Mathematische Logik
SS 2011

Prof. Dr. Erich Grädel

Mathematische Grundlagen der Informatik
RWTH Aachen

Inhaltsverzeichnis

2 Syntax und Semantik der Prädikatenlogik

Die Aussagenlogik behandelt ausschließlich Aussagen, welche aus atomaren Formeln mit Hilfe der aussagenlogischen Verknüpfungen $\wedge, \vee, \neg$ etc. zusammengesetzt werden. Eine aussagenlogische Interpretation ordnet den atomaren Formeln Wahrheitswerte 0 oder 1 zu, und dies setzt sich fort zu einer Interpretation beliebiger aussagenlogischer Formeln. Insbesondere haben die atomaren Aussagen selbst keine innere Struktur, ja wir abstrahieren vollständig vom mathematischen, umgangssprachlichen oder technischen Inhalt einer atomaren Aussage, nur ihr Wahrheitswert ist maßgebend.

Für die meisten mathematischen Anwendungen ist die Aussagenlogik viel zu ausdrucksschwach. Bereits sehr einfache, alltägliche Argumente über konkrete Strukturen, z.B. „alle Quadratzahlen sind positiv, $25 = 5 \cdot 5$, also ist 25 positiv“ widersetzen sich einer Formalisierung in der Aussagenlogik. Formal hat das Argument die Gestalt $\psi \wedge \varphi \to \vartheta$, aber ohne Zugriff auf die Struktur und den Zusammenhang der Teilaussagen ψ, φ, ϑ gibt es keinen Grund, warum eine solche Implikation wahr sein sollte.

Wir brauchen also ein ausdrucksstärkeres logisches System. Die Prädikatenlogik (abgekürzt FO für „first-order logic“) macht Aussagen, welche durch Strukturen und Elemente von Strukturen (also nicht durch bloße Wahrheitswerte) interpretiert werden. Bereits die atomaren Formeln haben eine kompliziertere Struktur, sie sprechen über Relationen zwischen Elementen einer Struktur (z.B. $2x < y + 3$) oder über die Gleichheit von Elementen (z.B. $x^2 = y$). Außerdem werden Aussagen nicht nur mit Hilfe der aussagenlogischen Junktoren miteinander verknüpft, es besteht auch die Möglichkeit, Existenz- oder Allaussagen über Elemente einer Struktur zu machen, der Art „es gibt eine reelle

Zahl x, so dass $x^2 = 2$" oder „zu jeder Primzahl gibt es eine größere". Was wir hingegen nicht zulassen, sind Existenz- oder Allaussagen über Mengen, Funktionen oder Relationen auf der zugrundegelegten Struktur.

2.1 Strukturen

Mathematische Strukturen bestehen aus einem Universum und aus ausgezeichneten Funktionen und Relationen auf diesem Universum. Beispiele sind:

- die additive Gruppe der ganzen Zahlen: $(\mathbb{Z}, +, 0)$
- der geordnete Körper der reellen Zahlen: $(\mathbb{R}, +, \cdot, 0, 1, <)$
- Graphen: Die Punkte des Graphen sind das Universum, die zweistellige Relation E beschreibt die Kantenbeziehung.

Die Namen (Symbole) für die in einer Struktur auftretenden Relationen und Funktionen bilden die Signatur der Struktur.

Definition 2.1. Eine *Signatur* τ ist eine Menge von Funktions- und Relationssymbolen. Jedes dieser Symbole hat eine feste endliche Stelligkeit.

Eine Signatur heißt *relational*, wenn sie nur Relationssymbole enthält bzw. *funktional* oder *algebraisch*, wenn sie ausschließlich Funktionssymbole enthält. Nullstellige Funktionssymbole heißen auch *Konstantensymbole*.

Andere Bezeichnungen für eine Signatur sind *Symbolmenge* oder *Vokabular*.

Beispiel.

- Die Signatur der Arithmetik ist $\tau_{ar} = \{+, \cdot, 0, 1\}$, wobei $+$ und $\cdot$ zweistellige Funktionsymbole, 0 und 1 Konstantensymbole sind.
- Die Signatur der geordneten Arithmetik ist $\tau_{ar}^{<} = \{+, \cdot, 0, 1, <\}$. Sie erweitert τ_{ar} um das zweistellige Relationssymbol $<$.
- Die Signatur von Graphen $\tau_G = \{E\}$, wobei E ein zweistelliges Relationssymbol ist.

Notation. Normalerweise verwenden wir

- $P, Q, R, \ldots, P_i, \ldots$ für Relationssymbole,
- $f, g, h, \ldots, f_i, \ldots$ für Funktionssymbole,
- $c, d, e, \ldots, c_i, \ldots$ für Konstantensymbole,
- σ, τ für Signaturen.

Relations- und Funktionssymbole in einer Signatur τ können natürlich in vielfältiger Weise durch konkrete Relationen und Funktionen interpretiert werden. Allgemein wird eine Struktur festgelegt durch Angabe ihres Universums und der Interpretation der Relations- und Funktionssymbole über diesem Universum.

Definition 2.2. Eine *τ-Struktur* $\mathfrak{A}$ besteht aus

- einer nichtleeren Menge A, dem *Universum* (oder *Träger*) von $\mathfrak{A}$,
- einer Interpretationsfunktion welche jedem n-stelligen Relationssymbol $P \in \tau$ eine n-stellige Relation $P^{\mathfrak{A}} \subseteq A^n$ und jedem n-stelligen Funktionssymbol $f \in \tau$ eine n-stellige Funktion $f^{\mathfrak{A}} : A^n \to A$ zuordnet.

Eine Struktur mit funktionaler Signatur τ heißt auch eine *τ-Algebra*.

Notation. Strukturen bezeichnen wir meist mit gotischen Buchstaben $\mathfrak{A}, \mathfrak{B}\, \mathfrak{C}, \ldots$, der entsprechende lateinische Buchstabe $A, B, C, \ldots$ steht für das Universum der Struktur. Mit $\mathfrak{A} = (A, P_1^{\mathfrak{A}}, P_2^{\mathfrak{A}}, \ldots, f_1^{\mathfrak{A}}, f_2^{\mathfrak{A}}, \ldots)$ bezeichnen wir also eine Struktur der Signatur $\tau = \{P_1, P_2, \ldots, f_1, f_2 \ldots\}$ mit Universum A.

Bemerkung. Es ist wichtig zwischen Relations- und Funktions*symbolen* R_i, f_j und ihrer Interpretation durch konkrete Relationen $R_i^{\mathfrak{A}}$ bzw. Funktionen $f_j^{\mathfrak{A}}$ zu unterscheiden.

Wir werden eine Reihe von Beispielen im nächsten Abschnitt diskutieren. Zuvor beschreiben wir zwei grundlegende Möglichkeiten, wie eine Struktur in einer andern enthalten sein kann.

Definition 2.3. Seien $\mathfrak{A}$ und $\mathfrak{B}$ τ-Strukturen. $\mathfrak{A}$ ist *Substruktur* von $\mathfrak{B}$ (kurz: $\mathfrak{A} \subseteq \mathfrak{B}$), wenn

- $A \subseteq B$,

- für alle Relationssymbole $R \in \tau$ gilt: $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$ (wobei n die Stelligkeit von R ist),
- für alle Funktionssymbole $f \in \tau$ gilt $f^{\mathfrak{A}} = f^{\mathfrak{B}}|_A$, d.h. $f^{\mathfrak{A}}$ ist die *Restriktion* von $f^{\mathfrak{B}}$ auf A.

Wenn $\mathfrak{A}$ Substruktur von $\mathfrak{B}$, so heißt $\mathfrak{B}$ *Erweiterung* von $\mathfrak{A}$.

Ist $\mathfrak{A}$ eine Substruktur der τ-Struktur $\mathfrak{B}$, so ist A *τ-abgeschlossen*, d.h. für alle n-stelligen $f \in \tau$ und alle $a_1, \ldots, a_n \in A$ ist $f^{\mathfrak{B}}(a_1, \ldots, a_n) \in A$. Umgekehrt gilt auch: Sei $\mathfrak{B}$ eine τ-Struktur. Zu jeder nicht-leeren, τ-abgeschlossenen Teilmenge $A \subseteq B$ gibt es genau eine Substruktur von $\mathfrak{B}$ mit Träger A. Wir nennen sie die *von A in $\mathfrak{B}$ induzierte Substruktur*.

Beispiel. $2\mathbb{N} := \{2n : n \in \mathbb{N}\}$ ist $\{+\}$-abgeschlossen. Also ist $(2\mathbb{N}, +) \subseteq (\mathbb{N}, +)$. Hingegen ist $2\mathbb{N} + 1 := \{2n + 1 : n \in \mathbb{N}\}$ nicht $\{+\}$-abgeschlossen und kann somit nicht Träger einer Substruktur von $(\mathbb{N}, +)$ sein.

Während beim Begriffspaar Substruktur/Erweiterung die Signatur fest bleibt und das Universum verändert wird, ist dies beim Begriffspaar Redukt/Expansion genau umgekehrt.

Definition 2.4. Seien $\sigma \subseteq \tau$ Signaturen, und sei $\mathfrak{B}$ eine τ-Struktur. Das *σ-Redukt* $\mathfrak{B} \restriction \sigma$ von $\mathfrak{B}$ ist die σ-Struktur, die wir aus $\mathfrak{B}$ erhalten, wenn wir die Relationen und Funktionen in $\tau \setminus \sigma$ einfach weglassen. Ist $\mathfrak{A}$ Redukt einer τ-Struktur $\mathfrak{B}$, so nennen wir $\mathfrak{B}$ eine *τ-Expansion* von $\mathfrak{A}$.

Beispiel. Die additive Gruppe der reellen Zahlen $(\mathbb{R}, +, 0)$ ist das $\{+, 0\}$-Redukt des Körpers der reellen Zahlen $(\mathbb{R}, +, \cdot, 0, 1)$.

2.2 Ein Zoo von Strukturen

Mengen. Sei $\tau = \emptyset$. Die $\emptyset$-Struktur mit Universum A ist einfach die Menge A.

Graphen. Die Signatur von Graphen ist $\tau_G = \{E\}$, wobei E ein binäres Relationssymbol ist. Eine beliebige τ_G-Struktur ist ein *gerichteter Graph*. Ein *ungerichteter Graph* ist eine τ_G-Struktur $G = (V, E^G)$ mit Punktmenge V (dem Universum von G) und einer Relation $E^G \subseteq V \times V$, welche folgende Bedingungen erfüllt:

(Keine Schlingen) Für alle $v \in V$ gilt: $(v, v) \notin E^G$.

(Symmetrie) Für alle $u, v \in V$: Wenn $(u, v) \in E^G$, dann auch $(v, u) \in E^G$.

LINEARE UND PARTIELLE ORDNUNGEN. Eine partielle Ordnung ist eine $\{<\}$-Struktur $(A, <)$ welche folgende Bedingungen erfüllt:

(Irreflexivität) Für kein $a \in A$ gilt $a < a$.

(Transitivität) Wenn $a < b$ und $b < c$, dann auch $a < c$.

Daraus folgt insbesondere auch, dass $<$ *antisymmetrisch* ist: Wenn $a < b$, dann *nicht* $b < a$.

Eine *lineare* oder *totale* Ordnung erfüllt als zusätzliche Bedingung:

(Vergleichbarkeit) Für alle a, b gilt $a < b$, $a = b$ oder $b < a$.

Offensichtlich sind $(\mathbb{N}, <)$ und $(\mathbb{R}, <)$ (mit der üblichen Interpretation von $<$) lineare Ordnungen. Für jede Menge A ist $(\mathcal{P}(A), \subset)$ eine partielle Ordnung, für $|A| > 1$ aber keine lineare Ordnung.

Eine lineare Ordnung ist *dicht*, wenn zu zwei beliebigen Elementen $a < b$ immer ein c existiert mit $a < c < b$.

Eine *Wohlordnung* ist eine lineare Ordnung $(A, <)$ ohne unendliche absteigende Ketten: Es gibt keine unendliche Folge $a_0, a_1, a_2, \ldots$ in A so dass $a_{i+1} < a_i$ für alle $i \in \mathbb{N}$. Zum Beispiel ist $(\mathbb{N}, <)$ eine Wohlordnung während $(\mathbb{Z}, <)$ oder $(\mathbb{Q}^+, <)$ keine Wohlordnungen sind.

WORTSTRUKTUREN. Sei Γ ein *Alphabet*, d.h. eine beliebige, in der Regel abzählbare, Menge von Symbolen. Ein *Wort* über Γ ist eine endliche Folge $w = w_0 \cdots w_{n-1}$ von Symbolen aus Γ. Jedem solchen Wort w ordnen wir eine Struktur $\mathfrak{B}(w)$ der Signatur $\{<\} \cup \{P_a : a \in \Gamma\}$ mit einstelligen Relationssymbolen P_a zu. Das Universum von $\mathfrak{B}(w)$ ist die Menge $\{0, \ldots, n-1\}$ der Positionen an denen Symbole stehen, $<$ ist die übliche Ordnung auf dieser Menge und $P_a := \{i < n : w_i = a\}$ ist die Menge der Positionen an denen im Wort w das Symbol a steht. Das Wort $w = abbcab$ über dem Alphabet $\{a, b, c\}$ wird also durch die Wortstruktur

$$\mathfrak{B}(w) = (\{0, 1, 2, 3, 4, 5\}, <, P_a, P_b, P_c)$$

mit $P_a = \{0, 4\}$, $P_b = \{1, 2, 5\}$ und $P_c = \{3\}$ repräsentiert.

In der Logik wird die Menge der natürlichen Zahlen oft mit ω bezeichnet. Ein *unendliches Wort* oder *ω-Wort* ist eine unendliche Folge $z = z_0 z_1 \cdots \in \Gamma^\omega$ von Symbolen aus Γ. Die entsprechende Wortstruktur ist $\mathfrak{B}(z) := (\omega, <, (P_a)_{a \in \Gamma})$ mit $P_a = \{i \in \omega : z_i = a\}$.

Transitionssysteme. Ein Transitionssystem besteht aus einer Menge S von *Zuständen* und aus einer Menge A von *Aktionen* oder *Programmen*, welche Zustände in neue Zustände überführen. Zusätzlich hat man in der Regel eine Menge B von Eigenschaften, welche die Zustände haben oder nicht haben können. Ein solches Transitionssystem wird beschrieben durch eine Struktur mit Universum S, einer Menge $\{P_b : b \in B\}$ von monadischen (d.h. einstelligen) Relationen und einer Menge $\{E_a : a \in A\}$ von binären Relationen auf S. Dabei soll P_b die Menge der Zustände mit der Eigenschaft b sein, und die Relation E_a soll auf ein Paar (s, t) von Zuständen zutreffen, genau dann, wenn das Programm a den Zustand s in den Zustand t überführt.

Eine wichtige Methode zur Verifikation paralleler Systeme besteht darin, diese als Transitionssysteme zu modellieren und Bedingungen wie Fairness, Sicherheit, Deadlock-Freiheit etc. in einer geeigneten logischen Sprache zu formulieren und auf dem Transitionssystem auszuwerten. Formale Spezifikation und Verifikation solcher Systeme ist eine der wichtigsten Anwendungen der Logik in der Informatik.

Relationale Datenbanken. Eine relationale Datenbank ist, informell gesprochen, eine endliche Kollektion von endlichen Tabellen, welche sich zeitlich verändern. Jede Zeile in einer solchen Tabelle R ist ein Tupel $(a_1, \ldots, a_n) \in D_1 \times \cdots \times D_n$ wobei $D_1, \ldots, D_n$ die den einzelnen Spalten (im Datenbank-Jargon: den Attributen) zugeordneten *Domänen* sind (z.B. Integers, Strings,...). Sei D die Vereinigung aller in der Datenbank vorkommenden Domänen. Die Tabelle R kann dann als eine n-stellige Relation über D aufgefasst werden: $R \subseteq D^n$.

Ein aktueller Zustand der Datenbank ist also eine endliche Kollektion von endlichen Relationen $R_1, \ldots, R_m$ über dem (in der Regel unendlichen) Universum D. Dies entspricht der Struktur $\mathfrak{D} = (D, R_1, \ldots, R_m)$.

Für viele Zwecke ist aber diese Formalisierung problematisch: Elementare Operationen wie die Bildung des Komplements einer Relation führen zu unendlichen Relationen. Daher ist eine Formalisierung durch eine *endliche* Struktur oft zweckmäßiger. Anstelle des unendlichen Universums D betrachte man die *aktive Domäne* $\mathrm{ad}(\mathfrak{D})$, welche aus all denjenigen Objekten besteht, die in einer der Relationen $R_1, \ldots, R_m$ vorkommen, also

$$\mathrm{ad}(\mathfrak{D}) := \{a \in D : \text{ es gibt ein } R_i \text{ und ein } (b_1, \ldots, b_r) \in R_i, \\ \text{so dass } b_j = a \text{ für ein } j \leq r\}.$$

Da alle Relationen R_i endlich sind, ist auch $\mathrm{ad}(\mathfrak{D})$ endlich und die endliche Substruktur $(\mathrm{ad}(\mathfrak{D}), R_1, \ldots, R_m)$ von $\mathfrak{D}$ ist eine adäquate endliche Formalisierung des Datenbank-Zustandes.

Anfragen an eine Datenbank entsprechen dem Auswerten logischer Formeln auf (endlichen) Strukturen. Es bestehen daher enge Verbindungen zwischen der Mathematischen Logik und der Theorie relationaler Datenbanken.

Arithmetische Strukturen. Die Signatur der Arithmetik ist $\tau_{\mathrm{ar}} = \{+, \cdot, 0, 1\}$, die Signatur der geordneten Arithmetik $\tau_{\mathrm{ar}}^{<} = \tau_{\mathrm{ar}} \cup \{<\}$, wobei wir annehmen, dass die Symbole $+, \cdot, 0, 1, <$ in der üblichen Weise interpretiert werden. Trotzdem gibt es natürlich ganz verschiedene arithmetische Strukturen, z.B.:

- $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1)$, die *Standard-Arithmetik* der natürlichen Zahlen. Die *geordnete Standard-Arithmetik* ist $\mathfrak{N}^{<} = (\mathbb{N}, +, \cdot, 0, 1, <)$. Sie ist eine Expansion von $\mathfrak{N}$.
- Beliebige *Ringe*, insbesondere der Ring $\mathfrak{Z} = (\mathbb{Z}, +, \cdot, 0, 1)$ der ganzen Zahlen. Offensichtlich ist $\mathfrak{Z}$ eine Erweiterung der Standard-Arithmetik $\mathfrak{N}$.
- Beliebige *Körper*, etwa den Körper $\mathfrak{R} = (\mathbb{R}, +, \cdot, 0, 1)$ der reellen Zahlen, den Körper $\mathfrak{Q} = (\mathbb{Q}, +, \cdot, 0, 1)$ der rationalen Zahlen oder endliche Körper.
- Die Standard-Arithmetik $\mathfrak{N}$ lässt sich durch Hinzunahme von 'unendlichen Elementen' zu neuen arithmetischen Strukturen erwei-

tern. Die einfachste Variante ist $(\mathbb{N} \cup \{\infty\}, +, \cdot, 0, 1)$ mit

$$a + \infty = \infty + a = a \cdot \infty = \infty \cdot a = \infty$$

für alle $a \in \mathbb{N} \cup \{\infty\}$.

Boolesche Algebren. Sei A eine beliebige Menge. Die Boolesche Algebra über A ist $\mathrm{BA}(A) = (\mathcal{P}(A), \cup, \cap, ^-, \emptyset, A)$, wobei $\cup, \cap, ^-$ Vereinigung, Durchschnitt und Komplement in A bedeuten.

Gruppen. Wie können Gruppen (im Sinne der Algebra) durch Strukturen gemäß Definition 2.2 formalisiert werden? Dafür gibt es mehrere Möglichkeiten, abhängig davon, welche in Gruppen vorkommenden Funktionen und Relationen explizit (d.h. in der Signatur) vorkommen sollen. Mit den üblichen Bezeichnungen $\circ$ für die Gruppenoperation, e für das neutrale Element, g^{-1} für das zu g inverse Element ergeben sich sofort die Möglichkeiten

(1) $\mathfrak{G} = (G, \circ)$,
(2) $\mathfrak{G} = (G, \circ, e)$ und
(3) $\mathfrak{G} = (G, \circ, e, {}^{-1})$.

Die Wahl der Signatur ist abhängig von der jeweiligen Absicht: Will man eine möglichst minimale Formalisierung, wird man (1) oder (2) wählen, da die Gruppe dadurch bereits eindeutig festgelegt ist. Andererseits gibt es algebraische Überlegungen, welche die dritte Möglichkeit nahelegen: Wenn die Funktion $^{-1}$ hinzugenommen wird, sind die Substrukturen von $\mathfrak{G}$ genau die Untergruppen. Dies ist nicht der Fall bei den beiden ersten Formalisierungen. So ist etwa $(\mathbb{N}, +, 0)$ eine Substruktur von $(\mathbb{Z}, +, 0)$ (der additiven Gruppe der ganzen Zahlen), aber offensichtlich keine Untergruppe.

In der Praxis sind oft noch ganz andere Operationen wesentlich, etwa die Multiplikation mit erzeugenden Elementen der Gruppe.

Vektorräume. Zum Abschluss diskutieren wir das Problem der Formalisierung von Vektorräumen. Interessant ist dies deshalb, weil hier Objekte verschiedener Art auftreten: Vektoren und Skalare.

Sei etwa V ein Vektorraum über dem Körper K. Man kann eine Formalisierung wählen, in der das Universum ausschließlich aus den Vektoren besteht, und die Elemente des Grundkörpers als Operationen auf dem Universum in Erscheinung treten. Dem Vektorraum entspricht dann die algebraische Struktur $(V, +, 0, (f_k)_{k\in K})$ mit $f_k(v) := kv$ (Multiplikation mit Skalar k). Für algebraische Überlegungen ist dies bei festem Grundkörper K die geeignete Formalisierung, da die Substrukturen genau den linearen Unterräumen entsprechen (Abgeschlossenheit unter Addition und unter Multiplikation mit Skalaren). Wenn wir im folgenden über Vektorräume sprechen, ist meistens diese Formalisierung gemeint.

2.3 Syntax der Prädikatenlogik

Wir fixieren eine Signatur τ und definieren die Menge der τ-Terme und die Menge der τ-Formeln induktiv als Wortmengen über einem Alphabet $\mathrm{Alph}(\tau)$, welches aus folgenden Symbolen besteht:

- den Relations- und Funktionssymbolen in τ,
- einer festen abzählbar unendlichen Menge $\mathrm{VAR} = \{v_0, v_1, v_2, \ldots\}$ von *Variablen*,
- dem *Gleichheitszeichen* $=$,
- den *aussagenlogischen Junktoren* $\neg, \wedge, \vee$ und $\rightarrow$,
- dem *Existenzquantor* $\exists$ und dem *Allquantor* $\forall$,
- den Klammersymbolen $(,)$.

τ-Terme sind bestimmte Wörter über diesem Alphabet, welche aus Variablen und Funktionszeichen zusammengesetzt sind. Wir verwenden hier eine klammerfreie Notation.

Definition 2.5. Die Menge $\mathrm{T}(\tau)$ der *τ-Terme* ist induktiv wie folgt definiert:

- $\mathrm{VAR} \subseteq \mathrm{T}(\tau)$, d.h. jede Variable ist ein τ-Term.
- Sind $t_1, \ldots, t_n$ τ-Terme und f ein n-stelliges Funktionssymbol aus τ, so ist auch $ft_1 \cdots t_n$ ein τ-Term.

Wenn wir einen Term in der Form $t(x_1, \ldots, x_n)$ schreiben, dann meinen wir, dass $x_1, \ldots, x_n$ paarweise verschiedene Variablen sind und dass in t keine anderen Variablen als diese vorkommen.

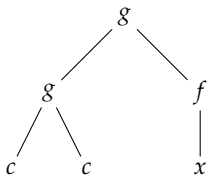
Man beachte, dass insbesondere jedes Konstantensymbol c aus τ ein τ-Term ist. Ein *Grundterm* ist ein Term in dem keine Variablen auftreten.

Beispiel. Die Signatur τ enthalte die Funktionssymbole f (einstellig), g (zweistellig) und c (nullstellig). Sei $x \in \mathrm{VAR}$ eine Variable. Dann sind die folgenden Wörter τ-Terme.

$$x, \quad c, \quad fx, \quad fc, \quad gxx, \quad gfxc, \quad ggccfx.$$

Dabei sind c und fc Grundterme.

Es ist oft nützlich, Terme als Bäume aufzufassen. Die Baumnotation des Terms $ggccfx$ ist:



Eindeutige Lesbarkeit von Termen. Jedes Wort in $\mathrm{Alph}(\tau)^*$ kann auf höchstens eine Weise als ein Term aufgefasst werden. Um dies nachzuweisen, zeigt man zunächst per Induktion über den Termaufbau, dass kein τ-Term ein echtes Anfangsstück eines andern τ-Terms sein kann. Daraus folgt, dass für jeden Term $ft_1 \cdots t_n$ die unmittelbaren Unterterme $t_1, \ldots, t_n$ eindeutig bestimmt sind.

Definition 2.6. Die Menge $\mathrm{FO}(\tau)$ der *τ-Formeln* der Prädikatenlogik ist induktiv definiert wie folgt:

(1) Sind t_1, t_2 τ-Terme dann ist $t_1 = t_2$ eine τ-Formel.
(2) Sind $t_1, \ldots, t_n$ τ-Terme und ist $P \in \tau$ ein n-stelliges Relationssymbol, dann ist $Pt_1 \cdots t_n$ eine τ-Formel.
(3) Wenn ψ eine τ-Formel ist, dann auch $\neg\psi$.

(4) Wenn ψ und φ τ-Formeln sind, dann auch $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$ und $(\psi \to \varphi)$.
(5) Wenn ψ eine τ-Formel ist und $x \in \mathrm{VAR}$ eine Variable, dann sind $\exists x\psi$ und $\forall x\psi$ τ-Formeln.

Eine Formel, die nur nach den Regeln (1) und (2) definiert ist, heißt *atomar*, *Atom-Formel* oder einfach *Atom*. *Literale* sind Atome und deren Negationen. Formeln, die nur nach den Regeln (1) – (4) definiert sind, heißen *quantorenfrei*.

Beispiel. Sei $\tau = \{E, f\}$, wobei E ein zweistelliges Relationssymbol und f ein einstelliges Funktionssymbol sind. Hier sind einige Formeln aus $\mathrm{FO}(\{E, f\})$:

- $v_0 = v_1$,
- $((Ev_0v_0 \vee fv_0 = v_1) \wedge \neg Ev_1fv_0)$,
- $\forall v_0 \forall v_1(\neg v_0 = v_1 \to Ev_0v_1)$,
- $\forall v_0 \forall v_1(Ev_0v_1 \to \exists v_2(Ev_0v_2 \wedge Ev_2v_0))$.

Konventionen zur Notation von Formeln. Wie bei der Aussagenlogik benutzen wir auch bei der Prädikatenlogik abkürzende oder vereinfachende Schreibweisen. Zum Beispiel bezeichnen wir Variablen in der Regel mit anderen Symbolen, etwa $x, y, z, x_0, x_1, \ldots$, anstelle von $v_0, v_1, \ldots \in \mathrm{VAR}$. Für Terme, die aus Funktionssymbolen wie $+$, $\cdot$, $\circ$ etc. gebildet werden, verwenden wir in der Regel die Infix-Notation $x + y$ statt $+xy$; ähnliches gilt für Atome wie etwa $t_1 < t_2$ oder gelegentlich auch xEy. Anstelle von $\neg t_1 = t_2$ schreiben wir $t_1 \neq t_2$. Wo dies für die Lesbarkeit nützlich ist, werden wir von der klammerfreien Notation von Termen abweichen: Zum Beispiel schreiben wir $x + (y + z) = (x + y) + z$ anstelle von $+x + yz = ++xyz$. Andererseits werden wir in Formeln oft Klammern weglassen, welche für das Verständnis überflüssig sind.

Man beachte, dass diese anschaulichen Mitteilungsweisen keine Terme und Formeln im eigentlichen Sinn mehr sind sondern metasprachliche Umschreibungen solcher Objekte. Die präzise formale Definition der syntaktischen Objekte ist notwendig für die Präzisierung des Begriffs einer logischen Aussage, für die Analyse des Beweisbegriffs und insbesondere für die maschinelle Verarbeitung mathematischer

Aussagen. Für die metasprachliche Kommunikation ist eine allzu formale Notation hingegen eher hinderlich als hilfreich. Dies gilt nicht nur für logische Formeln; auch in der Kommunikation über andere syntaktische Objekte, etwa Computer-Programme (für die eine präzise Syntax natürlich zwingend erforderlich ist), wird man, etwa bei der Konzeption und Analyse informellere Beschreibungen vorziehen.

Wir weisen außerdem darauf hin, dass ein Ausdruck $t_1 = t_2$ je nach Kontext entweder eine Formel aus $\mathrm{FO}(\tau)$ oder aber eine metasprachliche Aussage sein kann, welche die Gleichheit der beiden Terme t_1, t_2 als syntaktische Objekte ausdrückt. Um diese mögliche Quelle von Konfusionen zu vermeiden, kann man entweder zwei verschiedene Gleichheitszeichen einführen oder einfach versuchen, sorgfältig zu sein. Wir wählen hier die zweite Möglichkeit.

Freie und gebundene Variablen. Ein *Vorkommen* einer Variablen x in einer Formel ψ kann *frei* oder *gebunden* sein. Es ist gebunden, wenn es in einer Unterformel der Form $\exists x\psi$ oder $\forall x\psi$ stattfindet, andernfalls ist es frei.

Beispiel. In der folgenden Formel sind unterstrichene Vorkommen von Variablen gebunden, nicht unterstrichene Vorkommen sind frei.

$$\exists \underline{x}(Eyz \wedge \forall \underline{z}(\underline{z} = \underline{x} \vee E y \underline{z})).$$

Man beachte, dass z in dieser Formel sowohl frei als auch gebunden vorkommt.

Formal ist die Menge der in einer Formel frei auftretenden Variablen wie folgt definiert.

Definition 2.7. Sei $t \in \mathrm{T}(\tau)$ ein Term und $\psi \in \mathrm{FO}(\tau)$ eine Formel. Mit $\mathrm{var}(t)$ bzw. $\mathrm{var}(\psi)$ bezeichnen wir die Menge aller in t bzw. ψ auftretenden Variablen. Die Menge $\mathrm{frei}(\psi)$ der freien Variablen von ψ ist induktiv wie folgt definiert:

- Für atomare Formeln ψ ist $\mathrm{frei}(\psi) := \mathrm{var}(\psi)$.
- $\mathrm{frei}(\neg\psi) := \mathrm{frei}(\psi)$.
- $\mathrm{frei}(\psi \circ \varphi) := \mathrm{frei}(\psi) \cup \mathrm{frei}(\varphi)$ für $\circ \in \{\wedge, \vee, \rightarrow\}$.

- $\text{frei}(\exists x\psi) = \text{frei}(\forall x\psi) := \text{frei}(\psi) \setminus \{x\}$.

Oft bezeichnen wir eine Formel in der Form $\psi(x_1, \ldots, x_k)$, um anzudeuten, dass höchstens die Variablen $x_1, \ldots, x_k$ in ψ frei vorkommen. Ein τ-*Satz* ist eine τ-Formel ohne freie Variablen.

Mächtigkeit von $\mathrm{T}(\tau)$ *und* $\mathrm{FO}(\tau)$. Wenn τ abzählbar ist, dann auch das Alphabet $\text{Alph}(\tau)$. Es folgt dann, dass auch $\text{Alph}(\tau)^*$, und damit insbesondere $\mathrm{T}(\tau)$ und $\mathrm{FO}(\tau)$ abzählbar sind. Andererseits sind $\mathrm{T}(\tau)$ und $\mathrm{FO}(\tau)$ auch bei endlicher Signatur τ (sogar bei $\tau = \emptyset$) unendlich. In der Tat enthält $\mathrm{T}(\tau)$ alle Variablen und $\mathrm{FO}(\tau)$ alle Formeln $x = y$ für $x, y \in \text{VAR}$.

2.4 Semantik der Prädikatenlogik

Definition 2.8 (Modellbeziehung)**.** Sei τ eine Signatur. Eine τ-*Interpretation* ist ein Paar $\mathfrak{I} = (\mathfrak{A}, \beta)$, wobei $\mathfrak{A}$ eine τ-Struktur und $\beta : X \to A$ eine Belegung von Variablen durch Elemente von A ist. Dabei ist $X = \text{dom}(\beta) \subseteq \text{VAR}$. Eine τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ ordnet

- jedem Term $t \in \mathrm{T}(\tau)$ mit $\text{var}(t) \subseteq \text{dom}(\beta)$ einen Wert $[\![t]\!]^{\mathfrak{I}} \in A$ zu, und
- jeder Formel $\psi \in \mathrm{FO}(\tau)$ mit $\text{frei}(\psi) \subseteq \text{dom}(\beta)$ einen Wahrheitswert $[\![\psi]\!]^{\mathfrak{I}} \in \{0, 1\}$. (Wie üblich steht 0 für *falsch* und 1 für *wahr*.)

Die Zuordnung dieser Werte erfolgt induktiv gemäß dem Aufbau der Terme und Formeln. Für einen Term t ist $[\![t]\!]^{\mathfrak{I}}$ definiert durch:

- Für $x \in \text{dom}(\beta)$ ist $[\![x]\!]^{\mathfrak{I}} := \beta(x)$.
- Für $t = ft_1 \cdots t_n$ ist $[\![t]\!]^{\mathfrak{I}} := f^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{I}}, \ldots, [\![t_n]\!]^{\mathfrak{I}})$.

Für atomare Formeln ψ ist $[\![\psi]\!]^{\mathfrak{I}}$ wie folgt definiert:

- $[\![t_1 = t_2]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{wenn } [\![t_1]\!]^{\mathfrak{I}} = [\![t_2]\!]^{\mathfrak{I}}, \\ 0 & \text{sonst.} \end{cases}$
- $[\![Pt_1 \cdots t_n]\!]^{\mathfrak{I}} := \begin{cases} 1 & \text{wenn } ([\![t_1]\!]^{\mathfrak{I}}, \ldots, [\![t_n]\!]^{\mathfrak{I}}) \in P^{\mathfrak{A}}, \\ 0 & \text{sonst.} \end{cases}$

Die Bedeutung der Junktoren $\neg, \wedge, \vee$ und $\rightarrow$ ist genau die gleiche wie in der Aussagenlogik:

- $[\![\neg\psi]\!]^{\mathfrak{I}} := 1 - [\![\psi]\!]^{\mathfrak{I}}$.
- $[\![\psi \vee \varphi]\!]^{\mathfrak{I}} := \max([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.
- $[\![\psi \wedge \varphi]\!]^{\mathfrak{I}} := \min([\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.
- $[\![\psi \rightarrow \varphi]\!]^{\mathfrak{I}} := [\![\neg\psi \vee \varphi]\!]^{\mathfrak{I}} = \max(1 - [\![\psi]\!]^{\mathfrak{I}}, [\![\varphi]\!]^{\mathfrak{I}})$.

Um $[\![\exists x\psi]\!]^{\mathfrak{I}}$ und $[\![\forall x\psi]\!]^{\mathfrak{I}}$ zu definieren, verwenden wir folgende Notation: Sei $\beta : X \rightarrow A$ eine Belegung, x eine Variable und a ein Element von A. Wir definieren eine neue Belegung $\beta[x/a] : X \cup \{x\} \rightarrow A$ durch

$$\beta[x/a](y) := \begin{cases} \beta(y) & \text{wenn } y \neq x, \\ a & \text{sonst.} \end{cases}$$

Für $\mathfrak{I} = (\mathfrak{A}, \beta)$ setzen wir $\mathfrak{I}[x/a] := (\mathfrak{A}, \beta[x/a])$ und definieren:

- $[\![\exists x\psi]\!]^{\mathfrak{I}} := \max_{a \in A} [\![\psi]\!]^{\mathfrak{I}[x/a]}$.
- $[\![\forall x\psi]\!]^{\mathfrak{I}} := \min_{a \in A} [\![\psi]\!]^{\mathfrak{I}[x/a]}$.

Es gilt also genau dann $[\![\exists x\psi]\!]^{\mathfrak{I}} = 1$, wenn ein $a \in A$ existiert, so dass $[\![\psi]\!]^{\mathfrak{I}[x/a]} = 1$, und $[\![\forall x\psi]\!]^{\mathfrak{I}} = 1$, wenn für alle $a \in A$ gilt, dass $[\![\psi]\!]^{\mathfrak{I}[x/a]} = 1$.

Ein *Modell* einer Formel ψ ist eine Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$, so dass $\text{frei}(\psi) \subseteq \text{dom}(\beta)$ und $[\![\psi]\!]^{\mathfrak{I}} = 1$. Wir schreiben dann: $(\mathfrak{A}, \beta) \models \psi$ oder auch $\mathfrak{A} \models \psi[\beta]$ und sagen, dass ψ *in* $\mathfrak{A}$ *unter der Belegung* β *gilt*.

Ein *Modell einer Formelmenge* $\Phi \subseteq \text{FO}(\tau)$ ist eine τ-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$, so dass $\mathfrak{A} \models \varphi[\beta]$ für alle $\varphi \in \Phi$ gilt. Ein Modell einer Formelmenge erfüllt also alle Formeln in dieser Menge gleichzeitig.

Man beachte, dass eine Formel $\psi \in \text{FO}(\sigma)$ auch zu $\text{FO}(\tau)$ gehört, wenn $\sigma \subseteq \tau$. Eine Interpretation $(\mathfrak{A}, \beta)$ ist also *passend* für eine Formel ψ (oder eine Formelmenge Φ) wenn alle Funktions- und Relationssymbole von ψ (bzw. Φ) in der Signatur von $\mathfrak{A}$ enthalten sind und alle freien Variablen von ψ (bzw. Φ) zum Definitionsbereich von β gehören. Offensichtlich ist für die Modellbeziehung die Interpretation der Relations- und Funktionssymbole, welche in ψ gar nicht vorkommen,

sowie die Belegung der in ψ nicht frei auftretenden Variablen unerheblich. Dieser Sachverhalt, den man durch eine einfache, aber langweilige Induktion über den Formelaufbau nachweisen kann, wird durch das Koinzidenzlemma ausgedrückt.

Lemma 2.9 (Koinzidenzlemma)**.** Sei $\psi \in \mathrm{FO}(\sigma \cap \tau)$, $(\mathfrak{A}, \beta)$ eine σ-Interpretation und $(\mathfrak{A}', \beta')$ eine τ-Interpretation, so dass folgendes gilt:

(i) $\mathfrak{A}$ und $\mathfrak{A}'$ haben dasselbe $(\sigma \cap \tau)$-Redukt: $\mathfrak{A} \restriction (\sigma \cap \tau) = \mathfrak{A}' \restriction (\sigma \cap \tau)$.

(ii) $\mathrm{frei}(\psi) \subseteq \mathrm{dom}(\beta) \cap \mathrm{dom}(\beta')$ und $\beta(x) = \beta'(x)$ für alle $x \in \mathrm{frei}(\psi)$.

Dann gilt $\mathfrak{A} \models \psi[\beta]$ genau dann, wenn $\mathfrak{A}' \models \psi[\beta']$.

Notation. Wie erwähnt, deuten wir mit der Notation $\psi(x_1, \ldots, x_k)$ an, dass $\mathrm{frei}(\psi) \subseteq \{x_1, \ldots, x_k\}$. Sei nun $(\mathfrak{A}, \beta)$ eine Interpretation welche die Variablen $x_1, \ldots, x_k$ durch die Elemente $a_1 = \beta(x_1), \ldots, a_k = \beta(x_k)$ bewertet. Wir schreiben dann anstelle von $\mathfrak{A} \models \psi[\beta]$ meistens $\mathfrak{A} \models \psi(a_1, \ldots, a_k)$. (Diese Notation ist durch das Koinzidenzlemma gerechtfertigt, denn es gilt dann $\mathfrak{A} \models \psi[\beta']$ für *alle* Belegungen β', welche $x_1, \ldots, x_k$ auf $a_1, \ldots a_k$ abbilden.) Ist ψ ein Satz (also $\mathrm{frei}(\psi) = \emptyset$) so schreiben wir $\mathfrak{A} \models \psi$ und nennen $\mathfrak{A}$ ein Modell von ψ.

Beispiel. Sei $\psi := \exists z(Exz \wedge Ezy)$ und $\varphi := \forall x \forall y(Exy \to \psi)$. Offensichtlich ist ψ eine $\{E\}$-Formel mit $\mathrm{frei}(\psi) = \{x, y\}$ und φ ein $\{E\}$-Satz.

Die Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ mit $\mathfrak{A} = (\mathbb{N}, E^{\mathfrak{A}})$, $E^{\mathfrak{A}} = \{(m, n) : m \text{ ist ein echter Teiler von } n\}$ und $\beta(x) = 2$, $\beta(y) = 36$ ist ein Modell von $\psi(x, y)$, d.h. $\mathfrak{A} \models \psi(2, 36)$. In der Tat existiert ein $m \in \mathbb{N}$ (z.B. $m = 6$), so dass unter der Belegung $\beta[z/m]$ die Formel $(Exz \wedge Ezy)$ in $\mathfrak{A}$ gilt. Jedoch gilt *nicht* $\mathfrak{A} \models \varphi$, denn unter der Belegung $x \mapsto 2, y \mapsto 4$ ist $(Exy \to \psi)$ falsch in $\mathfrak{A}$ (2 ist echter Teiler von 4, aber es gibt keine Zahl, welche echt von 2 geteilt wird und ihrerseits 4 echt teilt). Hingegen ist $(\mathbb{Q}, <)$ ein Modell von φ, da $\mathbb{Q}$ dicht geordnet ist.

Definition 2.10. Sei Φ eine Menge von τ-Sätzen. Die *Modellklasse von* Φ (kurz: $\mathrm{Mod}(\Phi)$) besteht aus aus allen τ-Strukturen $\mathfrak{A}$ mit $\mathfrak{A} \models \Phi$. Eine Klasse $\mathcal{K}$ von τ-Strukturen ist *axiomatisiert durch* Φ, wenn $\mathcal{K} = \mathrm{Mod}(\Phi)$. Wir nennen Φ dann ein *Axiomensystem* für $\mathcal{K}$.

Beispiel.

- Die Klasse aller *ungerichteten Graphen* ist die Modellklasse von

$$\Phi_{\text{Graph}} = \{\forall x \neg Exx,\ \forall x \forall y (Exy \to Eyx)\}.$$

- Die Klasse aller *Gruppen* $(G, \circ, e, {}^{-1})$ ist axiomatisiert durch

$$\begin{aligned}\Phi_{\text{Gruppe}} = \{&\forall x \forall y \forall z (x \circ (y \circ z) = (x \circ y) \circ z),\\ &\forall x (x \circ e = x), \forall x (x \circ x^{-1} = e)\}.\end{aligned}$$

- Ein Axiomensystem für die Klasse aller linearen Ordnungen ist

$$\begin{aligned}\Phi_< = \{&\forall x \neg x < x, \forall x \forall y \forall z (x < y \wedge y < z \to x < z),\\ &\forall x \forall y (x < y \vee x = y \vee y < x)\}.\end{aligned}$$

- Für eine beliebige Signatur τ und $n \in \mathbb{N}$ sei $\mathcal{K}_{\geq n}$ die Klasse der τ-Strukturen mit mindestens n Elementen. $\mathcal{K}_{\geq n}$ ist (für $n \geq 2$) axiomatisiert durch den Satz

$$\varphi_{\geq n} := \exists x_1 \cdots \exists x_n \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j.$$

  Die Klasse $\mathcal{K}_\infty$ aller unendlichen τ-Strukturen ist axiomatisiert durch das unendliche Axiomensystem $\Phi_\infty = \{\varphi_{\geq n} : n \in \mathbb{N}\}$.

Die semantische Folgerungsbeziehung („ψ folgt aus Φ“), sowie die Begriffe „erfüllbar“, „allgemeingültig“ und „logisch äquivalent“ sind wie für die Aussagenlogik definiert.

Definition 2.11 (Semantische Folgerungsbeziehung)**.** Sei $\Phi \subseteq \text{FO}(\tau)$ eine Formelmenge, $\psi \in \text{FO}(\tau)$ eine Formel. Wir sagen, dass ψ *aus* Φ *folgt* (kurz: $\Phi \models \psi$), wenn jede zu $\Phi \cup \psi$ passende Interpretation, welche ein Modell von Φ ist, auch Modell von ψ ist. Wenn $\Phi = \{\varphi\}$ schreiben wir auch $\varphi \models \psi$ anstelle von $\{\varphi\} \models \psi$.

Beispiel.

- $\Phi_{\text{Gruppe}} \models \psi$ bedeutet, dass ψ in jeder Gruppe gilt. Man beachte, dass Φ_{Gruppe} eine Menge von Sätzen ist, dass aber in ψ durchaus

freie Variablen vorkommen dürfen. Da jedes Modell von Φ_{Gruppe} auch ein Modell von ψ sein muss, bedeutet $\Phi_{\text{Gruppe}} \models \psi$, dass $(\mathfrak{G}, \beta) \models \psi$ für jede Gruppe $\mathfrak{G}$ und jede Belegung β. Zum Beispiel gilt $\Phi_{\text{Gruppe}} \models x^{-1} \circ x = e$ (da in jeder Gruppe das (Rechts-)Inverse jedes Elements auch Linksinverses ist.) Hingegen ist $\Phi_{\text{Gruppe}} \not\models x \circ y = y \circ x$, da nicht jede Gruppe kommutativ ist.

- $\Phi_\infty \models \psi$ bedeutet, dass ψ in allen unendlichen Strukturen gilt.

Definition 2.12. Hat eine Formel ψ (oder eine Formelmenge Φ) ein Modell, so heißt ψ (bzw. Φ) *erfüllbar*, andernfalls *unerfüllbar*. Eine Formel ψ heißt *allgemeingültig* (kurz: $\models \psi$), wenn jede zu ψ passende Interpretation ein Modell von ψ ist. Dies ist äquivalent zu $\emptyset \models \psi$. Zwei Formeln ψ und φ heißen *logisch äquivalent* (kurz: $\psi \equiv \varphi$), wenn $\psi \models \varphi$ und $\varphi \models \psi$.

Definition 2.13. Sei ψ eine Formel mit freien Variablen $x_1, \ldots, x_k$. Dann nennen wir die Sätze $\exists x_1 \cdots \exists x_k \psi$ und $\forall x_1 \cdots \forall x_k \psi$ den *existentiellen* bzw. *universellen Abschluss* von ψ.

Lemma 2.14.

(i) Eine Formel ist genau dann erfüllbar, wenn ihr existentieller Abschluss erfüllbar ist.

(ii) Eine Formel ist genau dann allgemeingültig, wenn ihr universeller Abschluss allgemeingültig ist.

2.5 Normalformen

Der Begriff einer Normalform taucht in vielen Gebieten der Mathematik auf. Die allgemeine Situation ist die, dass auf einer Menge M von mathematischen Objekten (hier: von Formeln) eine Äquivalenzrelation $\sim$ gegeben ist. Angestrebt wird eine Aussage der Art, dass für eine bestimmte Teilmenge $N \subseteq M$ (von Objekten „in Normalform“) jede $\sim$-Äquivalenzklasse einen Repräsentanten in N besitzt. Oft sind auch stärkere Aussagen erwünscht, etwa über die effiziente Konstruierbarkeit solcher Repräsentanten. Ein bekanntes Beispiel aus der Linearen Algebra sind die Sätze über Normalformen von Matrizen.

Wir sind hier interessiert an Normalformen für Formeln der Prädikatenlogik. Die zugrunde gelegte Äquivalenzrelation ist in der Regel die

logische Äquivalenz; wir werden aber am Ende dieses Abschnitts auch eine Normalform für eine schwächere Äquivalenzrelation betrachten, nämlich die *Skolem-Normalform*.

Wir beginnen mit einer einfachen Beobachtung, welche die Technik begründet, Transformationen in äquivalente Formeln per Induktion über den Formelaufbau durchzuführen.

Lemma 2.15 (Ersetzungslemma)**.** Für beliebige Formeln $\psi, \psi', \varphi, \varphi' \in \mathrm{FO}(\tau)$ gilt:

(i) Wenn $\psi \equiv \varphi$, dann auch $\neg\psi \equiv \neg\varphi$.
(ii) Wenn $\psi \equiv \psi'$ und $\varphi \equiv \varphi'$, dann auch $(\psi \circ \varphi) \equiv (\psi' \circ \varphi')$ für $\circ \in \{\wedge, \vee, \rightarrow\}$.
(iii) Wenn $\psi \equiv \varphi$, dann auch $\exists x\psi \equiv \exists x\varphi$ und $\forall x\psi \equiv \forall x\varphi$.
(iv) Sei ϑ eine Teilformel von ψ und sei $\vartheta \equiv \varphi$. Sei weiter $\psi[\vartheta/\varphi]$ diejenige Formel, die man aus ψ erhält, indem man ϑ durch φ ersetzt. Dann ist $\psi \equiv \psi[\vartheta/\varphi]$.

Beweis. Die Aussagen (i)–(iii) sind trivial; (iv) ergibt sich durch Induktion über den Formelaufbau mittels (i)–(iii). Q.E.D.

Reduzierte Formeln. Aus der Definition der Modellbeziehung ergibt sich sofort, dass für beliebige Formeln ψ, φ folgende Äquivalenzen gelten. (1) und (2) kennen wir bereits aus der Aussagenlogik.

(1) $\psi \wedge \varphi \equiv \neg(\neg\psi \vee \neg\varphi)$,
(2) $\psi \rightarrow \varphi \equiv \neg\psi \vee \varphi$ und
(3) $\forall x\psi \equiv \neg\exists x\neg\psi$.

Daraus folgt, dass wir uns ohne Verlust an Ausdrucksstärke etwa auf die Junktoren $\vee, \neg$ und den Quantor $\exists$ beschränken können. Wir nennen Formeln, in denen die Symbole $\wedge, \rightarrow$ und $\forall$ nicht vorkommen, *reduziert*.

Lemma 2.16. Zu jeder Formel $\psi \in \mathrm{FO}(\tau)$ kann man effektiv eine logisch äquivalente reduzierte Formel konstruieren.

Wir können daher in vielen Fällen die Betrachtung auf reduzierte Formeln beschränken. Der Vorteil der Verwendung reduzierter Formeln liegt darin, dass sie aus weniger Symbolen aufgebaut sind und daher konzisere Definitionen und kürzere Induktionsbeweise erlauben.[1] Ein Nachteil reduzierter Formeln ist, dass sie länger und schlechter lesbar werden.

NEGATIONSNORMALFORM. In manchen Situationen (z.B. für Auswertungsalgorithmen oder für die spieltheoretische Deutung der Semantik, siehe Abschnitt 2.6) ist es praktisch, den nicht-monotonen Junktor $\rightarrow$ auszuschließen und die Anwendung der Negation auf atomare Formeln einzuschränken.

Definition 2.17. Eine Formel ist in *Negationsnormalform*, wenn sie aus Literalen (d.h. atomaren Formeln und Negationen atomarer Formeln) nur mit Hilfe der Junktoren $\vee$, $\wedge$ und der Quantoren $\exists$ und $\forall$ aufgebaut ist.

Satz 2.18. Jede Formel aus FO ist logisch äquivalent zu einer Formel in Negationsnormalform.

Beweis. Wir haben bereits gesehen, dass $\rightarrow$ eliminiert werden kann. Durch wiederholte Anwendung der De Morganschen Regeln

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

und den Quantorenregeln

$$\neg\exists x\psi \equiv \forall x\neg\psi\,, \qquad \neg\forall x\psi \equiv \exists x\neg\psi$$

sowie der Regel

$$\neg\neg\psi \equiv \psi$$

[1] Aus diesem Grund wird in einigen Lehrbüchern die Prädikatenlogik nur mit den Junktoren $\vee, \neg$ und dem Existenzquantor eingeführt. Formeln mit $\wedge, \vee, \rightarrow$ und $\forall$ werden als abkürzende, informelle Schreibweisen für die eigentlichen, reduzierten Formeln verstanden.

kann jede FO-Formel in eine äquivalente Formel transformiert werden, in der Negationen nur noch auf Atome angewandt werden. Q.E.D.

Beispiel. Um die Formel $\neg\exists x(Rxy \wedge \forall z(Sxz \to Ryy))$ in Negationsnormalform zu überführen, zieht man die Negationen schrittweise „nach innen“ und eliminiert $\to$:

$$\begin{aligned}\neg\exists x(Rxy \wedge \forall z(Sxz \to Ryy)) &\equiv \forall x\neg(Rxy \wedge \forall z(Sxz \to Ryy))\\ &\equiv \forall x(\neg Rxy \vee \neg\forall z(Sxz \to Ryy))\\ &\equiv \forall x(\neg Rxy \vee \exists z\neg(Sxz \to Ryy))\\ &\equiv \forall x(\neg Rxy \vee \exists z(Sxz \wedge \neg Ryy))\end{aligned}$$

Termreduzierte Formeln. Eine weitere Normalform, welche insbesondere für die Elimination von Funktionen nützlich ist, betrifft die Komplexität der darin auftretenden Terme. Eine Formel heißt *termreduziert*, wenn sie nur Atome der Form $R\bar{x}$, $f\bar{x} = y$ und $x = y$ enthält (also insbesondere keine Terme der Tiefe ≥ 2).

Lemma 2.19. Zu jeder Formel gibt es eine logisch äquivalente termreduzierte Formel.

Beweis. Wenn ψ nicht termreduziert ist, dann enthält ψ einen Term t der Form $t = f\bar{x}$, der in ψ an einer „verbotenen“ Stelle auftritt (z.B. als Argument in einem Atom $R \dots t \dots$ oder $t = t'$, oder als Subterm eines komplizierteren Terms). Führe eine neue Variable x_t ein und ersetze jedes Atom α, das t an einer solchen Stelle enthält, durch $\exists x_t(x_t = t \wedge \alpha[t/x_t])$, wobei $\alpha[t/x_t]$ die Formel sein soll, die man durch Ersetzten von t durch x_t gewinnt. Offensichtlich ist die modifizierte Formel logisch äquivalent zu ψ. Dieser Eliminationsschritt wird solange ausgeführt, bis ψ termreduziert ist. Q.E.D.

Pränex-Normalform. Wir betrachten zunächst einige logische Äquivalenzen für einfache Quantorenanwendungen.

Lemma 2.20. Für alle Formeln $\psi, \varphi \in \mathrm{FO}(\tau)$ gelten die folgenden logischen Äquivalenzen.

(i) $\exists x(\psi \vee \varphi) \equiv \exists x\psi \vee \exists x\varphi$ und $\forall x(\psi \wedge \varphi) \equiv \forall x\psi \wedge \forall x\varphi$.
(ii) Falls x nicht in ψ vorkommt, gilt:

$$\psi \vee \exists x\varphi \equiv \exists x(\psi \vee \varphi), \qquad \psi \wedge \exists x\varphi \equiv \exists x(\psi \wedge \varphi),$$
$$\psi \vee \forall x\varphi \equiv \forall x(\psi \vee \varphi), \qquad \psi \wedge \forall x\varphi \equiv \forall x(\psi \wedge \varphi).$$

(iii) $\neg\exists x\psi \equiv \forall x\neg\psi$ und $\neg\forall x\psi \equiv \exists x\neg\psi$.
(iv) $\exists x\exists y\psi \equiv \exists y\exists x\psi$ und $\forall x\forall y\psi \equiv \forall y\forall x\psi$.

Beweis. Wir führen exemplarisch den Beweis für die erste Behauptung in (ii) vor. Für jede zu beiden Seiten der Äquivalenz passende Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$ gilt:

	$\mathfrak{I} \models \psi \vee \exists x\varphi$
gdw.	$\mathfrak{I} \models \psi$ oder es gibt ein $a \in A$, so dass $\mathfrak{I}[x/a] \models \varphi$
gdw.	es gibt ein $a \in A$, so dass $\mathfrak{I}[x/a] \models \psi$ oder $\mathfrak{I}[x/a] \models \varphi$
	(Da $x \notin \text{frei}(\psi)$ gilt nach dem Koinzidenzlemma, dass $\mathfrak{I} \models \psi$ gdw. $\mathfrak{I}[x/a] \models \psi$.)
gdw.	es gibt ein $a \in A$, so dass $\mathfrak{I}[x/a] \models \psi \vee \varphi$
gdw.	$\mathfrak{I} \models \exists x(\psi \vee \varphi)$. Q.E.D.

Man beachte, dass einige zu (i) ganz ähnlich aussehende Formelpaare *nicht* äquivalent sind:

$$\exists x(\psi \wedge \varphi) \not\equiv \exists x\psi \wedge \exists x\varphi,$$
$$\forall x(\psi \vee \varphi) \not\equiv \forall x\psi \vee \forall x\varphi.$$

Weiter ist zu beachten, dass die Äquivalenzen in (ii) nicht gelten müssen, wenn x in ψ vorkommt.

Beispiel. Die Formel $\forall x(Px \vee Qx)$ ist weder zu $\forall xPx \vee \forall xQx$ noch zu $Px \vee \forall xQx$ äquivalent.

Wir sehen also, dass wir auf Konflikte zwischen freien und gebundenen Variablen achten müssen. Offensichtlich können wir aber gebundene Variablen umbenennen. Wenn die Variable y in $\exists x\psi$ nicht

vorkommt, dann ist nämlich $\exists x\psi \equiv \exists y\psi[x/y]$. Wir nennen eine Formel ψ *bereinigt*, wenn keine Variable in ψ sowohl frei wie gebunden auftritt, und wenn keine Variable mehr als einmal quantifiziert wird. Per Induktion über den Formelaufbau folgt, dass man durch systematisches Umbenennen gebundener Variablen zu jeder Formel eine äquivalente bereinigte Formel konstruieren kann.

Definition 2.21. Eine Formel ist in *Pränex-Normalform* (PNF), wenn sie bereinigt ist und die Form $Q_1x_1 \cdots Q_rx_r\varphi$ hat, wobei φ quantorenfrei und $Q_i \in \{\exists, \forall\}$ ist. Das Anfangsstück $Q_1x_1 \cdots Q_rx_r$ nennt man das *(Quantoren-)Präfix* der Formel.

Satz 2.22 (Satz über die Pränex-Normalform)**.** Jede Formel $\psi \in \mathrm{FO}(\tau)$ lässt sich in eine logisch äquivalente Formel in Pränex-Normalform transformieren.

Beweis. Der Beweis wird per Induktion über den Aufbau von ψ geführt. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass ψ den Junktor $\rightarrow$ nicht enthält.

- Quantorenfreie Formeln sind bereits in PNF.
- Sei $\psi = \neg\varphi$. Nach Induktionsvoraussetzung kann φ in eine logisch äquivalente Formel $\varphi' = Q_1x_1 \cdots Q_rx_r\vartheta'$ transformiert werden. Durch wiederholte Anwendung von Lemma 2.20 (iii) folgt, dass

  $$\psi \equiv \overline{Q_1}x_1 \cdots \overline{Q_r}x_r\neg\vartheta'$$

  wobei $\overline{\exists} := \forall$ und $\overline{\forall} := \exists$. Diese Formel hat die gewünschte Form.
- Sei $\psi = \varphi_1 \circ \varphi_2$ für $\circ \in \{\vee, \wedge\}$. Nach Induktionsvoraussetzung lassen sich φ_1 und φ_2 in logisch äquivalente Formeln in PNF umformen. Durch Umbenennung gebundener Variablen erreichen wir, dass diese Formeln die Form $\varphi_1' = Q_1x_1 \cdots Q_rx_r\vartheta_1$ und $\varphi_2' = Q_1'y_1 \ldots Q_s'y_s\vartheta_2$ haben, wobei $x_1, \ldots, x_r, y_1, \ldots, y_s$ paarweise verschieden und verschieden von allen freien Variablen in φ_1 und φ_2 sind. Sei nun

  $$\psi' := Q_1x_1 \cdots Q_rx_rQ_1'y_1 \cdots Q_s'y_s(\vartheta_1' \circ \vartheta_2').$$

Diese Formel hat die gewünschte Form, und da die Variablen $y_1, \dots, y_s$ nicht in φ_1' und $x_1, \dots, x_r$ nicht in φ_2' vorkommen, folgt mit Lemma 2.20 (ii), dass $\psi \equiv \psi'$.

- Sei $\psi = Qx\varphi$ für $Q \in \{\exists, \forall\}$ und sei $\varphi' := Q_1 x_1 \cdots Q_r x_r \vartheta'$ eine zu φ äquivalente Formel in PNF. Durch Umbenennen kann erreicht werden, dass die gebundenen Variablen von φ' von x verschieden sind. Dann ist $Qx\varphi'$ eine zu ψ äquivalente Formel in PNF. Q.E.D.

Beispiel. Sei $\psi := \neg\forall x \neg Rxx \wedge \forall x \exists y (Rxy \wedge (\neg Ryy \wedge \exists x Ryx))$. Die Transformation in eine äquivalente Formel in PNF, gemäß dem im Beweis beschriebenen Verfahren, ergibt:

$$\begin{aligned}\psi &\equiv \exists x Rxx \wedge \forall x \exists y (Rxy \wedge \exists x (\neg Ryy \wedge Ryx)) \\ &\equiv \exists u Ruu \wedge \forall x \exists y \exists z (Rxy \wedge (\neg Ryy \wedge Ryz)) \\ &\equiv \exists u \forall x \exists y \exists z (Ruu \wedge Rxy \wedge \neg Ryy \wedge Ryz).\end{aligned}$$

Übung 2.1. Geben Sie zu den folgenden Formeln äquivalente Formeln in PNF an:

(a) $\forall x \exists y Pxy \vee (\neg Qz \wedge \neg \exists x Rxy)$,
(b) $\exists y Rxy$ gdw. $\forall x Rxx$.

Skolem-Normalform. Im Gegensatz zur Pränex-Normalform ist die *Skolem-Normalform* einer Formel im Allgemeinen nicht zur ursprünglichen Formel logisch äquivalent; sie ist jedoch *erfüllbarkeitsäquivalent*.

Satz 2.23 (Satz über die Skolem-Normalform)**.** Zu jedem Satz $\psi \in \mathrm{FO}(\sigma)$ lässt sich ein Satz $\varphi \in \mathrm{FO}(\tau)$ mit $\sigma \subseteq \tau$ konstruieren, so dass gilt:

(i) $\varphi = \forall y_1 \cdots \forall y_s \varphi'$, wobei φ' quantorenfrei ist.
(ii) $\varphi \models \psi$.
(iii) Zu jedem Modell von ψ existiert eine Expansion, welche Modell von φ ist.

Die letzten beiden Punkte implizieren insbesondere, dass ψ und φ über den selben Universen erfüllbar sind.

Beweis. Nach dem Satz über die Pränex-Normalform können wir ohne Beschränkung der Allgemeinheit annehmen, dass

$$\psi = Q_1 x_1 \dots Q_r x_r \vartheta(x_1, \dots, x_r),$$

wobei $\vartheta(x_1, \dots, x_r)$ quantorenfrei ist. Für jedes $k \leq r$ sei

$$\psi_k(x_1, \dots, x_k) := Q_{k+1} x_{k+1} \dots Q_r x_r \vartheta(x_1, \dots, x_k, x_{k+1}, \dots, x_r).$$

Wir eliminieren Existenzquantoren schrittweise von außen nach innen durch folgenden Algorithmus. Sei Q_k der vorderste Existenzquantor. Die gegebene Formel hat also die Form

$$\psi = \forall x_1 \dots \forall x_{k-1} \exists x_k \psi_k(x_1, \dots, x_k).$$

Sei f ein neues, d.h. nicht in ψ vorkommendes, $(k-1)$-stelliges Funktionssymbol (für $k = 1$ also ein Konstantensymbol). Setze

$$\psi' := \forall x_1 \cdots \forall x_{k-1} \psi_k(x_1, \dots, x_{k-1}, f x_1 \cdots x_{k-1}).$$

Also ist ψ' die Formel, die wir aus ψ erhalten, indem wir die vorderste existentiell quantifizierte Variable x_k durch den Term $f x_1 \dots x_{k-1}$ ersetzen und den dazugehörenden Existenzquantor $\exists x_k$ eliminieren. Offensichtlich liefert die Iteration dieses Eliminationsschrittes schließlich eine Formel der gewünschten syntaktischen Gestalt. Zu zeigen bleibt, dass $\psi' \models \psi$ und dass jedes Modell von ψ zu einem Modell von ψ' expandiert werden kann.

Zur ersten Behauptung nehmen wir an, dass

$$\mathfrak{A} \models \psi' := \forall x_1 \cdots \forall x_{k-1} \psi_k(x_1, \dots, x_{k-1}, f x_1 \cdots x_{k-1}).$$

Also folgt, dass für alle $a_1, \dots, a_{k-1} \in A$, und für $b := f^{\mathfrak{A}}(a_1, \dots, a_{k-1})$ gilt, dass $\mathfrak{A} \models \psi_k(a_1, \dots, a_{k-1}, b)$. Damit ist gezeigt, dass

$$\mathfrak{A} \models \forall x_1 \cdots \forall x_{k-1} \exists x_k \psi_k(x_1, \dots, x_k),$$

also $\mathfrak{A} \models \psi$.

Zur zweiten Behauptung nehmen wir an, dass $\mathfrak{A} \models \psi$. Da f in ψ

nicht vorkommt, können wir annehmen, dass f nicht in der Signatur von $\mathfrak{A}$ enthalten ist. Wir definieren eine Funktion $f^{\mathfrak{A}} : A^{k-1} \to A$, so dass die Expansion $(\mathfrak{A}, f^{\mathfrak{A}})$ ein Modell von ψ' ist.

Da $\mathfrak{A} \models \forall x_1 \cdots \forall x_{k-1} \exists x_k \psi_k(x_1, \ldots, x_k)$ gibt es für alle $a_1, \ldots, a_k$ ein b, so dass $\mathfrak{A} \models \psi_k(a_1, \ldots, a_{k-1}, b)$. Wir wählen nun für jedes Tupel $(a_1, \ldots, a_{k-1})$ *ein* solches b und setzen $f^{\mathfrak{A}}(a_1, \ldots, a_{k-1}) := b$. Offensichtlich gilt also für alle $a_1, \ldots, a_{k-1}$, dass $(\mathfrak{A}, f^{\mathfrak{A}}) \models \psi_k(a_1, \ldots, a_{k-1}, b)$. Damit folgt, dass

$$(\mathfrak{A}, f^{\mathfrak{A}}) \models \forall x_1 \cdots \forall x_{k-1} \psi_k(x_1, \ldots, x_{k-1}, f x_1 \cdots x_{k-1}),$$

d.h. $(\mathfrak{A}, f^{\mathfrak{A}}) \models \psi'$. Q.E.D.

Übung 2.2 (Relationale Skolem-Normalform)**.** Zeigen Sie, dass zu jeder Formel $\psi \in \mathrm{FO}(\sigma)$ eine *relationale* Formel $\varphi \in \mathrm{FO}(\tau)$ der Gestalt $\forall x_1 \cdots \forall x_r \exists y_1 \cdots \exists y_s \eta$ mit quantorenfreiem η existiert, so dass ψ und φ über den selben Universen erfüllbar sind.

2.6 Spieltheoretische Semantik

> Der Mensch spielt nur,
> wo er in voller Bedeutung des Wortes Mensch ist,
> und er ist nur da ganz Mensch, wo er spielt.
> *Friedrich Schiller: Über die ästhetische Erziehung des Menschen*

> Nessuno ha mai sostenuto seriamente che i giochi siano inutili.
> *Umberto Eco*

Die Semantik der Prädikatenlogik kann man auch spieltheoretisch formulieren. Ein FO-Satz ψ und eine dazu passende Struktur $\mathfrak{A}$ definieren ein *Auswertungsspiel* $\mathrm{MC}(\mathfrak{A}, \psi)$ zwischen zwei Spielern, der *Verifiziererin* V und dem *Falsifizierer* F. Die Verifiziererin möchte zeigen, dass $\mathfrak{A}$ ein Modell für ψ ist, der Falsifizierer möchte nachweisen, dass dies nicht der Fall ist.

Der Einfachheit halber nehmen wir hier an, dass ψ in Negationsnormalform ist. Die Positionen des Spiels sind Paare (φ, β) bestehend aus einer Unterformel φ von ψ und einer Bewertung $\beta : \mathrm{frei}(\varphi) \to A$.

Für $\varphi = \varphi(\bar{x})$ und $\beta : \bar{x} \mapsto \bar{a}$ bezeichnen wir die Position (φ, β) in der Regel durch $\varphi(\bar{a})$.

Das Spiel beginnt bei der Position ψ. Sei $\varphi(\bar{a})$ die aktuelle Position. Dann geht das Spiel, abhängig von der Gestalt von φ, wie folgt weiter:

- Wenn φ ein Literal ist, dann ist das Spiel beendet. Die Verifiziererin hat gewonnen, falls $\mathfrak{A} \models \varphi(\bar{a})$, andernfalls hat der Falsifizierer gewonnen.
- An einer Position $(\vartheta \vee \eta)$ ist die Verifiziererin am Zug und kann entweder zu ϑ oder zu η ziehen.
- Analog zieht von einer Position $(\vartheta \wedge \eta)$ der Falsifizierer entweder zu ϑ oder zu η.
- An einer Position der Form $\exists x \vartheta(x, \bar{b})$ wählt die Verifiziererin ein Element $a \in A$ und zieht zu $\vartheta(a, \bar{b})$.
- Entsprechend darf an einer Position der Form $\forall x \vartheta(x, \bar{b})$ der Falsifizierer ein Element $a \in A$ auswählen und zur Position $\vartheta(a, \bar{b})$ ziehen.

Endliche Spiele. Wir geben hier eine allgemeinere Beschreibung von Spielen an (genauer: von Zweipersonenspielen mit vollständiger Information und positionaler Gewinnbedingung). Wir bezeichnen die Spieler als Spieler 0 und Spieler 1 und beschreiben das Spiel durch einen Spielgraphen $\mathcal{G} = (V, V_0, E)$ bestehend aus

- der Menge V aller *Spielpositionen*,
- der Teilmenge $V_0 \subseteq V$ der Positionen, an denen Spieler 0 am Zug ist; entsprechend ist $V_1 := V \setminus V_0$ die Menge der Positionen an denen Spieler 1 am Zug ist,
- der Menge $E \subseteq V \times V$ der möglichen *Züge.*

Für eine Position v sei $vE := \{w : (v, w) \in E\}$ die Menge der unmittelbaren Nachfolgepositionen. Eine Position v mit $vE = \emptyset$ ist eine *Endposition*. Wenn im Spiel eine Endposition erreicht wird, hat der Spieler verloren der am Zug ist (aber nicht ziehen kann). Mit anderen Worten: Für $\sigma \in \{0, 1\}$ ist die Menge T_σ der Endpositionen, an denen

Spieler σ gewonnen hat, definiert durch

$$T_\sigma := \{v \in V_{1-\sigma} : vE = \emptyset\}.$$

Eine *Partie* mit Anfangsposition v_0 ist ein endlicher oder unendlicher Pfad $(v_0, v_1, \ldots, v_m)$ bzw. $(v_0, v_1, \ldots)$, so dass $(v_{i-1}, v_i) \in E$ für alle $i > 0$ und v_m eine Endposition ist.

Auswertungsspiele für FO sind insofern speziell als alle Partien endlich sind (da jeder Zug die Komplexität der Formel reduziert). Spiele mit dieser Eigenschaft nennt man *fundiert*.[2]
Eine *Strategie* für Spieler σ ist eine Funktion

$$f : \{v \in V_\sigma : vE \neq \emptyset\} \to V,$$

so dass $(v, f(v)) \in E$; sie ordnet also jeder nicht-terminalen Position von Spieler σ einen Zug zu. Wenn Spieler σ jede Partie mit Anfangsposition v_0 gewinnt, wenn er mit Strategie f spielt, dann ist f eine *Gewinnstrategie* von Position v_0 aus. Formaler: Eine Partie $v_0 v_1 \ldots$ ist konsistent mit der Strategie f wenn für alle i mit $v_i \in V_\sigma$ gilt, dass $v_{i+1} = f(v_i)$; f ist Gewinnstrategie für Spieler σ von v_0, wenn jede bei v_0 beginnende und mit f konsistente Partie endlich ist und in einer Position in T_σ endet. Die *Gewinnregion* von Spieler σ ist

$$W_\sigma := \{v : \text{Spieler } \sigma \text{ hat eine Gewinnstrategie von Position } v\}.$$

Ein Spiel ist *determiniert*, wenn von jeder Position aus einer der beiden Spieler eine Gewinnstrategie hat, d.h. wenn $W_0 \cup W_1 = V$.

Übung 2.3. Zeigen Sie, dass fundierte Spiele determiniert sind.

Sei nun $\psi \in$ FO und $\mathfrak{A}$ eine zu ψ passende Struktur. Per Induktion über den Aufbau von $\varphi(\bar{x})$ zeigt man leicht, dass in dem Spiel $\mathrm{MC}(\mathfrak{A}, \psi)$ die Verifiziererin eine Gewinnstrategie von Position $\varphi(\bar{a})$ hat, wenn $\mathfrak{A} \models \varphi(\bar{a})$, und dass der Falsifizierer eine Gewinnstrategie von Position $\varphi(\bar{a})$ hat, wenn $\mathfrak{A} \models \neg\varphi(\bar{a})$. Insbesondere folgt damit:

[2] Allgemeine Spiele lassen auch unendliche Partien zu. In der Theorie unendlicher Spiele braucht man daher Gewinnbedingungen für unendliche Partien. Hier werten wir unendliche Partien als unentschieden.

Satz 2.24. Für jeden Satz $\psi \in \mathrm{FO}(\tau)$ und jede τ-Struktur $\mathfrak{A}$ gilt: $\mathfrak{A} \models \psi$ genau dann, wenn die Verifiziererin eine Gewinnstrategie für das Spiel $\mathrm{MC}(\mathfrak{A}, \psi)$ von der Anfangsposition ψ hat.

ALGORITHMEN FÜR STRATEGIEPROBLEME. Sei GAME das Strategieproblem für Spiele mit endlichen Spielgraphen, d.h.

$$\textsc{Game} = \{(\mathcal{G}, v) : \text{Spieler 0 hat eine Gewinnstrategie für } \mathcal{G} \text{ von Position } v\}.$$

Es ist nicht schwer einzusehen, dass man GAME in Polynomialzeit lösen kann. Sei W_σ^n die Menge der Positionen von denen Spieler σ eine Strategie hat, um in höchstens n Zügen zu gewinnen. Dann ist $W_\sigma^0 = T_\sigma = \{v \in V_{1-\sigma} : vE = \emptyset\}$ die Menge der Endpositionen an denen Spieler σ gewonnen hat, und wir können die Mengen W_σ^n induktiv berechnen mit

$$W_\sigma^{n+1} := \{v \in V_\sigma : vE \cap W_\sigma^n \neq \emptyset\} \cup \{v \in V_{1-\sigma} : vE \subseteq W_\sigma^n\}$$

bis $W_\sigma^{n+1} = W_\sigma^n$.

Man kann das GAME-Problem sogar in *Linearzeit* lösen. Der folgende Algorithmus ist eine Variante der Tiefensuche und berechnet die Gewinnregionen W_σ für beide Spieler in Zeit $O(|V| + |E|)$.

Satz 2.25. Die Gewinnregionen von endlichen Spielen kann man in Linearzeit berechnen.

Beweis. Wir präsentieren einen Algorithmus welcher für jede Position bestimmt, ob einer der Spieler von dieser Position aus eine Gewinnstrategie hat, und wenn ja welcher. Wir benutzen die folgenden Arrays:

- $\mathrm{win}[v]$ enthält entweder $\sigma \in \{0, 1\}$, wenn schon festgelegt ist, dass $v \in W_\sigma$ oder $\perp$, wenn dies noch nicht ausgerechnet ist, oder wenn keiner der Spieler von v aus eine Gewinnstrategie hat.
- $P[v]$ einhält die Vorgänger von v.
- $n[v]$ ist die Anzahl der Nachfolger $w \in vE$ für die $\mathrm{win}[w] = \perp$.

Algorithmus 2.1. Ein Linearzeit-Algorithmus für das GAME-Problem

Input: Ein Spiel $\mathcal{G} = (V, V_0, E)$

for all $v \in V$ **do** ($*$ 1: Initialisierung $*$)
  win$[v] := \bot$
  $P[v] := \emptyset$
  $n[v] := 0$
end do

for all $(u, v) \in E$ **do** ($*$ 2: Berechne P und n $*$)
  $P[v] := P[v] \cup \{u\}$
  $n[u] := n[u] + 1$
end do

for all $v \in V_0$ ($*$ 3: Berechne win $*$)
  if $n[v] = 0$ **then** Propagate(v, 1)
for all $v \in V \setminus V_0$
  if $n[v] = 0$ **then** Propagate(v, 0)
return win

procedure Propagate(v, σ)
  if win$[v] \neq \bot$ **then return**
  win$[v] := \sigma$ ($*$ 4: Markiere v als gewinnend für σ $*$)
  for all $u \in P[v]$ **do** ($*$ 5: Propagiere zu Vorgängern $*$)
    $n[u] := n[u] - 1$
    if $u \in V_\sigma$ or $n[u] = 0$ **then** Propagate(u, σ)
  end do
end

Der Kern von Algorithmus 2.1 ist die Prozedur Propagate(v, σ) welche immer dann aufgerufen wird, wenn festgestellt wurde, dass Spieler σ eine Gewinnstrategie von Position v hat. Propagate(v, σ) speichert dies ab und untersucht, ob wir nun den Gewinner für die Vorgänger von v bestimmen können. Dies wird mit folgenden Regeln festgestellt:

- Wenn der Vorgänger u auch eine Position von Spieler σ ist, dann hat er eine Gewinnstrategie, indem er im ersten Zug zu v zieht.
- Wenn der Gegner von Position u zieht, win$[u]$ noch undefiniert ist, und der Gewinner für alle Nachfolger w von u bereits festgestellt ist, dann ist win$[w] = \sigma$ für alle diese w, und Spieler σ gewinnt daher auch von u unabhängig vom Zug seines Gegners.

Da (4) und (5) für jede Position v nur einmal erreicht werden, wird der innere Teil der Schleife in (5) höchstens $\sum_v |P[v]| = |E|$-mal durchlaufen. Die Laufzeit des Algorithmus ist daher $O(|V| + |E|)$.

Die Korrektheit des ausgerechneten Wertes win$[v]$ beweist man durch Induktion über die minimale Anzahl der Züge mit der ein Spieler von v aus gewinnen kann. Man beachte, dass die Positionen mit $n[v] = 0$ in (3) genau die Endpositionen sind, auch wenn $n[v]$ durch Propagate modifiziert wird. Q.E.D.

Übung 2.4 (Auswertung von FO auf endlichen Strukturen)**.** Konstruieren Sie (auf der Basis des Auswertungsspiels) einen möglichst effizienten Auswertungsalgorithmus für FO-Sätze auf endlichen Strukturen. Schätzen Sie die Laufzeit und den Speicherbedarf des Algorithmus ab, abhängig von der Größe der gegebenen Struktur und der Länge (oder Komplexität) des gegebenen Satzes.

Übung 2.5. Formulieren Sie ein Auswertungsspiel für FO-Formeln, welche nicht notwendigerweise in Negationsnormalform sind. Welcher spieltheoretischen Operation entspricht die Negation?

Übung 2.6. Wir wissen bereits, dass das Erfüllbarkeitsproblem für aussagenlogische Hornformeln in Polynomialzeit lösbar ist. Mit Hilfe des Game-Problems kann man auf relativ einfache Weise zeigen, dass es sogar einen Linearzeit-Algorithmus gibt.

Konstruieren Sie zu einer gegebenen Hornformel $\psi = \bigwedge_{i \in I} C_i$ mit Aussagenvariablen $X_1, \ldots, X_n$ und Horn-Implikationen C_i der Form $X_{i_1} \wedge \cdots X_{i_m} \to Z$ ein Spiel $\mathcal{G}_\psi$: Die Positionen von Spieler 0 sind die Anfangsposition 0 und die Aussagenvariablen $X_1, \ldots, X_n$, die Positionen von Spieler 1 sind die C_i. Spieler 0 kann von einer Position X zu irgendeiner Implikation C_i mit rechter Seite X ziehen, und Spieler 1 kann von Position C_i zu irgendeiner Variable ziehen, die auf der linken Seite von C_i vorkommt. Zeigen Sie, dass Spieler 0 genau dann eine Gewinnstrategie für $\mathcal{G}_\psi$ von Position X hat, wenn $\psi \models X$. Insbesondere ist ψ genau dann unerfüllbar, wenn Spieler 0 von der Anfangsposition 0 gewinnt.

Übung 2.7 (Umkehrung der letzten Übung)**.** Konstruieren Sie zu jedem Spiel $\mathcal{G}$ eine aussagenlogische Hornformel $\psi_\mathcal{G}$, deren Aussagenvariablen die Positionen von $\mathcal{G}$ sind und deren minimales Modell gerade die Gewinnregion W_0 ist. Insbesondere ist $v \in W_0$ genau dann, wenn $\psi_\mathcal{G} \wedge (v \to 0)$ unerfüllbar ist.