschlussbedingungen (i)–(v).

Die analoge Behauptung im Falle von FO mit Gleichheit wird bewiesen indem man aus der Konstruktion der Mengen Γ_n und Δ_n eine Herbrand-Struktur gewinnt, in der man nach den in den $\hat{\Phi}$ geforderten Termgleichheiten faktorisieren kann. Die Quotientenstruktur, die man so erhält, ist dann ein Modell von Φ. Zu den Abschlussbedingungen (i)–(v) oben treten dafür noch die folgenden Bedingungen hinzu:

(vi) für alle $t \in T_0(S)$ ist die Termgleichheit $t = t$ in $\hat{\Phi}$.
(vii) ist $\varphi \in \hat{\Phi}$, $\varphi = \psi(t/x)$, und $t = t' \in \hat{\Phi}$ oder $t' = t \in \hat{\Phi}$, so ist auch $\psi(t'/x) \in \hat{\Phi}$.

Der induktive Prozess, der die Abschlusseigenschaften (i)–(vii) durch Wahl der Folgen Γ_n und Δ_n gewährleistet, soll hier nicht im Detail beschrieben werden. Die einzelnen Schritte (wie etwa die Deklaration von "Existenzbeispielen" für (iv)) greifen auf die Regeln des Kalküls zurück, um etwa zu zeigen, dass für eine geeignete Wahl der Konstanten c aus der Nichtableitbarkeit von $\Gamma, \exists x\psi(x) \vdash \Delta$ folgt, dass auch $\Gamma, \psi(c/x) \vdash \Delta$ nicht ableitbar ist. Tatsächlich: Wenn c nicht in $\Gamma, \Delta, \psi(x)$, so wäre aus $\Gamma, \psi(c/x) \vdash \Delta$ auch $\Gamma, \exists x\psi(x) \vdash \Delta$ ableitbar:

$$(\exists\mathrm{L}) \quad \frac{\Gamma, \psi(c/x) \vdash \Delta}{\Gamma, \exists x\psi(x) \vdash \Delta}$$

Eine Henkin-Konstruktion Einen etwas einfacheren Beweis für die Vollständigkeit kann man für Varianten des Sequenzenkalküls mit Schnittregeln führen (vgl. Seite 6.1).

Übung 6.12 Folgern Sie aus der Vollständigkeit von $\mathcal{SK}$, dass es zu jedem formalen Beweis, der eine der Schnittregeln benutzt, einen alternativen formalen Beweis gibt, der ohne Schnittregeln auskommt.

Wir betrachten für den Rest dieses Abschnitts den Sequenzenkalkül $\mathcal{SK}^+$. Entsprechend bedeutet jetzt *Konsistenz von* Φ, dass für kein $\Gamma \subseteq \Phi$ die Sequenz $\Gamma \vdash \emptyset$ (in $\mathcal{SK}^+$) ableitbar ist.

Beobachtung 6.13 Sei Φ konsistent. Dann gilt: $\Phi \cup \{\varphi\}$ konsistent, gdw. nicht $\Phi \vdash \neg\varphi$.

Begründung. $\Phi \vdash \neg\varphi$ bedeutet, dass für ein $\Gamma \subseteq \Phi$ die Sequenz $\Gamma \vdash \neg\varphi$ ableitbar ist. Dann ergibt sich folgende Ableitung von $\Gamma, \varphi \vdash \emptyset$; also ist $\Phi \cup \{\varphi\}$ nicht konsistent:

$$\text{(modus ponens)}\quad \dfrac{\Gamma \vdash \neg\varphi \qquad \dfrac{}{\Gamma, \neg\varphi, \varphi \vdash \neg\varphi}\,(\text{Ax})}{\text{(Kontr)}\ \dfrac{\Gamma, \varphi \vdash \neg\varphi \qquad \dfrac{}{\Gamma, \varphi \vdash \varphi}\,(\text{Ax})}{\Gamma, \varphi \vdash \emptyset}}$$

Ist umgekehrt $\Phi \cup \{\varphi\}$ nicht konsistent, so existiert $\Gamma \subseteq \Phi \cup \{\varphi\}$ und eine Ableitung von $\Gamma \vdash \emptyset$. Da Φ konsistent ist, muss $\varphi \in \Gamma$ sein, also $\Gamma = \Gamma', \varphi$. So bekommt man mit ($\neg$R) auch $\Gamma' \vdash \neg\varphi$ also $\Phi \vdash \neg\varphi$.

Die Vollständigkeit von $\mathcal{SK}^+$ erhält man aus der folgenden Behauptung.

Satz 6.14 *Sei $\Phi \subseteq \mathrm{FO}_0(S)$ konsistent bzgl. $\mathcal{SK}^+$. Dann ist Φ erfüllbar.*

Beweisskizze. Für abzählbare Signatur S. Wir wollen diese Satzmenge (schrittweise) zu einer konsistenten Satzmenge $\hat{\Phi} \supseteq \Phi$ (in einer um neue Konstantensymbole erweiterten Signatur) erweitern, die bestimmte Abschlusseigenschaften hat (ähnlich den Bedingungen an Hintikka-Mengen). Hier wird sogar (anstelle von (i) dort) verlangt, dass für jedes $\varphi \in \mathrm{FO}_0(S)$ genau einer der Sätze φ oder $\neg\varphi$ zu $\hat{\Phi}$ gehöre.
$\hat{\Phi} \subseteq \mathrm{FO}_0(S)$ ist eine *Henkin-Menge* wenn gilt:

(i) für jedes $\varphi \in \mathrm{FO}_0(S)$: $\quad \varphi \in \hat{\Phi} \;\Leftrightarrow\; \neg\varphi \notin \hat{\Phi}$. (Maximale Konsistenz)

(ii) für jedes $\psi(x) \in \mathrm{FO}(S)$ existiert ein Term $t \in T_0(S)$ mit $(\forall x\neg\psi(x) \vee \psi(t/x)) \in \hat{\Phi}$. (Existenzbeispiele)

Übung 6.15 Man zeige (für den Fall $\mathrm{FO}^{\neq}$), dass jede Henkin-Menge die Bedingungen (i)–(v) für Hintikka-Mengen erfüllt.

Um Bedingung (ii) zu realisieren, nimmt man in einem abzählbar unendlichen induktiven Prozess stets wieder für alle noch nicht behandelten Formeln $\psi(x)$ neue Konstantensymbole c_ψ und den Satz $\forall x\neg\psi(x) \vee \psi(c_\psi/x)$ hinzu. Wichtig ist dabei, dass dieser Schritt die Konsistenz erhält, wenn man dafür sorgt, dass c_ψ noch nirgends sonst vorkommt. Ist nämlich Φ konsistent, c nicht in Φ oder $\psi(x)$, so folgt, dass auch $\Phi \cup \{\forall x\neg\psi(x) \vee \psi(c/x)\}$ konsistent ist.

Begründung: Wäre $\Phi \cup \{\forall x\neg\psi(x) \vee \psi(c/x)\}$ nicht konsistent, so gäbe es ein $\Gamma \subseteq \Phi$, für das die Sequenz $\Gamma \vdash \neg(\forall x\neg\psi(x) \vee \psi(c/x))$ ableitbar ist. Dann wären auch die Sequenzen $\Gamma \vdash \neg\psi(c/x)$ und $\Gamma \vdash \neg\forall x\neg\psi(x)$ ableitbar (siehe Diagramm unten für $\Gamma \vdash \neg\psi(c/x)$; die mit Pünktchen angedeutete Ableitung von $\Gamma \vdash \neg\forall x\neg\psi(x)$ geht analog vor). Demnach ist weiter $\Gamma \vdash \forall x\neg\psi(x)$ mit ($\forall$R) ableitbar, da c sonst nicht vorkommt. Daraus dann $\Gamma \vdash \emptyset$, d.h. schon Φ inkonsistent.

$$\text{(modus ponens)}\quad \dfrac{\Gamma \vdash \neg(\forall x\neg\psi(x) \vee \psi(c/x)) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \psi(c/x) \vdash \forall x\neg\psi(x), \psi(c/x)}\,(\text{Ax})}{\Gamma, \psi(c/x) \vdash \forall x\neg\psi(x) \vee \psi(c/x)}\,(\vee\text{R})}{\Gamma \vdash \forall x\neg\psi(x) \vee \psi(c/x), \neg\psi(c/x)}\,(\neg\text{R})}{\Gamma, \neg(\forall x\neg\psi(x) \vee \psi(c/x)) \vdash \neg\psi(c/x)}\,(\neg\text{L})}{\text{(Kontr)}\ \dfrac{\text{(}\forall\text{R)}\ \dfrac{\Gamma \vdash \neg\psi(c/x)}{\Gamma \vdash \forall x\neg\psi(x)} \qquad \vdots\ \Gamma \vdash \neg\forall x\neg\psi(x)}{\Gamma \vdash \emptyset}}$$

Für eine konsistente Satzmenge Φ, die (ii) bereits erfüllt, kann man (i) wie folgt realisieren. Sei $\mathrm{FO}_0(S) = \{\varphi_0, \varphi_1, \varphi_2, \ldots\}$ eine Aufzählung aller $\mathrm{FO}(S)$-Sätze. Beginnend mit $\Phi_0 := \Phi$ wähle induktiv

$$\Phi_{n+1} := \begin{cases} \Phi_n \cup \{\varphi_n\} & \text{falls } \Phi_n \cup \{\varphi_n\} \text{ konsistent,} \\ \Phi_n \cup \{\neg\varphi_n\} & \text{sonst.} \end{cases}$$

Mit der Beobachtung (und (Kontr)) folgt, dass alle Φ_n konsistent bleiben. Also ist auch $\hat{\Phi} := \bigcup_{n\in\mathbb{N}} \Phi_n$ konsistent und erfüllt Bedingung (i). Der Rest des Beweises ergibt sich nun mit der folgenden Behauptung (analog zur Hintikka-Konstruktion).

Satz 6.16 (über Henkin-Mengen) *$\hat{\Phi} \subseteq \mathrm{FO}(S)$ sei eine Henkin-Menge. Dann ist die 2-stellige Relation $\sim$,*

$$t \sim t' \quad \textit{gdw.} \quad t = t' \in \hat{\Phi}.$$

eine Äquivalenzrelation auf $T_0(S)$. Ferner sind die Relationen und Funktionen in der durch $\hat{\Phi}$ definierten Herbrand-Struktur $\mathcal{H}(\hat{\Phi})$ (vgl. Satz 6.10) alle mit $\sim$ verträglich, und die Quotientenstruktur, deren Elemente die $\sim$-Äquivalenzklassen der Terme $t \in T_0(S)$ sind, ist ein Modell von $\hat{\Phi}$.

7 Unentscheidbarkeit

7.1 Unentscheidbarkeit von FO-Erfüllbarkeit

Aus dem Vollständigkeitssatz folgt, dass die Menge der allgemeingültigen $\mathrm{FO}(S)$-Sätze (für endliches oder rekursiv aufzählbares S) zumindest rekursiv aufzählbar ist. Dasselbe gilt für die Menge der unerfüllbaren Sätze, also für das Komplement von $\mathrm{SAT}(\mathrm{FO}(S))$, da $\varphi \notin \mathrm{SAT}$ gdw. $\neg\varphi$ allgemeingültig.

Wäre $\mathrm{SAT}(\mathrm{FO}(S))$ seinerseits rekursiv aufzählbar, so also entscheidbar (vgl. FG I, Kapitel 7). Aus dem ersten Teil wissen wir, dass $\mathrm{SAT}(\mathrm{AL})$ entscheidbar ist. Im Gegensatz dazu zeigen wir jetzt, dass $\mathrm{SAT}(\mathrm{FO}(S))$ unentscheidbar ist.

Reduktion des Halteproblems auf FO-Erfüllbarkeit Die Unentscheidbarkeit von $\mathrm{SAT}(\mathrm{FO}(S))$ folgt aus der Existenz einer Reduktion des unentscheidbaren Halteproblems für Turingmaschinen auf die Erfüllbarkeit von FO-Sätzen. Vgl. FG I, Kapitel 7, zum Halteproblem H und seiner Unentscheidbarkeit. Wir präsentieren eine berechenbare Abbildung

$$\mathcal{M}, w \longmapsto \varphi_{\mathcal{M},w}, \qquad (*)$$

die jeder DTM $\mathcal{M}$ über Σ und jedem $w \in \Sigma^*$ einen Satz $\varphi_{\mathcal{M},w}$ zuordnet, sodass

$$w \xrightarrow{\mathcal{M}} \infty \quad \text{gdw.} \quad \varphi_{\mathcal{M},w} \text{ erfüllbar.}$$

Daraus folgt dann, dass $\langle\mathcal{M}\rangle \in H$, gdw. $\varphi_{\mathcal{M},w} \notin \mathrm{SAT}(\mathrm{FO})$ für $w = \langle\mathcal{M}\rangle$. Wäre Erfüllbarkeit für die Sätze $\varphi_{\mathcal{M},w}$ algorithmisch entscheidbar, so auch das Haltproblem. Also folgt die Unentscheidbarkeit des Erfüllbarkeitsproblems für FO.

Wir geben eine einfache Reduktionsfunktion $(*)$ an, für die $\varphi_{\mathcal{M},w} \in \mathrm{FO}_0(S_\mathcal{M})$. Dabei besteht die Signatur $S_\mathcal{M}$ für $\mathcal{M} = (\Sigma, Q, q_0, \delta, q^+, q^-)$ aus folgenden Symbolen:

succ	Nachfolgerfunktion (für Schritt- und Positionszähler), 1-stellig.
pred	Vorgängerfunktion (für Positionszähler), 1-stellig.
0	Konstante (Startpunkt für Schritt- und Positionszähler).
R_a	2-stellige Relation für jedes $a \in \Sigma \cup \{\Box\}$; kodiert Bandbeschriftung.
Z_q	1-stellige Relation für jedes $q \in Q$; kodiert Zustand.
K	2-stellige Relation; kodiert Kopfposition.

Ziel ist es, in $\varphi_{\mathcal{M},w}$ die Berechnung von $\mathcal{M}$ auf Eingabe w als Folge $(C_i)_{i\in\mathbb{N}}$ von Konfigurationen zu beschreiben, und zum Ausdruck zu bringen, dass diese Folge *nicht* nach endlich vielen Schritten eine Endkonfiguration erreicht. In den intendierten Modellen von $\varphi_{\mathcal{M},w}$ umfasst der Träger eine isomorphe Kopie der ganzen Zahlen $\mathbb{Z}$, auf denen succ und pred den Nachfolger- und Vorgängerfunktionen entsprechen. Wir denken uns die Bandzellen von $\mathcal{M}$ durch die Elemente $i \in \mathbb{Z}$ numeriert, wobei die Startposition des Kopfes die Zelle 0 sei. Gleichzeitig benutzen wir die Elemente $t \in \mathbb{N} \subseteq \mathbb{Z}$ als Schrittzähler, beginnend mit $t = 0$ für die Startkonfiguration. Die intendierte Interpretation der Relationen R_a, Z_q, K ist wie folgt:

$$\begin{aligned} (t,i) \in R_a &: \text{ in Konfiguration } C_t \text{ steht ein } a \text{ in Zelle } i.\\ t \in Z_q &: \text{ in Konfiguration } C_t \text{ ist } \mathcal{M} \text{ im Zustand } q.\\ (t,i) \in K &: \text{ in Konfiguration } C_t \text{ steht der Kopf bei Zelle } i. \end{aligned}$$

$\varphi_{\mathcal{M},w}$ ist die Konjunktion der folgenden Teilformeln ($\mathsf{succ}^i\, 0$ steht für den Term, der den i-ten Nachfolger des Elements 0 beschreibt, $\mathsf{succ}^0\, 0 := 0$, $\mathsf{succ}^{i+1}\, 0 := \mathsf{succ}\,\mathsf{succ}^i\, 0$):

(Allgemeine Kodierungsbedingungen):

$$\varphi_0 \quad \begin{cases} \forall x \left(\mathsf{pred}\,\mathsf{succ}\, x = x \ \wedge\ \mathsf{succ}\,\mathsf{pred}\, x = x\right) & \\ \forall t \forall y\, \neg(R_a t y \wedge R_{a'} t y) & \text{für } a \neq a' \\ \forall t\, \neg(Z_q t \wedge Z_{q'} t) & \text{für } q \neq q' \\ \forall t \forall y \forall y'\, ((Kty \wedge Kty') \to y = y') & \end{cases}$$

(Startkonfiguration auf $w = a_1 \dots a_n$):

$$\varphi_{\text{start}} \begin{cases} K00 & \\ Z_{q_0}0 & \\ R_{a_i} 0 \mathsf{succ}^i\, 0 & \text{für } 1 \leqslant i \leqslant n \\ \forall y \left((\bigwedge_{i=1}^n \neg y = \mathsf{succ}^i\, 0) \to R_\Box 0 y\right) & \end{cases}$$

(Nachfolgekonfigurationen gemäß Übergangsfunktion δ):

$\varphi_\delta := \forall t \forall t' \left(t' = \mathsf{succ}\, t \to \psi(t,t')\right)$

wobei die Formel $\psi(t,t')$ die Konjunktion der folgenden Formeln ist:

$$\begin{aligned} &\forall y \left((Z_q t \wedge Kty \wedge R_b ty) \to (Z_{q'} t' \wedge Kt' \mathsf{succ}\, y \wedge R_{b'} t' y)\right) && \text{für } \delta(q,b) = (b', >, q') \\ &\forall y \left((Z_q t \wedge Kty \wedge R_b ty) \to (Z_{q'} t' \wedge Kt' \mathsf{pred}\, y \wedge R_{b'} t' y)\right) && \text{für } \delta(q,b) = (b', <, q') \\ &\forall y \left((Z_q t \wedge Kty \wedge R_b ty) \to (Z_{q'} t' \wedge Kt' y \wedge R_{b'} t' y)\right) && \text{für } \delta(q,b) = (b', \circ, q') \\ &\forall y \forall y' \left((Kty \wedge \neg y' = y) \to \textstyle\bigwedge_a (R_a ty' \leftrightarrow R_a t' y')\right) \end{aligned}$$

(Divergente Berechnung):

$\varphi_\infty := \forall t\, \neg(Z_{q^+} t \vee Z_{q^-} t)$

Beobachtung 7.1 Sei $\varphi_{\mathcal{M},w} := \varphi_0 \wedge \varphi_{\text{start}} \wedge \varphi_\delta \wedge \varphi_\infty$.

(a) Wenn $w \xrightarrow{\mathcal{M}} \infty$, so besitzt $\varphi_{\mathcal{M},w}$ ein Modell über $\mathbb{Z}$, in dem succ und pred als die üblichen Nachfolger- und Vorgängerfunktionen interpretiert sind, mit den oben beschriebenen Interpretationen der Relationen R_a, Z_q, K, die die Konfigurationenfolge von $\mathcal{M}$ auf Eingabe w beschreiben. Also ist in diesem Fall $\varphi_{\mathcal{M},w}$ erfüllbar.

(b) Wenn $w \xrightarrow{\mathcal{M}}$ STOP, so hat $\varphi_{\mathcal{M},w}$ kein Modell. Terminiert $\mathcal{M}$ auf Eingabe w im n-ten Schritt, so implizieren die übrigen Konjunktionsglieder $\varphi_0 \wedge \varphi_{\text{start}} \wedge \varphi_\delta$, dass $Z_{q^+}\mathsf{succ}^n\, 0 \vee Z_{q^-}\mathsf{succ}^n\, 0$, also $\neg\varphi_\infty$. Demnach ist $\varphi_{\mathcal{M},w}$ unerfüllbar.

Daraus erhalten wir den Satz von Church und Turing über die Unentscheidbarkeit des sogenannten *klassischen Entscheidungsproblems*.

Satz 7.2 (Church, Turing) *Das Erfüllbarkeitsproblem für* FO *ist unentscheidbar.*

Bem.: Man kann eine verbesserte Reduktion gewinnen, für die die Signatur der Formel $\varphi_{\mathcal{M},w}$ nicht von der Zustandsmenge Q von $\mathcal{M}$ und dem Alphabet Σ abhängt. (Tatsächlich reicht sogar eine Signatur aus einem einzigen 2-stelligen Relationssymbol aus). Da diese Reduktionen zwar nicht schwer aber weniger transparent sind, gehen wir darauf nicht explizit ein.

7.2 Die Sätze von Traktenbrot und von Tarski

Eine kleine Modifikation der obigen Reduktionsidee liefert den Satz von Traktenbrot.

Betrachtet man anstelle der Erfüllbarkeit (SAT) die *Erfüllbarkeit in endlichen Modellen* (FINSAT), so ergibt sich eine genaue Umkehrung der Verhältnisse hinsichtlich rekursiver Aufzählbarkeit. Für endliche Signatur S ist

- die Menge FINSAT(FO(S)) aller FO(S)-Sätze, die ein endliches Modell besitzen, rekursiv aufzählbar.
- die Menge FINSAT(FO(S)) nicht entscheidbar. Also ist das Komplement von FINSAT(FO(S)), und damit auch die Menge der in *über endlichen Strukturen allgemeingültigen* FO(S)-Sätze nicht rekursiv aufzählbar. Es folgt, dass es keinen Beweiskalkül für Allgemeingültigkeit in endlichen Strukturen geben kann (warum?).

Die erste Aussage ergibt sich daraus, dass man systematisch alle endlichen S-Strukturen $\mathcal{A}$ (genauer: alle bis auf Isomorphie) der Reihe nach (mit wachsender Größe) generieren und jeweils $\mathcal{A} \models \varphi$ testen kann, bis man ggf. Erfolg hat.

Die zweite Aussage folgt dann mit dem folgenden Satz.

Satz 7.3 (Traktenbrot) FINSAT(FO) *ist unentscheidbar.*

Beweisidee. Man findet eine Reduktion $\mathcal{M}, w \longmapsto \varphi^{\text{fin}}_{\mathcal{M},w}$ mit

$$w \xrightarrow{\mathcal{M}} \text{STOP} \quad \text{gdw.} \quad \varphi^{\text{fin}}_{\mathcal{M},w} \text{ ein endliches Modell hat.}$$

Dazu kann man etwa das $\varphi_{\mathcal{M},w}$ von oben modifizieren, indem man ein weiteres 2-stelliges Relationssymbol $<$ (für eine endliche lineare Ordnung) und ein weiteres Konstantensymbol $c_{\max}$ (für das größte Element der Ordnung) hinzunimmt. Wir modifizieren die Bedingungen in $\varphi_{\mathcal{M},w}$ wie folgt:

φ^{fin}_0 besage nun, dass $<$ eine lineare Odnung mit kleinstem Element 0 und größtem Element $c_{\max}$ ist; dass $\mathsf{succ}\, x$ für alle $x \neq c_{\max}$ der direkte Nachfolger von x im Sinne von

$<$ ist (und $\mathsf{succ}\,(c_{\max}) = c_{\max}$); dass $\mathsf{pred}\,x$ für alle $x \neq 0$ der direkte Vorgänger ist (und $\mathsf{pred}\,(0) = 0$); dazu Bedingungen hinsichtlich R, Z und K wie in φ_0 oben.
φ_{start} unverändert und $\varphi^{\text{fin}}_{\delta} := \forall t \forall t' \left((t' \neq 0 \wedge \neg Z_{q^+} t \wedge \neg Z_{q^-} t \wedge t' = \mathsf{succ}\, t) \rightarrow \psi(t,t')\right)$ für $\psi(t,t')$ wie oben.
Anstelle von φ_∞ tritt nun der Satz $\varphi_{\text{STOP}} = \exists t Z_{q^+} T \vee Z_{q^-} t$.
Dann hat $\varphi^{\text{fin}}_{\mathcal{M},w} = \varphi^{\text{fin}}_0 \wedge \varphi_{\text{start}} \wedge \varphi^{\text{fin}}_{\delta} \wedge \varphi_{\text{STOP}}$ ein endliches Modell gdw. die Berechnung von $\mathcal{M}$ auf w terminiert.

Eine kompliziertere Modifikation der Reduktionsidee zeigt, dass die Standardstruktur der Arithmetik, $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ über $S = S_{\text{ar}} = \{+, \cdot,), 1, <\}$, ausreichend interne Kodierungsmechanismen hat, dass man zu jeder DTM $\mathcal{M}$ und Eingabe w einen Satz $\varphi^{\text{ar}}_{\mathcal{M},w} \in \text{FO}_0(S_{\text{ar}})$ konstruieren kann, derart dass

$$w \xrightarrow{\mathcal{M}} \infty \quad \text{gdw.} \quad \mathcal{N} \models \varphi^{\text{ar}}_{\mathcal{M},w}.$$

Wir zitieren diesen wichtigen klassischen Satz ohne Beweis.

Satz 7.4 (Tarski)
Die FO*-Theorie der Arithmetik, d.h. die Menge* $\text{Th}(\mathcal{N})$ *aller in* $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ *wahren* $\text{FO}(S_{ar})$*-Sätze ist unentscheidbar (nicht einmal rekursiv aufzählbar, oder durch ein rekursiv aufzählbares Axiomensystem beschreibbar).*

Übung 7.5 Diskutieren Sie, wie die beiden Zusatzaussagen des Satzes direkt aus der Unentscheidbarkeit der Theorie von $\mathcal{N}$ von folgen.
Hinweis: Aus "$\mathcal{N} \models \varphi$ gdw. nicht $\mathcal{N} \models \neg\varphi$" hat man eine Reduktion zwischen der betrachteten Satzmenge und ihrem Komplement; ferner kann man auf die Grundidee der Argumentation zurückgreifen, die uns gezeigt hat, dass die allgemeingültigen FO-Sätze rekursiv aufzählbar sind (vgl. Folgerung 2 in Abschnitt 6.2).

7.3 Ausblick: Entscheidbare Formelklassen, Logiken und Theorien

Entscheidbare Teilklassen von FO Während FO insgesamt ein unentscheidbares Erfüllbarkeitsproblem hat, gibt es eine Reihe von spezielleren Formelklassen in FO, für die das Erfüllbarkeitsproblem entscheidbar ist. Klassisch hat man vor allem sogenannte *Präfixklassen* untersucht, d.h. Klassen von Formeln in pänexer Normalform mit Einschränkungen bezüglich des Quantorenpräfixes und der Signatur. Für relationale Signaturen (Signaturen ohne Funktionssymbole) haben z.B. die folgenden Präfixklassen ein entscheidbares Erfüllbarkeitsproblem

$\forall^*$	universeller Quantorenpräfix
$\exists^*$	existentieller Quantorenpräfix
$\exists^*\forall\forall\exists^*_{\neq}$	Quantorenpräfixe mit zwei $\forall$ in einem Block, ohne $=$

Für viele Formelklassen, die ein entscheidbares Erfüllbarkeitsproblem haben, kann Entscheidbarkeit darauf zurückführen, dass SAT und FINSAT für die betreffende Formelklasse übereinstimmen. Eine Klasse von Formeln hat die *Endliche-Modell-Eigenschaft* (*finite model property*), wenn jede erfüllbare Formel auch ein endliches Modell besitzt. Dann folgt Entscheidbarkeit des Erfüllbarkeitsproblem aus der Semi-Entscheidbarkeit des Komplements von SAT(FO) (rekursive Aufzählbarkeit der allgemeingültigen FO Sätze, siehe Folgerung 2, Seite 32) und von FINSAT(FO) (rekursive Aufzählbarkeit der Sätze, die endliche Modelle besitzen, vgl. Abschnitt 7.2). Auch Modallogiken und die 2-Variablen-Logik FO^2 (s.u.) lassen sich als syntaktische Fragmente von FO mit entscheidbarem Erfüllbarkeitsproblem auffassen.

Entscheidbare Logiken Fragmente von FO mit entscheidbarem Erfüllbarkeitsproblem können in Anwendungen nützlich sein, wenn sie für bestimmte Zwecke ausreichend ausdrucksstark sind. Anwendungsbereiche, in denen Fragmente von FO mit guten algorithmischen Eigenschaften (die Entscheidbarkeit des Erfüllungsproblems ist hier i.d.R. nur eine Minimalforderung) gebraucht werden, sind u.a. die Verifikation und Wissensrepräsentation. Hier spielen Prozesslogiken, temporale Logiken und verschiedene *Modallogiken* eine große Rolle.

Einfache Modallogiken z.B. lassen sich als Fragmente von FO zu Signaturen mit 1- und 2-stelligen Relationssymbolen auffassen, die zur Modellierung von Transitionssystemen (oder auch Wissensrepräsentationssystemen) geeignet sind (vgl. Abschnitt 1: Beispiele, und Abschnitt 8.2: insbesondere Definition 8.21). Charakteristisch für die Modallogik, für die wie ML schreiben, ist die Beschränkung der Quantifizierung. Anstelle einer globalen Quantifizierung mit $\forall x$ oder $\exists x$ über die gesamte Trägermenge der Struktur hat man in ML sogenannte Modalquantoren, die von einem aktuellen Aufpunkt aus gesehen lediglich über alle direkt über Transitionen erreichbaren Elemente quantifizieren. Die auf diese eingeschränkte, lokale Quantifizierung aufgebaute Modallogik hat ein entscheidbares Erfüllbarkeitsproblem (und auch die Endliche-Modell-Eigenschaft).

Ähnliches gilt für das Fragment von $\mathrm{FO}(S)$ über relationalen Signaturen S, in dem nur zwei verschiedene Variablensymbole x und y verwendet werden dürfen, FO^2 (2-Variablen-Logik). Nicht-trivial ist dieses Fragment dadurch, dass man dieselbe Variable wiederholt abquantifizieren kann, wie etwa in der Formel

$$\varphi(x) = \exists y\big(Exy \wedge \exists x(Eyx \wedge \forall y\neg Exy)\big) \ \in \mathrm{FO}^2(\{E\}).$$

(Was besagt diese Fomel über den Knoten x in einem Graphen mit Kantenrelation E?)

Weiter gibt es aber auch viele interssante Logiken, die nicht als Fragmente von FO aufgefasst werden können, da sie z.B. auch gewisse Eigenschaften formalisieren können, die in FO nicht ausdrückbar sind. Ein wichtiges Beispiel ist die Erweiterung der Logik erster Stufe um die Möglichkeit auch über Teilmengen der Trägermenge zu quantifizieren (*monadische Logik zweiter Stufe,* MSO). MSO ist eine Erweiterung von FO, für die es keinen vollständigen Beweiskalkül (im Stile des Sequenzenkalküls für FO) geben kann, da die Menge der allgemeingültigen MSO Sätze nicht mehr rekursiv aufzählbar ist. [Dass MSO nicht rekursiv aufzählbar für Allgemeingültigkeit ist, folgt aus dem Satz von Traktenbrot (Satz 7.3) und der Tatsache, dass es MSO Sätze mit beliebig großen endlichen aber keinen unendlichen Modellen gibt.] Andererseits hat MSO über bestimmten Strukturklassen algorithmisch gute Eigenschaften *und* eine interessante Ausdrucksstärke. So kann man über Wortstrukturen (vgl. Abschnitt 1, Beispiele, und Abschnitt 8.2) in MSO gerade genau diejenigen Eigenschaften von Wörtern definieren, die zu regulären Sprachen gehören (Satz von Büchi, siehe Satz 8.20). In Einschränkung auf (endliche oder auch unendliche) Wortstrukturen wie auch über (endlichen oder unendlichen) Bäumen ist das Erfüllbarkeitsproblem für MSO-Sätze entscheidbar (Satz von Rabin). Die Entscheidbarkeit vieler sehr ausdrucksstarker Temporallogiken und Prozesslogiken lässt sich auf dieses zentrale Resultat zurückführen.

Entscheidbare Theorien Das Verhältnis zwischen entscheidbaren und unentscheidbaren FO Theorien ist auf den ersten Blick oft überraschend. Als FO-Theorie einer S-Struktur $\mathcal{A}$ bezeichen wir die Menge

$$\mathrm{Th}(\mathcal{A}) := \big\{\varphi \in \mathrm{FO}_0(S)\colon \mathcal{A} \models \varphi\big\}.$$

Das zugehörige Entscheidungsproblem ist also, zu gegebenen FO(S)-Sätzen φ zu entscheiden, ob φ in $\mathcal{A}$ wahr ist oder nicht. Für unendliche Strukturen kann man den Wahrheitswert von φ i.d.R. nicht einfach algorithmisch auswerten. Wir haben in Satz 7.4 ein typisches Beispiele einer unentscheidbaren FO-Theorie gesehen: die FO-Theorie der Arithmetik der natürlichen Zahlen, $\mathrm{Th}(\mathcal{N})$ für $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ ist unentscheidbar.

Im Gegensatz dazu ist die FO-Theorie der *reellen Arithmetik*, $\mathrm{Th}(\mathcal{R})$ für $\mathcal{R} = (\mathbb{R}, +, \cdot, 0, 1, <)$, entscheidbar (Tarski); die FO-Theorie der *rationalen Arithmetik*, $\mathrm{Th}(\mathcal{Q})$ für $\mathcal{Q} = (\mathbb{Q}, +, \cdot, 0, 1, <)$, allerdings ist ebenfalls unentscheidbar (J. Robinson).

Entscheidbar ist die FO-Theorie der additiven Arithmetik der natürlichen Zahlen, $\mathrm{Th}((\mathbb{N}, +, 0))$ (Presburger, daher auch: *Presburger Arithmetik*).

Ebenso kann man FO-Theorien von interessanten S-Strukturklassen betrachten. Ist die betreffende Klasse in FO(S) axiomatisiert, so ist ihre FO-Theorie gerade die Menge aller FO(S)-Sätze, die aus den Axiomen folgen (ableitbar sind). Für endliche (oder rekursiv aufzählbare) Axiomatisierungen ergibt sich so die rekursive Aufzählbarkeit der betreffenden Theorie aus dem Vollständigkeitssatz (nämlich wie?). Dies gilt zum Beispiel für die Theorie der Gruppen, oder die Theorie der abelschen (kommutativen) Gruppen. Interessanterweise ist hier die Theorie der Gruppen unentscheidbar (Tarski), die Theorie der abelschen Gruppen dagegen entscheidbar (Szmielew).

8 Fragen der Ausdrucksstärke

Für die Anwendung von unterschiedlichen Logiken sind vor allem folgende Kriterien wesentlich:

- Ausdrucksstärke: welche Struktureigenschaften sind in der Logik formalisierbar?
- algorithmische Eigenschaften: Entscheidbarkeit und Komplexität des Erfüllbarkeitsproblems, Komplexität der Formelauswertung (model checking complexity), usw.

Gute Logiken müssen für ihren Einsatzbereich ausreichend ausdrucksstark sein und sollen gleichzeitig noch günstige algorithmische Eigenschaften haben. Diese Aspekte sind gegenläufig, und man muss in der Regel zweckbezogen abwägen, welche Logik für bestimmte Zwecke geeignet ist. Mit der Analyse der Ausdrucksstärke, also der Frage, *was* in einer Logik über Strukturen eines vorgegebenen Typs ausdrückbar ist, befasst sich in der mathematischen Logik die Teildisziplin der *Modelltheorie*. Während die Ausdrückbarkeit einer gegebenen Struktureigenschaft i.d.R. direkt durch Angabe einer entsprechenden Formel erbracht werden kann, braucht man besondere Techniken, um nachzuweisen, dass eine gegebene Struktureigenschaft *nicht* ausdrückbar ist. Wir haben im Rahmen der Logik erster Stufe bereits ein Instrument für diesen Zweck kennengelernt: der Kompaktheitssatz kann häufig benutzt werden, um indirekt nachzuweisen, dass kein FO Satz (oder nicht einmal eine FO-Satzmenge) eine bestimmte Eigenschaft formalisieren kann.

Beispiel 8.1 Zusammenhang von Graphen (also die Eigenschaft, dass je zwei Knoten durch einen Pfad verbunden sind) ist nicht FO-definierbar. Wir nehmen an es gäbe $\Phi \subseteq \mathrm{FO}_0(\{E\})$ derart, dass eine Struktur $\mathcal{G} = (V, E)$ mit Knotenmenge V und Kantenrelation $E \subseteq V \times V$ zusammenhängend ist gdw. $\mathcal{G} \models \Phi$. Wir wollen diese Annahme zum Widerspruch führen.

Für $n \in \mathbb{N}$ besage die Formel $\varphi_n(x, y) \in \mathrm{FO}(\{E\})$ dass es einen Pfad der Länge $\leqslant n$ von x nach y gibt. Die $\varphi_n(x, y)$ kann man induktiv leicht erhalten, indem man

etwa $\varphi_0(x,y) := x = y$ und $\varphi_{n+1}(x,y) := \varphi_n(x,y) \vee \exists z(\varphi_n(x,z) \wedge Ezy)$ setzt. Dann wäre für zwei zusätzliche Konstantensymbole c und d die unendliche Satzmenge $\Phi \cup \{\neg\varphi_n(c,d) \colon n \in \mathbb{N}\}$ erfüllbar (Kompaktheit! Man überlege sich die Details). Andererseits kann kein Modell von $\{\neg\varphi_n(c,d) \colon n \in \mathbb{N}\}$ zusammenhängend sein; Widerspruch.

Nicht immer jedoch kommt man mit Kompaktheit durch. Insbesondere kann man z.B. nicht mittels Kompaktheit nachweisen, dass es keinen FO($\{E\}$)-Satz gibt, der für *endliche* Graphen gerade besagt, dass sie zusammenhängend sind.[1]

Eine weitreichende und nützliche Methode zur Analyse der Ausdrucksstärke verschiedenster Logiken auch über speziellen Strukturklassen bieten *Ehrenfeucht-Fraïssé Spiele*. Wir erläutern diese Methode für FO über (den besonders einfachen) Wortstrukturen. Danach folgt dann ein Ausblick auf Varianten und Erweiterungen für zwei für die Logik in der Informatik besonders wichtige Bereiche: die monadische Logik zweiter Stufe (MSO) über Wortstrukturen und die Modallogik (ML) über Transitionssystemen.

8.1 Ehrenfeucht-Fraïssé Spiele

Zur Erinnerung: Der Quantorenrang einer FO-Formel misst die Schachtelungstiefe von Quantoren, Definition 2.3. Wir beschränken uns der Einfachheit halber im Folgenden meist auf Wortstrukturen. Alle unsere Betrachtungen lassen sich aber unmittelbar auf allgemeine endliche relationale Signaturen übertragen.

Zu Wortstrukturen vgl. Abschnitt 1, Seite 3. Wortstrukturen (zum Alphabet Σ) sind endliche Strukturen zu einer relationalen Signatur $S = \{<\} \cup \{P_a \colon a \in \Sigma\}$ mit zweistelligem $<$ und einstelligen P_a, in denen $<$ als lineare Ordnung der endlichen Trägermenge interpretiert wird, und in denen die P_a die Trägermenge disjunkt zerlegen. (Die Trägermenge mit ihrer Ordnung indiziert die Positionen im zugehörigen Wort, P_a markiert diejenigen Positionen, in denen der Buchstabe a steht.)

Wir bezeichnen Strukturen oder Parametertupel in Strukturen als q-äquivalent falls sie sich in keiner Eigenschaft unterscheiden, die mit Quantorenrang $\leqslant q$ in FO ausdrückbar ist.

Definition 8.2 Sei $q \in \mathbb{N}$.
Zwei S-Strukturen $\mathcal{V}$ und $\mathcal{W}$ heissen *q-äquivalent*, $\mathcal{V} \equiv_q \mathcal{W}$, falls

$$\mathcal{V} \models \varphi \quad \Leftrightarrow \quad \mathcal{W} \models \varphi \qquad \text{für alle FO}(S)\text{-Sätze } \varphi \text{ mit } \mathrm{qr}(\varphi) \leqslant q.$$

Für S-Strukturen mit ausgezeichneten Parametertupeln $\mathbf{m} = (m_1, \ldots, m_k)$ in $\mathcal{V}$ und $\mathbf{n} = (n_1, \ldots, n_k)$ in $\mathcal{W}$ entsprechend: $\mathcal{V}, \mathbf{m} \equiv_q \mathcal{W}, \mathbf{n}$, falls

$$\mathcal{V} \models \varphi[\mathbf{m}] \quad \Leftrightarrow \quad \mathcal{W} \models \varphi[\mathbf{n}] \qquad \text{für alle FO}(S)\text{-Formeln } \varphi \text{ mit } \mathrm{qr}(\varphi) \leqslant q.$$

Offenbar ist $\equiv_q$ für jedes q und k eine Äquivalenzrelation über der Klasse der S-Strukturen mit k ausgezeichneten Parametern. Für endliche relationale S haben diese Äquivalenzrelationen nur endlich viele Äquivalenzklassen (endlichen Index).

Beobachtung 8.3 Für endliches relationales S und feste $k, q \in \mathbb{N}$ gibt es jeweils bis auf logische Äquivalenz nur endlich viele Formeln vom Quantorenrang $\leqslant q$ in $\mathrm{FO}_k(S)$.

[1] Warum nicht? Hinweis: Die Nebenbedingung der Endlichkeit ist ihrerseits nicht in FO erfassbar; in Beschränkung auf endliche Strukturen steht Kompaktheit für FO nicht zur Verfügung; es gibt FO-Satzmengen ohne endliche Modelle, deren endliche Teilmengen aber endliche Modelle besitzen (Beispiel?). Mit den Besonderheiten, die sich aus der in der Informatik häufig wesentlichen Beschränkung auf endliche Strukturen ergeben, befasst sich die sogenannte *Endliche Modelltheorie*.

Übung 8.4 Zeigen Sie, dass jede Formel vom Quantorenrang $q+1$ in $\mathrm{FO}_k(S)$ logisch äquivalent ist zu einer Konjunktion von Formeln vom Quantorenrang $\leqslant q$ in $\mathrm{FO}_k(S)$ und Formeln der Gestalt $\exists x_{k+1}\varphi$ bzw. $\forall x_{k+1}\varphi$ für Formeln φ vom Quantorenrang $\leqslant q$ in $\mathrm{FO}_{k+1}(S)$. Weisen Sie damit nach, dass alle $\equiv_q$ endlichen Index haben.

Definition 8.5 Zwei Parametertupel $\mathbf{m} = (m_1, \ldots, m_k)$ in $\mathcal{V}$ und $\mathbf{n} = (n_1, \ldots, n_k)$ in $\mathcal{W}$ heissen *lokal isomorph* falls die Abbildung $\rho\colon (m_i \mapsto n_i)_{1\leqslant i\leqslant k}$ eine Bijektion ist, die mit den Interpretationen aller Relationen in $\mathcal{V}$ und $\mathcal{W}$ verträglich ist (also ein Isomorphismus der Substrukturen, die von den Tupeln $\mathbf{m}$ und $\mathbf{m}'$ gebildet werden).

Im Fall von Wortstrukturen verlangt die Verträglichkeitsbedingung, dass $m_i <^{\mathcal{V}} m_j$ gdw. $n_i <^{\mathcal{W}} n_j$ (Verträglichkeit mit $<$) und dass $m_i \in P_a^{\mathcal{V}}$ gdw. $n_i \in P_a^{\mathcal{W}}$ (Verträglichkeit mit P_a für $a \in \Sigma$).

Insbesondere für zwei strikt aufsteigend angeordnete Tupel $\mathbf{m}$ bzw. $\mathbf{n}$ in Wortstrukturen $\mathcal{V}$ und $\mathcal{W}$ zu Σ-Wörtern $v = a_1 \ldots a_s$ und $w = b_1 \ldots b_t$: $\mathbf{m}$ und $\mathbf{n}$ sind lokal isomorph genau dann, wenn die "Auszugswörter" in diesen Positionen gleich sind $a_{m_1} \ldots a_{m_k} = b_{n_1} \ldots b_{n_k}$. (Warum?)

Übung 8.6 Zeigen Sie, dass $\mathbf{m} = (m_1, \ldots, m_k)$ in $\mathcal{V}$ und $\mathbf{n} = (n_1, \ldots, n_k)$ in $\mathcal{W}$ lokal isomorph sind gdw. $\mathcal{V}, \mathbf{m} \equiv_0 \mathcal{W}, \mathbf{n}$.

Das Spiel Das Ehrenfeucht-Fraïssé Spiel ist ein kombinatorisches Spiel zwischen zwei Spielern, die wir mit **I** und **II** bezeichnen. Das Spiel dient der vergleichenden Analyse zweier Strukturen $\mathcal{W}$ und $\mathcal{W}'$, über denen das Spiel ausgetragen wird. Dabei markieren die Spieler Elemente der beiden Strukturen, wodurch endliche Konfigurationen von Elementen verglichen werden. Man kann sich vorstellen, dass die betreffenden Elemente durch Spielsteine markiert werden, daher auch englisch "pebble game". Die Regeln sind so, dass **I** versuchen muss, strukturelle Unterschiede zwischen $\mathcal{W}$ und $\mathcal{W}'$ herauszustellen, während **II** versucht, nachzuweisen, dass $\mathcal{W}$ und $\mathcal{W}'$ ununterscheidbar sind.

Für das Spiel über den S-Strukturen $\mathcal{W}$ und $\mathcal{W}'$:

Spielkonfigurationen: korrespondierende Tupel ausgezeichneter Elemente in $\mathcal{W}$ und $\mathcal{W}'$; wir schreiben $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ mit $\mathbf{m} = (m_1, \ldots, m_k)$ und $\mathbf{m}' = (m'_1, \ldots, m'_k)$ für eine typische Konfiguration, in der über $\mathcal{W}$ und $\mathcal{W}'$ jeweils k Elemente markiert sind.

Spielzüge: In jeder neuen Runde wählt **I** eine der beiden Strukturen und markiert in der gewählten Struktur ein weiteres Element; **II** markiert in der anderen Struktur ein Element. Eine einzelne Runde führt so von einer Konfiguration mit je k markierten Elementen $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ zu einer Nachfolgekonfiguration der Form $(\mathcal{W}, \mathbf{m}, m_{k+1}; \mathcal{W}', \mathbf{m}', m'_{k+1})$, in der gerade ein zusätzliches Paar (m_{k+1}, m'_{k+1}) markiert wurde.

Gewinnbedingung: **II** verliert sobald in der aktuellen Konfiguration kein lokaler Isomorphismus vorliegt, d.h., wenn $\mathcal{W}, \mathbf{m} \not\equiv_0 \mathcal{W}', \mathbf{m}'$.

Die Gewinnbedingung besagt, dass **II** so antworten muss, dass die markierten Elemente jeweils lokal isomorph in $\mathcal{W}$ und $\mathcal{W}'$ liegen.

Im *q-Runden-Spiel* auf $\mathcal{W}$ und $\mathcal{W}'$, $G^q(\mathcal{W}, \mathcal{W}')$, werden bis zu q Runden nach obigem Protokoll gespielt. Spieler **II** gewinnt eine solche Partie, falls sie durch alle q Runden hindurch antworten kann, ohne die Gewinnbedingung zu verletzen; und **I** gewinnt wenn im

Laufe der Partie nicht lokal isomorphe Konfigurationen auftreten. Das q-Runden-Spiel $G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ mit bereits ausgezeichneten Tupeln $\mathbf{m}$ und $\mathbf{m}'$ in der Startkonfiguration $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ ist analog definiert.

Wir sagen dass **I** beziehungsweise **II** eine *Gewinnstrategie* im Spiel $G^q(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ hat, wenn der betreffende Spieler in jeder Partie Gewinn erzwingen kann. Am klarsten ist die induktive Definition, z.B. für Spieler **II**: **II** hat eine Gewinnstrategie in $G^0(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ wenn die Gewinnbedingung nicht schon in der Startkonfiguration verletzt ist; **II** hat eine Gewinnstrategie in $G^{q+1}(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ wenn sie jeden möglichen ersten Zug von **I** so beantworten kann, dass sie für das Restspiel $G^q(\mathcal{W}, \mathbf{m}, m; \mathcal{W}', \mathbf{m}', m')$ eine Gewinnstrategie hat.

Bemerkung: Man vergleiche den Aufbau dieses Struktur-Vergleichs-Spiels (back-and-forth game) mit dem Semantik-Spiel (model checking game) in Abschnitt 2.4.

Satz 8.7 (Ehrenfeucht-Fraïssé) *Für alle $q \in \mathbb{N}$ und S-Strukturen $\mathcal{W}$ und $\mathcal{W}'$ mit Tupeln $\mathbf{m} = (m_1, \ldots, m_k)$ in $\mathcal{W}$ und $\mathbf{m}' = (m'_1, \ldots, m'_k)$ in $\mathcal{W}'$ sind äquivalent:*

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

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

Beweis Für (i) $\Rightarrow$ (ii) zeigen wir induktiv über q, dass **I** eine Gewinnstrategie hat, wenn $\mathcal{W}, \mathbf{m} \not\equiv_q \mathcal{W}', \mathbf{m}'$.

Induktionsanfang, $q = 0$. Für $q = 0$ (0 Runden) hat **I** eine Strategie gdw. **II** schon in der Startkonfiguration $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ verloren hat. Dies ist genau dann der Fall, wenn $\mathcal{W}, \mathbf{m}$ und $\mathcal{W}', \mathbf{m}'$ nicht lokal isomorph sind, d.h., wenn $\mathcal{W}, \mathbf{m} \not\equiv_0 \mathcal{W}', \mathbf{m}'$ (vgl. Übung 8.6).

Induktionsschritt von q nach $q+1$. Sei $\mathcal{W}, \mathbf{m} \not\equiv_{q+1} \mathcal{W}', \mathbf{m}'$. Also existiert ein $\varphi(\mathbf{x}) \in \mathrm{FO}(S)$ mit $\mathrm{qr}(\varphi) \leqslant q+1$ so dass $\mathcal{W} \models \varphi[\mathbf{m}]$ aber $\mathcal{W}' \not\models \varphi[\mathbf{m}']$ (oder umgekehrt). Wenn φ sogar von kleinerem Quantorenrang als $q+1$ ist, so liefert die Induktionsannahme, dass **I** sogar schon in weniger als $q+1$ Runden gewinnen kann. Wenn φ eine Konjunktion bzw. eine Disjunktion ist, so können wir anstelle von φ eines der Konjunktions- bzw. Disjunktionsglieder von φ zur Unterscheidung benutzen; wenn $\varphi = \neg\psi$ ist, so können wir anstelle von φ auch ψ benutzen. O.B.d.A. können wir also annehmen, dass φ von der Form $\varphi(\mathbf{x}) = \exists z \psi(\mathbf{x}, z)$ mit $\mathrm{qr}(\psi) = q$ ist.

Wir nehmen an, dass $\mathcal{W} \models \varphi[\mathbf{m}]$ und $\mathcal{W}' \not\models \varphi[\mathbf{m}']$ (der umgekehrte Fall ist symmetrisch). Das bedeutet, dass es in $\mathcal{W}$ ein Element m gibt mit $\mathcal{W} \models \psi[\mathbf{m}, m]$, während in $\mathcal{W}'$ für alle m' gilt $\mathcal{W}' \not\models \psi[\mathbf{m}', m']$. Wenn also **I** in der ersten Runde von $G^{q+1}(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ in $\mathcal{W}$ das Element m markiert, so führt *jeder* Antwortzug von **II** zu einer Konfiguration $(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$, in der $\mathcal{W}, \mathbf{m} \not\equiv_q \mathcal{W}', \mathbf{m}'$. Nach Induktionsannahme hat also **I** eine Gewinnstrategie für die verbleibenden q Runden, d.h. im Restspiel $G^q(\mathcal{W}, \mathbf{m}, m; \mathcal{W}', \mathbf{m}', m')$. Insgesamt hat daher **I** eine Gewinnstrategie in $G^{q+1}(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$.

Für (ii) $\Rightarrow$ (i) zeigen wir induktiv über q, dass **II** eine Gewinnstrategie hat, wenn $\mathcal{W}, \mathbf{m} \equiv_q \mathcal{W}', \mathbf{m}'$.

Der Induktionsanfang für $q = 0$ ist wieder mit Übung 8.6 offensichtlich.

Für den Induktionsschritt von q nach $q+1$ sei nun $\mathcal{W}, \mathbf{m} \equiv_{q+1} \mathcal{W}', \mathbf{m}'$. Wir müssen zeigen, dass **II** zu jedem Zug von **I** in der ersten Runde des Spieles $G^{q+1}(\mathcal{W}, \mathbf{m}; \mathcal{W}', \mathbf{m}')$ eine Antwort hat, die zu einer Konfiguration $(\mathcal{W}, \mathbf{m}, m; \mathcal{W}', \mathbf{m}', m')$ mit $\mathcal{W}, \mathbf{m}, m \equiv_q \mathcal{W}', \mathbf{m}', m'$ führt.

Wir nehmen z.B. an, das **I** auf ein m in $\mathcal{W}$ zieht (der Fall, dass **I** ein m' in $\mathcal{W}'$ markiert ist hierzu symmtrisch). Angenommen, kein m' in $\mathcal{W}'$ ist so, dass $\mathcal{W}, \mathbf{m}, m \equiv_q \mathcal{W}', \mathbf{m}', m'$.

Das heisst, zu jedem m' existiert eine Formel $\varphi_{m'}(\mathbf{x}, z)$ von Quantorenrang $\leqslant q$, derart dass $\mathcal{W} \models \varphi_{m'}[\mathbf{m}, m]$ aber $\mathcal{W}' \not\models \varphi_{m'}[\mathbf{m}', m']$.[2] Wir betrachten nun die Formel

$$\varphi(\mathbf{x}) := \exists z \bigwedge_{m' \in \mathcal{W}'} \varphi_{m'}(\mathbf{x}, z).$$

Offenbar ist $\mathrm{qr}(\varphi) \leqslant q+1$ und $\mathcal{W} \models \varphi[\mathbf{m}]$, da ja $\mathcal{W} \models \varphi_{m'}[\mathbf{m}, m]$ für alle m'. Mit $\mathcal{W}, \mathbf{m} \equiv_{q+1} \mathcal{W}', \mathbf{m}'$ folgt, dass auch $\mathcal{W}' \models \varphi[\mathbf{m}']$. Dies steht aber im Widerspruch zur Wahl der $\varphi_{m'}$, denn *jedes* $m' \in \mathcal{W}'$ macht ja gerade $\varphi_{m'}[\mathbf{m}', m']$ *nicht* wahr. □

Übung 8.8 Man kann zu $\mathcal{W}, \mathbf{m}$ und q eine Formel $@^q_{(\mathcal{W},\mathbf{m})}(\mathbf{x})$ vom Quantorenrang q konstruieren, derart dass für alle $\mathcal{W}', \mathbf{m}'$ gilt:

$$\mathcal{W}, \mathbf{m} \equiv_q \mathcal{W}', \mathbf{m}' \;\Leftrightarrow\; \mathcal{W}' \models @^q_{(\mathcal{W},\mathbf{m})}[\mathbf{m}'].$$

Geben Sie an, wie man $@^0_{(\mathcal{W},\mathbf{m})}(\mathbf{x})$ zu gegebenem $\mathcal{W}, \mathbf{m}$ bekommt, und überlegen Sie sich anhand des Spiels ein Rezept, wie man die Formel $@^{q+1}_{(\mathcal{W},\mathbf{m})}(\mathbf{x})$ aus breits gewonnenen Formeln $@^q_{(\mathcal{W},\mathbf{m},m)}(\mathbf{x}, z)$ für $m \in \mathcal{W}$ bilden kann. Geben Sie Formeln $@^q_{(\mathcal{W},\mathbf{m})}(\mathbf{x})$ konkret an zur Wortstruktur $\mathcal{W}$ zum Wort $w = aabaaa$ und für $q = 0, 1, 2$ für einige Parameterwahlen $\mathbf{m}$. Man mache sich anhand des Spiels klar, welche Positionen bzw. Paare von Positionen $\mathbf{m}$ bis zu welchem $q \leqslant 2$ ununterscheidbar sind und worauf es im Spiel $G^2(\mathcal{W}; \mathcal{W})$ ankommt.

Übung 8.9 Bis zu welchem Grade sind die Wortstrukturen zu den Wörtern $w = aaabbbaaabbbaaa$ und $w' = aaabbbaabbaabbbaaa$ äquivalent? Analysieren Sie Spielverläufe und Strategien um diese Frage präzise zu beantworten. Geben Sie einen Satz von möglichst geringem Quantorenrang an, der diese Wortstrukturen unterscheidet.

Beispiele Als einfache aber typische Beispiele zur Anwendung der Ehrenfeucht-Fraïssé Technik wollen wir nachweisen:

- es gibt keinen FO-Satz, der von Wortstrukturen zum Ausdruck bringt, dass sie gerade Länge haben (eine der einfachsten regulären Bedingungen an Worte!).
- es gibt keinen FO-Satz, der von endlichen Graphen zum Ausdruck bringt, dass sie zusammenhängend sind.

Für den erste Punkt untersuchen wir q-Äquivalenz über nackten endlichen linearen Ordnungen. Man kann aber natürlich statt dessen auch an Wortstrukturen zu einem Alphabet mit nur einem Buchstaben denken. Für $n \geqslant 1$ sei $\mathcal{O}_n := \big(\{1, \ldots, n\}, <\big)$ mit der Einschränkung der üblichen linearen Ordnung $<$ auf den natürlichen Zahlen.

(†) Frage: Für welche n, n' gilt $\mathcal{O}_n \equiv_q \mathcal{O}_{n'}$?

Wir stellen zunächst fest, dass für Wortstrukturen allgemein $\equiv_q$ mit Konkatenation (dem Hintereinanderfügen) verträglich ist. Also induziert $\equiv_q$ eine Kongruenzrelation auf dem Wortmonoid, das von Σ^* mit der Konkatenationsoperation gebildet wird (vgl. FG I).

[2] Im Falle von Wortstrukturen gibts es nur endliche viele Auswahlen für m', da W' endlich ist; aber auch in unendlichen Strukturen zu einer endlichen relationalen Signatur S gibt es nach Beobachtung 8.3 – bis auf logische Äquivalenz – nur endlich viele $\varphi_{m'}$. So ist die angegebene Formel φ auch in diesem Fall als eine endliche Konjunktion verfügbar.

Zu linear geordneten $\mathcal{A} = (A, <^{\mathcal{A}}, \ldots)$ und $\mathcal{B} = (B, <^{\mathcal{B}}, \ldots)$ mit disjunkten Trägermengen sei $\mathcal{A} \oplus \mathcal{B}$ die linear geordnete Struktur $(A \cup B, <^{\mathcal{A}\oplus\mathcal{B}}, \ldots)$, die man erhält indem man $\mathcal{B}$ im Sinne der Ordnung hinten an $\mathcal{A}$ anfügt, d.h. mit der Interpretation

$$<^{\mathcal{A}\oplus\mathcal{B}} := \; A \times B \; \cup \; <^{\mathcal{A}} \; \cup \; <^{\mathcal{B}},$$

für die zusammengesetzte lineare Ordnung und der disjunkten Vereinigung der Interpretationen für die übrigen Relationen. Die gewählte Interpretation $<^{\mathcal{A}\oplus\mathcal{B}}$ führt gerade dazu, dass A und B angeordnet sind wie zuvor und dass A im Sinne der Ordnung vor B kommt. Sind $\mathcal{A}$ und $\mathcal{B}$ nicht bereits disjunkt, so ersetzt man sie durch isomorphe disjunkte Kopien.

Beispiel 8.10 Sind $\mathcal{V}$ und $\mathcal{W}$ Wortstrukturen zu Σ-Wörtern v und w, so ist $\mathcal{V} \oplus \mathcal{W} \simeq \mathcal{U}$ für $u := v \cdot w$. Natürlich ist insbesondere auch $\mathcal{O}_n \oplus \mathcal{O}_m \simeq \mathcal{O}_{n+m}$.

Beobachtung 8.11 Für Wortstrukturen $\mathcal{V}$, $\mathcal{W}$ und $\mathcal{V}'$, $\mathcal{W}'$ mit Parametertupeln passender Längen gilt:

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

Zur Begründung überlegt man sich, wie man aus Gewinnstrategien in $G^q(\mathcal{V}, \mathbf{m}; \mathcal{V}', \mathbf{m}')$ und $G^q(\mathcal{W}, \mathbf{n}; \mathcal{W}', \mathbf{n}')$ eine Gewinnstrategie für **II** im Spiel über $\mathcal{V} \oplus \mathcal{W}$ und $\mathcal{V}' \oplus \mathcal{W}'$ zusammensetzen kann.

Beobachtung 8.12 Zu $q \geqslant 1$ existieren Sätze $\varphi_q \in \mathrm{FO}_0(\{<\})$ vom Quantorenrang q derart dass $\mathcal{O}_n \models \varphi_q$ gdw. $n \geqslant 2^q - 1$.

Beweis Der (allgemeingültige) Satz $\varphi_1 := \exists x \; x = x$ ist wie gewünscht für $q = 1$. Induktiv setze $\varphi_{q+1} := \exists z\big([\varphi_q]^{<z} \wedge [\varphi_q]^{>z}\big)$. Hierbei sei z eine Variable, die nicht in φ_q vorkommt und $[\varphi_q]^{<z}$ entstehe aus φ_q indem man jede Quantifizierung der Form $\exists x \ldots$ durch $\exists x(x < z \wedge \ldots)$ ersetzt und analog $\forall x \ldots$ durch $\forall x(x < z \to \ldots)$; $[\varphi_q]^{>z}$ ist analog mit $x > z$ anstatt $x < z$ definiert. Dann besagt φ_{q+1} in einer linearen Ordnung gerade, dass es ein Element m gibt, derart dass der Teil unterhalb m und ebenso der Teil oberhalb m jeweils mindestens $2^q - 1$ Elemente haben; insgesamt also mindestens $2(2^q - 1) + 1 = 2^{q+1} - 1$ viele Elemente. □

Übung 8.13 Geben Sie die Sätze φ_q für kleine Werte von q konkret an.

Als partielle Antwort auf unsere Frage (†) sehen wir also zumindest schon, dass

$$\mathcal{O}_n \not\equiv_q \mathcal{O}_{n'} \quad \text{wenn } n < 2^q - 1 \text{ und } n' \geqslant 2^q - 1.$$

Man kann auch zeigen, dass $\mathcal{O}_n \not\equiv_q \mathcal{O}_{n'}$ für $n < n' < 2^q - 1$ gilt (s.u.). Können Sie Spieler **I** schon hier eine entsprechende Strategie empfehlen?

Wir schreiben $d \stackrel{q}{=} d'$ für die Bedingung dass $d = d'$ oder $d, d' \geqslant 2^q - 1$.

In $\mathcal{O}_n$ sind im Folgenden für $1 \leqslant m_1 < m_2 < \cdots m_k \leqslant n$ die Anzahlen von Elementen in den durch die m_i gebildeten Abschnitten wichtig:

0-ter Abschnitt,	$x < m_1$:	$d_0 := m_1 - 1$ Elemente
i-ter Abschnitt,	$m_i < x < m_{i+1}$:	$d_i := m_{i+1} - (m_i + 1)$ Elemente
k-ter Abschnitt,	$x > m_k$:	$d_k := n - m_k$ Elemente

Für den Fall $k = 0$ (keine Parameter) ist sinngemäß $d_0 = n$ zu setzen.

Lemma 8.14 *Sei $q \in \mathbb{N}$. Zu $\mathcal{O}_n$ und $\mathcal{O}_{n'}$ mit Parametern $\mathbf{m} = m_1 < \ldots < m_k$ in $\mathcal{O}_n$ und $\mathbf{m} = m'_1 < \ldots < m'_k$ in $\mathcal{O}_{n'}$ seien d_i und d'_i die Anzahlen von Elementen in den entsprechenden Abschnitten wie oben. Dann gilt:*

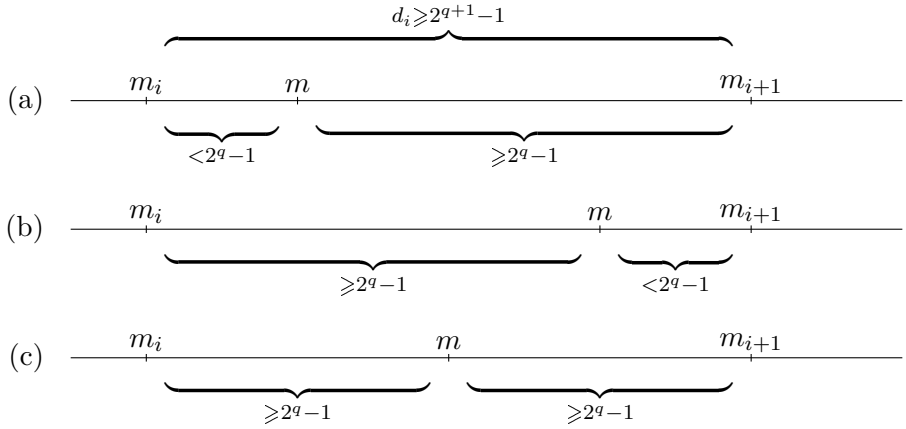
$$\mathcal{O}_n, \mathbf{m} \equiv_q \mathcal{O}_{n'}, \mathbf{m}' \quad \text{gdw.} \quad d_i \stackrel{q}{=} d'_i \text{ für } i = 0, \ldots k.$$

Korollar 8.15 *$\mathcal{O}_n \equiv_q \mathcal{O}_{n'}$ gdw. $n \stackrel{q}{=} n'$. Insbesondere gilt dies also für alle $n, n' \geqslant 2^q - 1$. Für $n = 2^q - 1$ (ungerade) und $n' = 2^q$ (gerade) sieht man also, dass kein Satz vom Quantorenrang q die Ordnungen gerader Länge von den Ordnungen ungerader Länge trennen kann. Demnach ist "gerade Länge" als Eigenschaft endlicher linearer Ordnungen (oder von Wortstrukturen) nicht in* FO *ausdrückbar.*

Beweis [des Lemmas, per Induktion über q.]
Für $q = 0$ sind rechte und linke Seite der behaupteten Äquivalenz beide stets wahr.
Induktionsschritt von q nach $q + 1$.

(1) Seien $\mathcal{O}_n, \mathbf{m}$ und $\mathcal{O}_{n'}, \mathbf{m}'$ mit $d_i \stackrel{q+1}{=} d'_i$, $i = 0, \ldots, k$ gegeben. Wir weisen nach, dass **II** eine Strategie in $G^{q+1}(\mathcal{O}_n, \mathbf{m}; \mathcal{O}_{n'}, \mathbf{m}')$ hat. Dazu geben wir an, wie jeder mögliche erste Zug von **I** so beantwortet werden kann, dass **II** im Restspiel eine Gewinnstrategie hat. Aus Symmetriegründen reicht es, z.B. den Fall zu betrachten, dass **I** ein m in $\mathcal{O}_n$ markiert. Falls $m = m_i$ mit einem der bereits markierten Elemente übereinstimmt, liefert die Antwort $m' := m'_i$ natürlich eine Gewinnstrategie. Andernfalls fällt m ins Innere eines der durch die m_i gebildeten Abschnitte; offenbar muss **II** seine Antwort im Inneren des entsprechenden Abschnitts von $\mathcal{O}_{n'}$ wählen (warum?). Der relevante Abschnitt sei der i-te Abschnitt, der in $\mathcal{O}_n$ die Länge d_i, in $\mathcal{O}_{n'}$ die Länge d'_i hat. Wir wissen dass $d_i \stackrel{q+1}{=} d'_i$ ist. Falls $d_i = d'_i$ sind die betrachteten Abschnitte isomorph und **II** kann einfach anhand dieser Isomorphie ziehen. Für das Restspiel gilt automatisch die Bedingung auf der rechten Seite mit $\stackrel{q}{=}$.

Falls $d_i, d'_i \geqslant 2^{q+1} - 1$, sehen wir uns die Unterteilung des i-ten Abschnitts durch das neue Element m an. Hinsichtlich der Unterteilung gibt es drei Möglichkeiten im Vergleich zur kritischen Schranke $2^q - 1$ sind:



Man beachte hierzu, dass höschtens einer der zwei neuen Teilabschnitte weniger als $2^q - 1$ Elemente enthalten kann, da $2(2^q - 2) + 1 < 2^{q+1} - 1 \leqslant d_i$ ist.

Wenn (wie in (a)) der untere Abschnitt weniger als $2^q - 1$ Elemente hat, so wählt **II** seine Antwort m' so, dass dort der untere Teilabschnitt des i-ten Abschnitts genau dieselbe Länge hat. Die oberen Teilabschnitte haben dann beiderseits Längen $\geqslant 2^q - 1$; also ist die Bedingung für das Restspiel mit $\stackrel{q}{=}$ erfüllt.

Wenn (wie in (b)) der obere Teilabschnitt weniger als $2^q - 1$ Element hat, verfährt man analog.

Wenn (wie in (c)) beide Teilabschnitte mindestens $2^q - 1$ Elemente haben, so findet **II** auch im i-ten Abschnitt von $\mathcal{O}_{n'}$ ein Element m', das beiden Teilabschnitten eine Länge $\geqslant 2^q - 1$ gibt, sodass die Bedingung für das Restspiel mit $\stackrel{q}{=}$ erfüllt ist.

(2) Seien nun umgekehrt $\mathcal{O}_n, \mathbf{m}$ und $\mathcal{O}_{n'}, \mathbf{m}'$ so dass für mindestens ein i nicht $d_i \stackrel{q+1}{=} d_i'$ gilt. Wir weisen nach, dass in diesem Fall **I** eine Strategie in $G^{q+1}(\mathcal{O}_n, \mathbf{m}; \mathcal{O}_{n'}, \mathbf{m}')$ hat. Sei z.B. $d_i' < 2^{q+1} - 1$ und $d_i' < d_i$. Dann markiere **I** ein Element m im i-ten Abschnitt von $\mathcal{O}_n$ derart dass beide Teilabschnitte mindestens $\lfloor (d_i - 1)/2 \rfloor$ Elemente haben. Man prüft nach, dass daraus folgt, dass für jede Antwort m' von **II** im i-ten Abschnitt von $\mathcal{O}_{n'}$ mindestens einer der beiden neuen Teilabschnitte die Längenbedingung für $\stackrel{q}{=}$ verletzt (da d_i' zu klein ist). Wenn **I** in dieser Manier fortfährt ergibt sich im Laufe der q weiteren Runden eine Situation wo ein Abschnitt auf der einen Seite auf Länge 0 geschrumpft ist, während **I** auf der anderen Seite im entsprechenden Abschnitt noch ein Element markieren kann. In dieser Situation verliert **II**. □

Übung 8.16 Man überlege sich eine (optimale) Strategien für **I** im Spiel auf Ordnungen der Längen 3 gegenüber 4 bzw. 4 gegenüber 6. Ebenso gebe man Strategieanweisungen für **II** an, mit der sie 2 Runden im Spiel auf irgendwelchen Ordnungen von mindestens 3 Elementen übersteht. Wer gewinnt $G^3(\mathcal{O}_7; \mathcal{O}_8)$? Beschreiben Sie eine Gewinnstrategie.

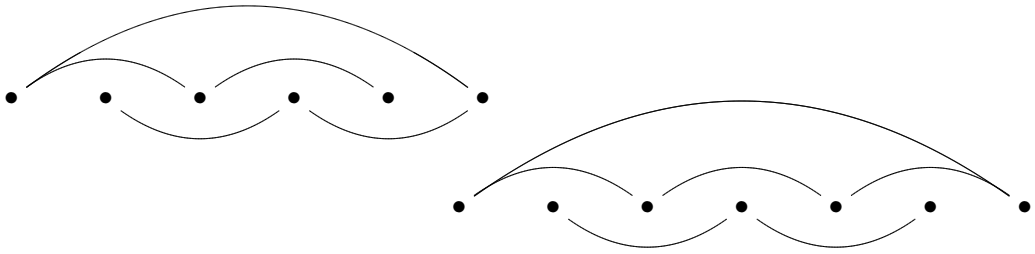
Korollar 8.17 *Zusammenhang ist als Eigenschaft endlicher Graphen nicht in* FO *ausdrückbar.*

Beweis Indirekt. Wir nehmen an, dass es einen FO($\{E\}$)-Satz φ gäbe, der in einem endlichen Graphen $\mathcal{G} = (V, E)$ genau dann wahr ist, wenn $\mathcal{G}$ zusammenhängend ist.

Über endlichen linearen Ordnungen $\mathcal{O}_n$ mit $n \geqslant 5$ Elementen sei E_n die zweistellige Relation, die gerade die Paare $(1, n), (n, 1)$ und sämtliche Paare (m, m') mit $|m - m'| = 2$ enthält. Der Graph mit Knotenmenge $\{1, \ldots, n\}$ und Kantenrelation E_n ist zusammenhängend wenn n gerade ist, unzusammenhängend wenn n ungerade ist. Es ist nicht schwer, eine Formel $\psi(x, y) \in$ FO($\{<\}$) anzugeben, die über den $\mathcal{O}_n$ genau die Relation E_n definiert (man benutzt als Hilfsformeln FO-Definitionen des ersten und des letzten Elements einer endlichen linearen Ordnung und der Relation "direkter $<$-Nachbar").

Wenn man nun in $\varphi \in \mathrm{FO}_0(\{E\})$ alle atomaren Bestandteile der Form Exy durch $\psi(x, y)$ ersetzt, so erhält man einen FO($\{<\}$)-Satz, der in endlichen linearen Ordnungen $\mathcal{O}_n$ genau dann wahr ist, wenn der Graph mit Kantenrelation E_n zusammenhängend ist, d.h., genau dann, wenn n gerade ist; im Widerspruch zum letzten Korollar. □

Die verwendeten Graphen für $n = 6$ und $n = 7$:



8.2 Ausblick: Andere Logiken – andere Spiele

Die hier angesprochenen Logiken, MSO und ML, wurden bereits in Abschnitt 7.3 als interessante Alternativen zu FO für bestimmte Zwecke angesprochen.

Monadische Logik zweiter Stufe über Wörtern

Die monadische Logik zweiter Stufe (MSO) hat gegenüber FO erheblich erweiterte Ausdrucksmöglichkeiten dadurch, dass zusätzlich über Variablen zweiter Stufe (Mengenvariablen) quantifiziert werden kann, deren Belegungen beliebige Teilmengen der Trägermenge sind. Wir benutzen Variablensymbole $X, Y, \ldots, X_1, X_2, \ldots$ für solche Mengenvariablen und schreiben $\exists X$ bzw. $\forall X$ für entsprechende Quantifizierungen. Als neue atomare Formeln treten Formeln wie Xy auf: für Belegungen $P \subseteq A$ für X und $a \in A$ für x in $\mathcal{A}$ ist Xy wahr wenn $a \in P$ ist.[3]

Beispiel 8.18 Der folgende MSO-Satz besagt für endliche lineare Ordnungen, dass die Anzahl der Elemente ungerade ist:

$$\varphi = \exists X\Big(\exists x\big(\psi_{\min}(x) \wedge Xx\big) \wedge \exists x\big(\psi_{\max}(x) \wedge Xx\big) \wedge \forall x \forall y\big(\psi_{\text{next}}(x,y) \to (Xx \leftrightarrow \neg Xy)\big)\Big),$$

wo $\psi_{\min}(x) \in \mathrm{FO}(\{<\})$ besagt dass x das minimale Element der Ordnung ist; entsprechend $\psi_{\max}(x)$ für das maximale Element; und $\psi_{\text{next}}(x,y)$, dass y direkter Nachfolger von x im Sinne von $<$ ist (d.h. $x < y$ und kein Element dazwischen). Dann ist $\mathcal{O}_n \models \varphi$ genau dann, wenn n ungerade.

Übung 8.19 Zu einem gegebenen NFA $\mathcal{A} = (\Sigma, Q, q_0, \Delta, A)$ soll ein MSO-Satz $\varphi_{\mathcal{A}}$ angegeben werden, derart dass für alle Σ-Wörter w mit zugehöriger Wortstruktur $\mathcal{W}$ gilt:

$$\mathcal{W} \models \varphi \quad \text{gdw.} \quad w \in L(\mathcal{A}).$$

Dazu verwende man Mengenvariablen X_q für $q \in Q$, die dazu dienen sollen ggf. eine Zustandsfolge in einer akzeptierenden Berechnung von $\mathcal{A}$ auf w über den Elementen von $\mathcal{W}$ zu kodieren. (Das vorige Beispiel kann im Wesentlichen als ein Spezialfall zur regulären Sprache der Σ-Wörter ungerader Länge aufgefasst werden.)

Man erhält aus der Übung die Teilaussage (a) des Satzes von Büchi, der die regulären Sprachen als genau die MSO-definierbaren Sprachen charakterisiert:

Satz 8.20 (Büchi)

(a) *Die Klasse der Wortstrukturen zu einer regulären Σ-Sprache ist* MSO*-definierbar.*

(b) *Für jeden* MSO*-Satz φ zur Signatur der Wortstrukturen über Σ ist die Σ-Sprache derjenigen Wörter w, deren Wortstruktur φ erfüllt, regulär.*

Die Aussage (b) des Satzes von Büchi, dass jede MSO-definierbare Eigenschaft von Wortstrukturen zu einer *regulären* Sprache korrespondiert, kann man auch so deuten, dass das *model checking* für MSO über Wortstrukturen mit endlichen Automaten implementiert werden kann.[4]

[3] Syntaktisch behandeln wir die Mengenvariablen genau wie einstellige Relationssymbole.

[4] Diese Aussage hat wesentliche Verallgemeinerungen auf das model checking über Bäumen, mit Konsequenzen wie etwa den Satz von Rabin zur Entscheidbarkeit von MSO über Bäumen. Aus diesem automatentheoretischen Ansatz ergeben sich weitere wichtige Anwendungen in der Informatik, die auch Gegenstand aktueller Forschung sind.

Eine elegante Methode zum Nachweis der Aussage (b) basiert auf der Analyse von Ehrenfeucht-Fraïssé Spielen für MSO. In diesen Spielen gibt es neben den Zügen, in denen Elemente markiert werden, auch Züge, in denen Teilmengen markiert (angefärbt) werden. Das q-Runden-Spiel für MSO zeigt dann das Analogon von Beobachtung 8.11 für Ununterscheidbarkeit bis Quantorenrang q in MSO, $\equiv_q^{\mathrm{MSO}}$.

Man erhält daraus, dass $\equiv_q^{\mathrm{MSO}}$ eine Kongruenzrelation von endlichem Index auf dem Wortmonoid von Σ^* bezüglich Konkatenation ist. Die (über die Wortstrukturen) von einem gegebenen MSO-Satz φ definierte Sprache ist offenbar abgeschlossen unter $\equiv_q^{\mathrm{MSO}}$ wenn $\mathrm{qr}(\varphi) \leqslant q$:

$$\mathcal{V} \equiv_q^{\mathrm{MSO}} \mathcal{W} \quad \text{und} \quad \mathcal{V} \models \varphi \qquad \text{impliziert} \qquad \mathcal{W} \models \varphi.$$

Also ist die zugehörige Sprache eine Vereining von Äquivalenzklassen einer Kongruenzrelation von endlichem Index über Σ^*. Eine Variante des Satzes von Myhill und Nerode liefert dann die Regularität dieser Sprache und damit den Beweis für (b) im Satz.

Modallogik und Bisimulation über Transitionssystemen

Die Modallogik (ML) lässt sich als Teillogik von FO über Strukturen vom Typ von Transitionssystemen auffassen. Dabei verstehen wir Transitionssysteme hier als Strukturen der Form $\mathcal{Q} = (Q, (E_a)_{a\in\Sigma}, P_1, \ldots, P_s)$. Die Trägermenge Q wird als Menge von Zuständen verstanden; die zweistelligen $E_a \subseteq Q \times Q$ deuten wir als Transitionsrelationen (für $a \in \Sigma$ bedeutet $(q, q') \in E_a$, dass es eine a-Transition von q nach q' gibt); und die einstelligen Relationen $P_i \subseteq Q$ beschreiben atomare Eigenschaften der Zustände. Als typische Signatur verwenden wir in diesem Abschnitt

$$S = \{E_a \colon a \in \Sigma\} \cup \{P_i \colon 1 \leqslant i \leqslant n\}.$$

Modallogische Formeln sollen Eigenschaften von Zuständen in S-Strukturen beschreiben, die neben den atomaren Zustandseigenschaften P_i Bezug nehmen auf mögliche Transitionen zu Nachfolgezuständen. Lokal in einem aktuellen Zustand q hat man so gerade AL_n: Aussagenlogik zu atomaren Aussagen p_i, deren Wahrheitswert in q gerade daran geknüpft ist, ob $q \in P_i$; d.h. die AL-Belegung hängt vom betrachteten Zustand ab. Dieses aussagenlogische Bild wird nun erweitert um Modalquantoren, die es erlauben, ebenso über benachbarte (über a-Transitionen zugängliche) andere Zustände und die dortige AL-Interpretation zu sprechen.

Definition 8.21 [Syntax und Semantik der Modallogik]
Die Menge $\mathrm{ML}(S)$ der modallogischen Formeln zur Signatur S wie oben wird induktiv erzeugt gemäß:

- (atomare Formeln) wie in AL_n: $\top, \bot$ und p_i für $1 \leqslant i \leqslant s$.
- (AL-Junktoren) wie in AL: $\neg$, $\wedge$, $\vee$.
- (Modalquantoren) zu $a \in \Sigma$ und $\varphi \in \mathrm{ML}(S)$ sind in $\mathrm{ML}(S)$:
  $\Diamond_a\varphi$ (existentielle Modalquantifizierung),
  $\Box_a\varphi$ (universelle Modalquantifizierung).

Die Semantik wird definiert indem wir induktiv über den Aufbau der Formeln definieren, wann φ in einem Zustand $q \in Q$ in einer S-Struktur $\mathcal{Q}$ erfüllt ist (φ wahr in $\mathcal{Q}, q$ bzw.

$\mathcal{Q}, q$ ein Modell von φ; in Symbolen: $\mathcal{Q}, q \models \varphi$).

- (atomare Formeln) $\top$ ist überall wahr, $\bot$ nirgends; $\mathcal{Q}, q \models p_i$ gdw. $q \in P_i^{\mathcal{Q}}$.
- (AL-Junktoren) wie in AL.
- (Modalquantoren):
  $\mathcal{Q}, q \models \Diamond_a \varphi$ gdw. es ein r gibt, sodass $(q, r) \in E_a^{\mathcal{Q}}$ und $\mathcal{Q}, r \models \varphi$;
  $\mathcal{Q}, q \models \Box_a \varphi$ gdw. für alle r mit $(q, r) \in E_a^{\mathcal{Q}}$ gilt $\mathcal{Q}, r \models \varphi$.

Übung 8.22 Geben Sie eine Übersetzung von ML(S) in FO(S) an, derart, dass jedem $\varphi \in \mathrm{ML}(S)$ Formeln $\hat{\varphi}(x)$ in einzelnen freien Variablen x zugeordnet werden mit

$$\mathcal{Q}, q \models \varphi \quad \text{gdw.} \quad \mathcal{Q} \models \hat{\varphi}[q].$$

Die linke Seite bezieht sich auf Syntax und Semantik von ML, die rechte auf Syntax und Semantik von FO. Man geht am besten induktiv vor. Der entscheidende Schritt betrifft die Modalquantoren. Idee: $(\Diamond_a \varphi)(x)$ soll besagen, dass es ein y gibt, das von x über eine E_a-Kante erreicht wird und wo $\hat{\varphi}(y)$ gilt.

Übung 8.23 Wir betrachten einen Spielgraph $\mathcal{G} = (V, E_a, E_b)$ mit 2-stelligen Transitionsrelationen E_a und E_b für Züge von Spieler a bzw. b. Ausgehend von einem Startknoten $q \in V$ ziehen die Spieler abwechselnd längs a- bzw. b-Transitionen, bis ggf. der Spieler, der am Zug ist nicht ziehen kann und verliert. Für den Start muss neben dem Startknoten q gestartet angegeben werden, welcher Spieler am Zug ist. Das n-Züge-Spiel mit Startknoten q und Spieler s am Zug sei mit $(\mathcal{G}, n, q, s)$ bezeichnet.

Geben Sie Formeln $\varphi^t_{n,s}, \varphi^t_{n,s} \in \mathrm{ML}(\{E_a, E_b\})$ an, die von einer Position q in $\mathcal{G}$ besagen, dass Spieler t eine Gewinnstrategie im Spiel $(\mathcal{G}, n, q, s)$ hat.

Hinweis: Man geht induktiv über n vor. Dazu macht man sich zunächst klar, was es bedeutet, dass z.B. Spieler a eine Gewinnstrategie in $(\mathcal{G}, n+1, q, a)$ bzw. in $(\mathcal{G}, n+1, q, b)$ hat, und wie sich das anhand von Gewinnstrategien in $(\mathcal{G}, n, q', a)$ und $(\mathcal{G}, n, q', b)$ für geeignete q' erfassen lässt. Die Bedeutung der Modalquantifizierung $\Diamond_a \ldots$ ist hier gerade "Spieler a kann einen Zug ausführen sodass ..."; entsprechend besagt $\Box_a \ldots$ dass "jeder mögliche Zug von Spieler a in eine Position führt, in der ..."; so besagt insbesondere $\Box_a \bot$, dass Spieler a nicht ziehen kann.

Der (modale) Quantorenrang von Formeln $\varphi \in \mathrm{ML}$ ist induktiv so definiert, dass er gerade die Schachtelungstiefe der Modalquantoren misst. Ununterscheidbarkeit bis zum Quantorenrang q in ML notieren wir mit $\equiv_q^{\mathrm{ML}}$:

$$\mathcal{Q}, q \equiv_n^{\mathrm{ML}} \mathcal{Q}', q' \quad \text{falls} \qquad \mathcal{Q}, q \models \varphi \quad \Leftrightarrow \quad \mathcal{Q}', q' \models \varphi \text{ für alle ML-Formeln } \varphi \text{ mit } \mathrm{qr}(\varphi) \leqslant n.$$

Das Ehrenfeucht-Fraïssé Spiel für ML Mit Modalquantoren bewegt man sich längs einer E_a-Kante in der Struktur, anstatt wie bei FO Quantifizierung ein zusätzliches Element irgendwo in der Struktur anzusehen. Dementsprechend werden die Spielkonfigurationen im ML-Spiel über zwei Transitionssystemen $\mathcal{Q}$ und $\mathcal{Q}'$ nun durch Angabe je eines markierten Elementes beschrieben. Die Spielzüge erlauben das voranrücken der Spielsteine längs E_a-Kanten (Rücken statt Setzen).

Spielkonfigurationen: $(\mathcal{Q}, q; \mathcal{Q}', q')$ bezeichnet die Konfiguration, in der Zustand q in $\mathcal{Q}$ und Zustand q' in $\mathcal{Q}'$ (durch Spielsteine) markiert sind.

Spielzüge: In jeder neuen Runde wählt **I** eine der beiden Strukturen, eine der Relationen E_a und bewegt den Spielstein in dieser Struktur längs einer E_a-Kante vorwärts; **II** muss den Spielstein in der anderen Struktur ebenfalls längst einer E_a-Kante (dasselbe a!) vorwärts bewegen.

Gewinnbedingung: **II** verliert falls sie einen Zug von **I** garnicht beantworten kann (weil keine E_a-Kante zur Verfügung steht) oder wenn die markierten Zustände in der aktuellen Konfiguration aussagenlogisch verschieden sind (d.h., wenn in $(\mathcal{Q}, q; \mathcal{Q}', q')$ für mindestens ein P_i die Bedingung $q \in P_i^{\mathcal{Q}} \Leftrightarrow q' \in P_i^{\mathcal{Q}'}$ verletzt ist).

Im *n-Runden-Spiel* $G^n(\mathcal{Q}, q; \mathcal{Q}', q')$, werden bis zu q Runden nach obigem Protokoll ausgehend von $(\mathcal{Q}, q; \mathcal{Q}', q')$ gespielt. Spieler **II** gewinnt eine solche Partie, falls sie durch alle n Runden hindurch antworten kann, ohne die Gewinnbedingung zu verletzen; **II** gewinnt auch wenn **I** am Zug wäre aber nicht ziehen kann.[5]

Satz 8.24 *Für alle $n \in \mathbb{N}$ und S-Strukturen $\mathcal{Q}$ und $\mathcal{Q}'$ mit ausgezeichneten Elementen $q \in \mathcal{Q}$ und $q' \in \mathcal{Q}'$ sind äquivalent:*

(i) **II** *hat eine Gewinnstrategie im Spiel $G^n(\mathcal{Q}, q; \mathcal{Q}', q')$.*

(ii) $\mathcal{Q}, q \equiv_n^{\mathrm{ML}} \mathcal{Q}', q'$.

Der Beweis verläuft in völliger Analogie zum Beweis des klassischen Ehrenfeucht-Fraïssé Satzes für FO – dabei ist das Spiel hier sogar einfacher.

Bisimulation Der Äquivalenzbegriff, der sich aus dem obigen ML-Spiel ergibt, ist auch unabhängig von der Analyse der Ausdrucksstärke von ML bereits in der Analyse von Prozessen (concurrency theory) untersucht worden. Man kann, ausgehend von unserem spielorientierten Standpunkt, den zugrundeliegenden Begriff der *Bisimulationsäquivalenz* wie folgt fassen. Die Idee ist hier eine wechselseitige Simulationsrelation zwischen Zuständen in Transitionssystemen (Bisimulation = Bi-Simulation). Es sei $G^\infty(\mathcal{Q}, q; \mathcal{Q}', q')$ das Spiel, das wie das ML-Spiel gespielt wird, aber ohne Beschränkung der Rundenzahl, sodass, wenn nicht einer der beiden Spieler (weil es keine zulässigen Züge gibt, oder weil die Gewinnbedingung verletzt ist) verliert, die Partie unendlich weitergeht. Wir sagen dass Spieler **II** eine Gewinnstrategie in $G^\infty(\mathcal{Q}, q; \mathcal{Q}', q')$ hat, wenn sie stets so spielen kann, dass sie nie in Zugnot gerät oder die Gewinnbedingung verletzt. Man nennt $\mathcal{Q}, q$ und $\mathcal{Q}', q'$ *bisimulationsäquivalent*, in Symbolen $\mathcal{Q}, q \sim \mathcal{Q}', q'$, wenn **II** in diesem Sinne eine Gewinnstrategie in $G^\infty(\mathcal{Q}, q; \mathcal{Q}', q')$ hat.

$$\mathcal{Q}, q \sim \mathcal{Q}', q' \quad \text{gdw.} \quad \textbf{II} \text{ hat Gewinnstrategie in } G^\infty(\mathcal{Q}, q; \mathcal{Q}', q').$$

Man kann relativ leicht zeigen, dass diese Definition äquivalent ist dazu dass es eine sogenannte *Bisimilationsrelation* Z zwischen $\mathcal{Q}$ und $\mathcal{Q}'$ gibt mit $(q, q') \in Z$. Dabei heisst $Z \subseteq Q \times Q'$ Bisimilationsrelation zwischen $\mathcal{Q}$ und $\mathcal{Q}'$ falls folgende Bedingungen erfüllt sind:

(i) für alle $(q, q') \in Z$ und P_i gilt: $q \in P_i^{\mathcal{Q}} \Leftrightarrow q' \in P_i^{\mathcal{Q}'}$.

(ii) (forth/Hin für $a \in \Sigma$): für alle $(q, q') \in Z$ und r sodass $(q, r) \in E_a^{\mathcal{Q}}$ gibt es auch ein r' sodass $(q', r') \in E_a^{\mathcal{Q}'}$ und $(r, r') \in Z$.

(iii) (back/Her für $a \in \Sigma$): für alle $(q, q') \in Z$ und r' sodass $(q', r') \in E_a^{\mathcal{Q}'}$ gibt es auch ein r sodass $(q, r) \in E_a^{\mathcal{Q}}$ und $(r, r') \in Z$.

[5] Das kann passieren, wenn vor Ablauf der n Runden eine Konfiguration erreicht wird, in der beide markierten Knoten garkeine Transitionen erlauben.

Man kann eine Bisimulationsrelation Z direkt als relationale Beschreibung einer Gewinnstrategie für **II** in Spielen $G^\infty(\mathcal{Q}, q; \mathcal{Q}', q')$ für $(q, q') \in Z$ auffassen.

Lemma 8.25 *Für $\mathcal{Q}, q \sim \mathcal{Q}', q'$ und $\varphi \in \mathrm{ML}$ gilt stets: $\mathcal{Q}, q \models \varphi$ gdw. $\mathcal{Q}', q' \models \varphi$.*

Beweis Man beweist die Behauptung induktiv über den Aufbau der Formeln $\varphi \in \mathrm{ML}$. Bedingung (i) für Bisimulationsrelationen (oder dass **II** nicht in der Startkonfiguration schon verloren hat) impliziert die Behauptung für atomare Formeln.

Die Induktionsschritte für AL Junktoren sind trivial.

Betrachtet man nun etwa $\varphi = \Diamond_a \psi$ und setzt die Behauptung für ψ voraus, so folgt die Behauptung für φ mit den Hin-/Her-Bedingungen (ii)/(iii) für Bisimulationsrelationen oder aus dem Verhalten für eine Runde im Spiel. Ist nämlich z.B. $\mathcal{Q}, q \models \Diamond_a \psi$, so gibt es ein r mit $(q, r) \in R_a^{\mathcal{Q}}$ und $\mathcal{Q}, r \models \psi$. Nach der Hin-Bedingung (ii) existiert aber dann in $\mathcal{Q}'$ entsprechend ein r' mit $(q', r') \in R_a^{\mathcal{Q}'}$ derart dass $\mathcal{Q}, r \sim \mathcal{Q}', r'$ und also (nach Induktionsvoraussetzung) $\mathcal{Q}', r' \models \psi$. Demnach also $\mathcal{Q}', q' \models \Diamond_a \psi$. Der $\Box_a$-Schritt ist analog. □

Ein direkter Zusammenhang mit Ununterscheidbarkeit in ML ergibt sich für Transitionssysteme, in denen jeder Zustand nur endlich viele direkte Nachfolgerzustände hat (*endlich verzweigte* Systeme).

Satz 8.26 (Hennessy-Milner) *Für endlich verzweigte Transitionssysteme $\mathcal{Q}$ und $\mathcal{Q}'$ zur endlichen Signatur S sind äquivalent:*

(i) $\mathcal{Q}, q \sim \mathcal{Q}', q'$.

(ii) $\mathcal{Q}, q \equiv^{\mathrm{ML}} \mathcal{Q}', q'$,
d.h., für alle Formeln $\varphi \in \mathrm{ML}(S)$ gilt: $\mathcal{Q}, q \models \varphi$ gdw. $\mathcal{Q}', q' \models \varphi$.

Beweis (i) $\Rightarrow$ (ii) folgt aus Lemma 8.25. Für (ii) $\Rightarrow$ (i) kann man die Beweisidee zur entsprechenden Richtung im Beweis von Satz 8.7 benutzen. Hier ist nun zu zeigen: In einer Konfiguration $(\mathcal{Q}, q; \mathcal{Q}', q')$ mit $\mathcal{Q}, q \sim \mathcal{Q}', q'$ hat **II** zu jedem Zug von **I** in der ersten Runde von $G^\infty(\mathcal{Q}, q; \mathcal{Q}', q')$ eine Antwort, die zu einer Konfiguration $(\mathcal{Q}, r; \mathcal{Q}', r')$ führt in der wieder $\mathcal{Q}, r \sim \mathcal{Q}', r'$ ist. □

Bemerkung Ein zentraler Satz von van Benthem besagt, dass in ML genau diejenigen FO-Eigenschaften ausdrückbar sind, die im Sinne von Lemma 8.25 unter Bisimulationsäquivalenz erhalten sind.

Index