

Prädikatenlogik 1. Stufe

- ▶ **Strukturen**
- ▶ **Syntax und Semantik**
- ▶ **Normalformen**
- ▶ **Sequenzenkalkül**
- ▶ **Fundamentale Sätze**
- ▶ **(Un-)Entscheidbarkeit**
- ▶ **Prädikatenlogik in PVS**
- ▶ **Ausdrucksstärke**
- ▶ **Peano-Arithmetik**

Schwäche der Aussagenlogik

Aussagenlogik hat zwar **Vorteile** (z.B. Entscheidbarkeit mittels Sequenzenkalkül, Resolution, DPLL, etc.), ist jedoch für viele Anwendungen **nicht ausdrucksstark** genug.

Wie z.B. formalisieren:

- “Jede Quadratzahl ist positiv” und “25 ist Quadratzahl”, also “25 ist positiv”. Ist offensichtlich richtig, hat aber Struktur $A \wedge B \rightarrow C$. **Abstraktion** in reine Aussagen verdeckt hier den Grund für die Wahrheit.
- “Partielle Ordnung $(M, \leq)$ ist total”. $\bigwedge_{x,y \in M} A_{x,y} \vee A_{y,x}$
funktioniert nur für **endliche** Mengen M . Außerdem wünschenswert: **eine** Formel, die dies für **alle** partiellen Ordnungen besagt.

Interpretation, die lediglich Aussagenvariablen Wahrheitswerte zuordnen, reichen dann nicht aus.

Signaturen

Def.: Eine Signatur τ ist eine Menge/Liste von **Relationssymbolen** R und **Funktionssymbolen** f , jeweils mit **Stelligkeit** $st(R), st(f) \geq 0$. Null-stellige Funktionssymbole heißen **Konstanten**, null-st. Relationssymbole **Propositionen**.

Bsp.:

- $\tau_{ar}^< = (<, +, \cdot, 0, 1)$ ist Signatur der **geordneten Arithmetik** mit $<$ 2-st. Relationssymbol, $+, \cdot$ 2-st. Funktionssymbole, $0, 1$ Konstanten.
- $\tau_{ar} = (+, \cdot, 0, 1)$ wie oben ist Signatur der **Arithmetik**.
- $\tau_{Gr} = (E)$ ist Signatur der Graphen.
- $\tau_{VR} = (+, \bar{0}, (\cdot_k)_{k \in K})$ ist Signatur der Vektorräume über Körper K .
- ...

τ -Strukturen

Def. Sei $\tau = (R_1, \dots, R_n, f_1, \dots, f_m)$. Eine τ -Struktur ist ein $\mathcal{A} = (A, R_1^{\mathcal{A}}, \dots, R_n^{\mathcal{A}}, f_1^{\mathcal{A}}, \dots, f_m^{\mathcal{A}})$, wobei

- A nicht-leere Menge, genannt **Universum** von $\mathcal{A}$
- $R_i^{\mathcal{A}} \subseteq \underbrace{A \times \dots \times A}_{st(R_i)}$ für $i \in \{1, \dots, n\}$
- $f_i^{\mathcal{A}} : \underbrace{A \times \dots \times A}_{st(f_i)} \rightarrow A$ für $i \in \{1, \dots, m\}$

Beachte Unterscheidung zwischen **Relationssymbol** R und konkreter **Relation** $R^{\mathcal{A}}$ in $\mathcal{A}$.

Bsp.:

- $(\mathbb{N}, +, \cdot, 0, 1, <)$ ist $\tau_{ar}^{<}$ -Struktur.
- $(\{\bullet\}, f, g, c, d, R)$ mit $f(\bullet, \bullet) = g(\bullet, \bullet) = \bullet = c = d$ und $R(\bullet, \bullet)$ oder $R = \emptyset$ ist jeweils ebenfalls $\tau_{ar}^{<}$ -Struktur.

Beispiele

- $\tau_{LTS} = ((\xrightarrow{a})_{a \in Act}, P_1, \dots, P_n)$, wobei Act endliche Menge von Aktionsnamen, $\xrightarrow{a}$ jeweils 2-st., P_i einstellige Relationen (Prädikate)

Ein τ_{LTS} -Struktur ist ein **beschriftetes Transitionssystem**, modelliert operationale Semantik eines Programms: $\xrightarrow{a}$ ist Übergangsrelation zwischen Zuständen (z.B. "Eintritt in Methode f "), P_i beschreibt, was in einzelnen Zuständen gilt (z.B. "Programmvariable x hat Wert im erlaubten Bereich").

- **Relationale Datenbank** mit Tabellen $T_1, \dots, T_n$ kann leicht als τ -Struktur mit entsprechendem τ aufgefasst werden.

Terme

Ab sofort wird Signatur τ als festgelegt angenommen.

Sei $\mathcal{V} = \{x, y, \dots\}$ Vorrat an Variablen.

Def.: Terme sind induktiv definiert wie folgt:

- Jede Variable ist ein Term.
- Sind $t_1, \dots, t_n$ Terme und f ein n -st. Funktionssymbol, so ist auch $f(t_1, \dots, t_n)$ Term.

Beachte: Mit $n = 0$ im zweiten Fall sind somit auch Konstanten Terme.

Bsp.: $+(*(x, +(1, y)), 0)$

In solchen Fällen benutzen wir auch Infix-Notation $(x * (1 + y)) + 0$, mit entsprechender Klammerung, da keine Präzedenzen festgelegt sind.

Formeln

Def.: **Formeln** der **Prädikatenlogik 1. Stufe mit Gleichheit** (FO) sind induktiv aufgebaut wie folgt.

- Sind t_1, t_2 Terme, so ist $t_1 \doteq t_2$ Formel.
- Sind $t_1, \dots, t_n$ Terme, so ist $R(t_1, \dots, t_n)$ Formel, falls $st(R) = n$.
- Sind φ, ψ Formeln, so auch $\neg\varphi, \varphi \vee \psi, \varphi \wedge \psi, \varphi \rightarrow \psi$,
- Ist φ Formel und x Variable, so sind auch $\exists x.\varphi$ und $\forall x.\varphi$ Formeln.

Wir verwenden $\varphi \leftrightarrow \psi$ evtl. als Abkürzung für $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

Bsp.: $\exists x.\forall y.R(f(x, y)) \rightarrow \forall x.\exists y.y \doteq f(x, x)$

Bem.: Die Bezeichnung “erststufig” bedeutet, dass nur über Elemente des Universums quantifiziert werden kann, nicht jedoch über Teilmengen, Funktionen, Relationen, etc.

Freie Variablen

Def.: Ist φ Formel, so bezeichnet $\text{frei}(\varphi)$ die in φ **frei**, d.h. nicht durch einen **Quantor** $\exists$ oder $\forall$ **vorkommenden** Variablen.

Bsp.: $\text{frei}(\forall y.R(x, f(c, y)) \vee \exists x.\neg(y \doteq f(d, x))) = \{x, y\}!$

Übung: Definiere $\text{frei}(\varphi)$ induktiv über den Term- und Formelaufbau.

Def.: Ist $\text{frei}(\varphi) = \emptyset$, so heißt φ auch **Satz**.

Bsp.: $\exists x.\forall y.R(x, y) \rightarrow \forall y.\exists x.R(x, y)$ ist Satz

Wir schreiben auch $\varphi(x_1, \dots, x_n)$ um auszudrücken, dass $\text{frei}(\varphi) \subseteq \{x_1, \dots, x_n\}$.

Substitutionen

Def.: $\varphi[t/x]$ bezeichnet das **simultane Ersetzen** aller freien Vorkommen der Variable x in φ durch den Term t , wobei quantifizierte Variablen, die auch in t vorkommen, in φ eindeutig umbenannt werden.

Bsp.:

$$(\forall y.(\exists x.R(x, z)) \wedge Q(x, y))[f(y)/x] = \forall v.(\exists x.R(x, z)) \wedge Q(f(y), v)$$

Interpretationen für Terme

In der Aussagenlogik waren Interpretation lediglich Belegungen der Aussagenvariablen. Dies ist hier offensichtlich nicht ausreichend, um einer Formel einen Wahrheitswert zuzuordnen.

Def.: Eine **Interpretation** einer FO-Formel über der Signatur τ ist ein $\mathcal{I} = (\mathcal{A}, \vartheta)$, wobei $\mathcal{A}$ τ -Struktur mit Universum A und $\vartheta : \mathcal{V} \rightarrow A$ ist. Dies induziert gleich auch eine Interpretation aller Terme.

$$\begin{aligned}\llbracket x \rrbracket_{\vartheta}^{\mathcal{A}} &:= \vartheta(x) \\ \llbracket f(t_1, \dots, t_n) \rrbracket_{\vartheta}^{\mathcal{A}} &:= f^{\mathcal{A}}(\llbracket t_1 \rrbracket_{\vartheta}^{\mathcal{A}}, \dots, \llbracket t_n \rrbracket_{\vartheta}^{\mathcal{A}})\end{aligned}$$

Bsp.:

- $\mathcal{A} = (\mathbb{N}, +, \cdot, 0, 1)$, $\vartheta(x) = 3$, $\vartheta(y) = 4$. Dann ist $\llbracket (x * (1 + y)) + 0 \rrbracket_{\vartheta}^{\mathcal{A}} = 15$.
- $\mathcal{B} = (\{\mathbf{tt}, \mathbf{ff}\}, \vee, \wedge, \mathbf{tt}, \mathbf{ff})$. $\vartheta(x) = \mathbf{tt}$, $\vartheta(y) = \mathbf{ff}$. Dann ist $\llbracket (x * (1 + y)) + 0 \rrbracket_{\vartheta}^{\mathcal{B}} = \mathbf{tt}$.

... und für Formeln

Def.: Sei $\mathcal{I} = (\mathcal{A}, \vartheta)$, A Universum von $\mathcal{A}$, $c \in A$. Mit $\vartheta[x \mapsto c]$ bezeichnen wir den üblichen Update von ϑ an der Stelle x auf c .

$\mathcal{I}$ ist **Modell** von φ oder **erfüllt** φ , wenn $\mathcal{I} \models \varphi$ gilt, wobei

$$\mathcal{A}, \vartheta \models t_1 \doteq t_2 \quad \text{gdw.} \quad \llbracket t_1 \rrbracket_{\vartheta}^{\mathcal{A}} = \llbracket t_2 \rrbracket_{\vartheta}^{\mathcal{A}}$$

$$\mathcal{A}, \vartheta \models R(t_1, \dots, t_n) \quad \text{gdw.} \quad (\llbracket t_1 \rrbracket_{\vartheta}^{\mathcal{A}}, \dots, \llbracket t_n \rrbracket_{\vartheta}^{\mathcal{A}}) \in R^{\mathcal{A}}$$

$$\mathcal{A}, \vartheta \models \neg \varphi \quad \text{gdw.} \quad \mathcal{A}, \vartheta \not\models \varphi$$

$$\mathcal{A}, \vartheta \models \varphi \wedge \psi \quad \text{gdw.} \quad \mathcal{A}, \vartheta \models \varphi \text{ und } \mathcal{A}, \vartheta \models \psi$$

$$\mathcal{A}, \vartheta \models \varphi \vee \psi \quad \text{gdw.} \quad \mathcal{A}, \vartheta \models \varphi \text{ oder } \mathcal{A}, \vartheta \models \psi$$

$$\mathcal{A}, \vartheta \models \varphi \rightarrow \psi \quad \text{gdw.} \quad \text{wenn } \mathcal{A}, \vartheta \not\models \varphi \text{ dann } \mathcal{A}, \vartheta \models \psi$$

$$\mathcal{A}, \vartheta \models \exists x. \varphi \quad \text{gdw.} \quad \text{es gibt } c \in A \text{ mit } \mathcal{A}, \vartheta[x \mapsto c] \models \varphi$$

$$\mathcal{A}, \vartheta \models \forall x. \varphi \quad \text{gdw.} \quad \text{für alle } c \in A \text{ gilt } \mathcal{A}, \vartheta[x \mapsto c] \models \varphi$$

Erfüllbarkeit, Äquivalenz, etc.

Die Begriffe **Erfüllbarkeit**, **Allgemeingültigkeit** und **Äquivalenz** ($\iff$), Erfüllbarkeitsäquivalenz ($\equiv_{sat}$) sind wie bei der Aussagenlogik definiert.

Beachte: Interpretation ist Paar aus Struktur und Variablenbelegung. Also ist z.B. $\exists x.R(x, y)$ erfüllbar trotz freier Variablen.

Insbesondere ist φ erfüllbar gdw. $\neg\varphi$ nicht allgemeingültig ist.

Bsp.: Neben den üblichen aussagenlogischen Äquivalenzen gelten weitere, z.B.

- $\exists x.\varphi \iff \neg\forall x.\neg\varphi$
- $\exists x.\exists y.\varphi \iff \exists y.\exists x.\varphi$
- $\exists x.\varphi \iff \exists y.\varphi[y/x]$
- $\exists x.\varphi \vee \exists x.\psi \iff \exists x.(\varphi \vee \psi)$
- ...

Die Theorie einer Strukturklasse

Wir untersuchen kurz Beziehungen zwischen Klassen von Strukturen und Klassen von Formeln.

Def.: Sei $\mathcal{K}$ eine Klasse von τ -Strukturen. Ihre (FO-)Theorie ist $Th(\mathcal{K}) := \{\varphi \mid \varphi \text{ ist FO-Satz und } \mathcal{A} \models \varphi \text{ für alle } \mathcal{A} \in \mathcal{K}\}$.

Bsp.: Sei $\mathcal{K}_G$ die Klasse aller Gruppen. Dann ist

$$\forall x.(\exists y.x \circ y \doteq 1) \rightarrow y \doteq i(x) \in Th(\mathcal{K}_G)$$

denn inverse Elemente in Gruppen sind eindeutig.

Definierbarkeit

Def.: Sei Φ eine Menge von Sätzen über einer Signatur τ . Ihre **Modellklasse** ist $Mod(\Phi) := \{\mathcal{A} \mid \mathcal{A} \text{ ist } \tau\text{-Struktur und } \mathcal{A} \models \varphi \text{ für alle } \varphi \in \Phi\}$.

Bsp.: $\tau = (\circ, i, 1)$,

$$\Phi_{Gruppe} = \{\forall x. \forall y. \forall z. (x \circ y) \circ z \doteq x \circ (y \circ z), \forall x. x \circ i(x) \doteq 1, \forall x. x \circ 1 \doteq x\}$$

Dann ist $Mod(\Phi_{Gruppe})$ die Klasse aller **Gruppen**.

Bsp.: $\tau = (E)$

$$\Phi_{Digraph} = \{\forall x. \forall y. E(x, y) \leftrightarrow E(y, x), \forall x. \neg E(x, x)\}$$

Dann ist $Mod(\Phi_{Digraph})$ die Klasse aller **ungerichteten Graphen**.

Semantische Folgerung

Def.: Sei Φ Formelmenge, ψ Formel. Dann **folgt** ψ aus Φ , $\Phi \models \psi$, falls für alle Interpretation $\mathcal{I}$ gilt: wenn $\mathcal{I} \models \varphi$ für alle $\varphi \in \Phi$, dann gilt $\mathcal{I} \models \psi$.

Bsp.:

- $\Phi_{\text{Gruppe}} \models \forall x. i(x) \circ x \doteq 1$, denn in jeder Gruppe ist das Rechts-Inverse von x auch Links-Inverses.
- $\Phi_{\text{Gruppe}} \not\models \forall x. \forall y. x \circ y \doteq y \circ x$, denn es gibt auch nicht-kommutative Gruppen.

Definierbarkeit von Relationen

Def.: Eine n -stellige Relation R heißt **definierbar in der Strukturklasse** $\mathfrak{K}$, wenn es eine Formel $\varphi(x_1, \dots, x_n)$ gibt, so dass für alle $\mathcal{A} \in \mathfrak{K}$ mit Universum A und alle $a_1, \dots, a_n \in A$ gilt:

$$(a_1, \dots, a_n) \in R^{\mathcal{A}} \quad \text{gdw.} \quad \mathcal{A}, [x_1 \mapsto a_1, \dots, x_n \mapsto a_n] \models \varphi$$

Bsp.: Sei $\mathfrak{K} = \{(\mathbb{R}, +, \cdot, 0, 1)\}$ mit üblicher Bedeutung. Dann ist die übliche totale Ordnung $<$ darin definierbar.

$$\varphi^{<}(x, y) := \exists z. \neg(z \doteq 0) \wedge y \doteq x + z \cdot z$$

Bsp.: $\tau = (ChildOf, SiblingOf, Male, Female)$. Dann ist z.B. die 2-stellige Relation des Onkel-Seins definierbar.

$$UncleOf(x, y) = \exists z. ChildOf(y, z) \wedge Sibling(x, z) \wedge Male(x)$$

Bem.: Relation des Verwandt-Seins ist **nicht** definierbar. Aber wie zeigt man das?

Die Sonderrolle der Gleichheit

Beachte: Gleichheit ($=$) ist zweistellige Relation auf Universum. Warum wird diese dann **gesondert** behandelt, d.h. kommt nicht in den Signaturen aber in Formeln (als $\doteq$) vor?

Antwort: Dann könnte die Relation $\doteq$ **irgendwie** interpretiert werden.

Bsp.: $\exists x.\exists y.\exists z.x \doteq y \wedge y \doteq z \wedge \neg(x \doteq z)$ wäre dann erfüllbar. Dies **widerspricht** jedoch der Intuition von Gleichheit, die ja modelliert werden soll.

Es reicht selbst nicht, wenn man verlangt, dass $\doteq$ immer reflexiv, transitiv und symmetrisch sein soll, da es auch größere Äquivalenzrelationen als der Gleichheit gibt.

Gleichheit ist auch **nicht definierbar**.

Normalformen

Wie bei der Aussagenlogik lassen sich Formeln wieder in dazu **äquivalente** umwandeln, die eine bestimmte Form haben.

Achtung: verschiedene Äquivalenzbegriffe möglich, z.B. starke Äquivalenz $\iff$ oder Erfüllbarkeitsäquivalenz $\equiv_{sat}$

Normalformen vereinfachen häufig Beweise

hier:

- positive Normalform
- Pränex-Normalform
- Skolem-Normalform

Positive Normalform

Def.: Eine Formel φ ist in **positiver Normalform**, wenn das Negationssymbol in ihr nur unmittelbar vor atomaren Formeln der Form $t_1 \doteq t_2$ oder $R(t_1, \dots, t_n)$ vorkommt. Als Operatoren sind nur $\wedge$, $\vee$, $\exists$, $\forall$ erlaubt.

Thm.: Für jedes $\varphi \in \text{FO}$ existiert ψ in positiver Normalform, so dass $\varphi \iff \psi$.

BEWEIS: Übung.

Bem.: Blow-up ist linear.

Pränex-Normalform

Def.: φ ist in **Pränex-Normalform**, falls

$$\varphi = Q_1 x_1. Q_2 x_2 \dots Q_n x_n. \chi$$

wobei $Q_1, \dots, Q_n \in \{\exists, \forall\}$ und χ **quantorenfrei**.

Thm.: Für jedes $\varphi \in \text{FO}$ gibt es ψ in Pränex-Normalform, so dass $\psi \iff \varphi$ und $|\psi| = \mathcal{O}(|\varphi|)$.

BEWEIS: O.B.d.A. sei φ in positiver Normalform. Konstruktion von ψ per Induktion über den Aufbau von φ . Ist φ atomar, dann ist φ offensichtlich bereits in Pränex-Normalform. Sei φ nicht atomar. Dann gibt es vier Fälle.

- $\varphi = Qx.\varphi'$ für ein $Q \in \{\exists, \forall\}$. Die Hypothese liefert ein ψ' in Pränex-Normalform mit $\psi' \iff \varphi'$. Setze $\psi := \exists x.\psi'$. Dann gilt offensichtlich $\varphi \iff \psi$ und ψ ist in Pränex-Normalform.
- $\varphi = \varphi_1 \vee \varphi_2$. Nach Hypothese gibt es ψ_1, ψ_2 in Pränex-Normalform, mit $\varphi_i \iff \psi_i$.

Umwandlung in Pränex-Normalform

Seien

$$\psi_1 = Q_1 x_1 \dots Q_n x_n \cdot \psi'_1 \qquad \psi_2 = Q'_1 y_1 \dots Q'_m y_m \cdot \psi'_2$$

Durch evtl. Umbenennen von gebundenen Variablen und Eliminieren von Quantoren über unbenutzten Variablen kann man erreichen, dass

- $x_i \in \text{frei}(\psi'_1) \setminus \text{frei}(\psi'_2)$ für alle $i = 1, \dots, n$,
- $y_i \in \text{frei}(\psi'_2) \setminus \text{frei}(\psi'_1)$ für alle $i = 1, \dots, m$.

Durch sukzessives Anwenden der Äquivalenzen

$$(Qx.\varphi) \vee \psi \iff Qx.(\varphi \vee \psi) \quad \text{falls } x \notin \text{frei}(\psi)$$

sieht man, dass z.B.

$$\psi_1 \vee \psi_2 \iff Q_1 x_1 \dots Q_n x_n \cdot Q'_1 y_1 \dots Q'_m y_m \cdot \psi'_1 \vee \psi'_2$$

Der Fall $\varphi = \psi_1 \wedge \psi_2$ ist analog.



Skolem-Normalform

Die obigen Normalformen beziehen sich auf echte Äquivalenz, die Skolem-Normalform jedoch “nur” auf **Erfüllbarkeitsäquivalenz**.

Def.: φ ist in **Skolem-Normalform**, falls

$$\varphi = \forall x_1 \dots \forall x_n. \psi$$

wobei ψ quantorenfrei ist.

Thm.: Zu jedem τ -Satz φ existiert eine τ' -Formel ψ in Skolem-Normalform mit $\tau' \supseteq \tau$, so dass $\varphi \equiv_{sat} \psi$.

Konstruktion der Skolem-Normalform

BEWEIS: O.B.d.A. sei φ in Pränex-Normalform. Falls kein $\exists$ im Quantorenpräfix vorkommt, dann ist φ bereits in Skolem-Normalform. Betrachte das äußerste $\exists$. Sei also

$$\varphi = \forall x_1 \dots \forall x_{i-1} . \exists x_i . \psi$$

Achtung: ψ ist nicht unbedingt quantoren-frei!

Sei f ein Funktionssymbol, welches nicht in τ vorkommt. Definiere dieses als $(i - 1)$ -stellig und

$$\varphi' := \forall x_1 \dots \forall x_{i-1} . \psi[f(x_1, \dots, x_{i-1})/x_i]$$

Nicht schwer zu sehen: φ erfüllbar gdw. φ' erfüllbar.

Dies wird solange iteriert, bis alle Existenzquantoren eliminiert sind. □

Redukte und die Skolem-Normalform

Def. Seien τ, τ' Signaturen mit $\tau \subseteq \tau'$. Seien $\mathcal{A}$ τ -Struktur und $\mathcal{B}$ τ' -Struktur. Dann ist $\mathcal{A}$ **τ -Redukt** von $\mathcal{B}$, falls ihre Universen gleich sind und die Interpretation aller Funktions- und Relationssymbole aus τ in $\mathcal{A}$ mit denen in $\mathcal{B}$ übereinstimmt.

Bsp.: $(\mathbb{N}, +, 0)$ ist $(+, 0)$ -Redukt von $(\mathbb{N}, +, \cdot, 0, 1)$.

leicht zu sehen:

Thm.: Sei φ Skolem-Normalform von einer τ -Formel ψ . Jedes τ -Redukt eines Modells von φ ist Modell von ψ .

Der Sequenzenkalkül

Wie bei der Aussagenlogik lernen wir eine Charakterisierung der logischen Schlussfolgerung kennen: den **Sequenzenkalkül für die Prädikatenlogik**.

Sequenzen sind wiederum von der Form $\Gamma \Longrightarrow \Delta$, wobei Γ als Konjunktion und Δ als Disjunktion bezeichnet wird.

Eine Sequenz ist wiederum **gültig**, falls $(\bigwedge \Gamma) \rightarrow \bigvee \Delta$ allgemeingültig ist.

Der Sequenzenkalkül für FO ist eine **Erweiterung** des Sequenzenkalküls für die Aussagenlogik. D.h. alle Axiome und Regeln dessen bleiben bestehen.

Die Frage ist insbesondere, wie mit Quantoren, Variablen und der Gleichheit umzugehen ist.

Kontraktion

Kontraktion bedeutet das Vervielfältigen von Formeln im Antezedens oder Sukzedens, wenn man von der Konklusion zur Prämisse übergeht.

$$\frac{\Gamma, \varphi, \varphi \Longrightarrow \Delta}{\Gamma, \varphi \Longrightarrow \Delta} \text{ (Kontr}_L\text{)} \qquad \frac{\Gamma \Longrightarrow \Delta, \varphi, \varphi}{\Gamma \Longrightarrow \Delta, \varphi} \text{ (Kontr}_R\text{)}$$

Da Antezedens und Sukzedens als Mengen interpretiert werden, sind diese Regel eigentlich bereits implizit vorhanden.

Sie sind außerdem deswegen offensichtlich korrekt und invertierbar.

Wir machen diese Regeln hier explizit, da es in Beweisen häufig notwendig ist, Voraussetzungen mehrfach zu benutzen, z.B. in $(\forall x. P(x) \wedge Q(x)) \rightarrow \exists y. P(y) \wedge \exists z. Q(z)$.

Regeln und Axiome für Gleichheit

$$\frac{\Gamma, t \doteq t \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta} (=L)$$

$$\frac{}{\Gamma \Longrightarrow \Delta, t \doteq t} (\text{Ref1})$$

$$\frac{\Gamma, \varphi[t/x] \Longrightarrow \Delta}{\Gamma, s \doteq t, \varphi[s/x] \Longrightarrow \Delta} (\text{Subst}_L)$$

$$\frac{\Gamma \Longrightarrow \Delta, \varphi[t/x]}{\Gamma, s \doteq t \Longrightarrow \Delta, \varphi[s/x]} (\text{Subst}_R)$$

wobei $s \doteq t$ Abkürzung für $s \doteq t$ oder $t \doteq s$ ist.

Regeln für die Quantoren

Wie **beweist** man **intuitiv** eine **existentielle** Aussage $\exists x.\varphi$? Man gibt explizit **eine Instanziierung** von x an und beweist φ für diese.

Wie **beweist** man **intuitiv** eine **universelle** Aussage $\forall x.\varphi$? Man sagt, dass x **beliebig** instanziiert ist und beweist φ dafür, ohne irgendwelche weiteren Annahmen darüber zu machen.

Im Sequenzenkalkül in Sukzedentien:

- **existentiell** quantifizierte Variablen durch **Terme** ersetzen
- **universell** quantifizierte Variablen durch **neue Konstantensymbole** ersetzen

Vorgehen in Antezedentien dann dual wegen $\neg\exists x.\varphi \iff \forall x.\neg\varphi$.

Die Regeln für Quantoren

$$\frac{\Gamma \Longrightarrow \Delta, \varphi[t/x]}{\Gamma \Longrightarrow \Delta, \exists x. \varphi} \quad (\exists_R)$$

$$\frac{\Gamma, \varphi[t/x] \Longrightarrow \Delta}{\Gamma, \forall x. \varphi \Longrightarrow \Delta} \quad (\forall_L)$$

$$\frac{\Gamma \Longrightarrow \Delta, \varphi[c/x]}{\Gamma \Longrightarrow \Delta, \forall x. \varphi} \quad (\forall_R)$$

$$\frac{\Gamma, \varphi[c/x] \Longrightarrow \Delta}{\Gamma, \exists x. \varphi \Longrightarrow \Delta} \quad (\exists_L)$$

wobei c jeweils in Γ , Δ und φ nicht vorkommt

Beispiele

Sind die folgenden Sequenzen beweisbar? Wie sehen die Beweise / Beweisversuche aus?

① $\emptyset \Longrightarrow \forall x. \forall y. \forall z. x = y \wedge y = z \rightarrow x = z$

② $P(f(c)), \forall x. f(x) = x \Longrightarrow P(f(f(c)))$

③ $\forall x. P(x) \rightarrow P(f(x)) \Longrightarrow \forall x. P(x) \rightarrow P(f(f(x)))$

④ $\Phi_{Gruppe} \Longrightarrow \forall x. i(x) \circ x = 1$

⑤ $\Phi_{Gruppe} \Longrightarrow \forall x. \forall y. x \circ y = y \circ x$

Korrektheit und Vollständigkeit

Ziel ist es wieder zu zeigen, dass der Sequenzenkalkül **korrekt** (jede beweisbare Sequenz ist gültig) und **vollständig** (jede gültige Sequenz ist beweisbar) ist.

Üblicherweise ist Korrektheit einfacher zu zeigen, insbesondere hier.

Def.: Eine Regel heißt

- **korrekt**, wenn aus der Gültigkeit aller Prämissen die Gültigkeit der Konklusion folgt,
- **invertierbar**, wenn aus der Gültigkeit der Konklusion die Gültigkeit aller Prämissen folgt. Bei den Regeln $(\exists_R)$ und $(\forall_L)$ ist dies so zu verstehen, dass es **einen Term** t gibt, der die Prämisse gültig macht.

Korrektheit der Regeln

Lemma 1: Alle Axiome sind gültig.

BEWEIS: Bei (Ref1) trivial, bei allen anderen bereits gezeigt. $\square$

Lemma 2: Alle Beweisregeln sind korrekt.

BEWEIS: Exemplarisch für $(\exists_R)$ und $(\forall_R)$.

Fall $(\exists_R)$: Angenommen die Konklusion $\Gamma \implies \Delta, \exists x.\varphi$ ist nicht gültig. Dann gibt es eine Interpretation $\mathcal{I}$, so dass $\mathcal{I} \models \gamma$ für jedes $\gamma \in \Gamma$ und $\mathcal{I} \not\models \psi$ für jedes $\psi \in \Delta \cup \{\exists x.\varphi\}$. Sei $\mathcal{I} = (\mathcal{A}, \vartheta)$ und $\mathcal{A} = (A, \tau)$. Insbesondere gibt es kein $a \in A$, so dass $\mathcal{A}, \vartheta[x \mapsto a] \models \varphi$.

Beachte: Für jeden Term t ist $\llbracket t \rrbracket_{\vartheta}^{\mathcal{A}} \in A$. Also gibt es auch keinen Term t , so dass $\mathcal{A}, \vartheta[x \mapsto \llbracket t \rrbracket_{\vartheta}^{\mathcal{A}}] \models \varphi$. Also gibt es eine Interpretation $\mathcal{I}$, die die Gültigkeit von $\Gamma \implies \Delta, \varphi[t/x]$ für jeden Term t widerlegt. Damit ist die Prämisse ebenfalls ungültig.

Korrektheit der Regeln

Fall $(\forall_R)$: Angenommen die Konklusion $\Gamma \Longrightarrow \Delta, \forall x.\varphi$ ist ungültig. Dann gibt es eine Interpretation $\mathcal{I} = (\mathcal{A}, \vartheta)$ mit $\mathcal{A} = (A, \tau)$, so dass $\mathcal{I} \models \gamma$ für alle $\gamma \in \Gamma$ und $\mathcal{I} \not\models \psi$ für alle $\psi \in \Delta \cup \{\forall x.\varphi\}$. Insbesondere gibt es dann ein $a \in A$, so dass $\mathcal{A}, \vartheta[x \mapsto a] \not\models \varphi$. Sei nun c ein neues Konstantensymbol und

- $\tau' = (\tau, c)$,
- $\mathcal{A}'$ wie $\mathcal{A}$, jedoch mit $c^{\mathcal{A}'} = a$,
- $\mathcal{I}' = (\mathcal{A}', \vartheta)$.

Dann widerlegt $\mathcal{I}'$ die Gültigkeit der Prämisse $\Gamma \Longrightarrow \Delta, \varphi[c/x]$.



Beachte: Der letzte Schritt wäre i.A. nicht richtig, falls c in Γ , Δ oder φ vorkäme.

Korrektheit des Sequenzenkalküls

Thm.: Ist $\Gamma \Longrightarrow \Delta$ beweisbar im Sequenzenkalkül, dann ist $\Gamma \Longrightarrow \Delta$ gültig.

BEWEIS: Sei ein Beweis für $\Gamma \Longrightarrow \Delta$ gegeben. Nach Lemma 1 sind alle Axiome darin gültig. Nach Lemma 2 sind dann auch alle inneren Sequenzen gültig, inklusive derjenigen an der Wurzel. $\square$

Vollständigkeit des Sequenzenkalküls

Zuerst ersetzen wir die Regeln $(\exists_R)$, $(\forall_L)$ und (Subst_L) durch

$$\frac{\Gamma \Longrightarrow \Delta, \exists x.\varphi, \varphi[t/x]}{\Gamma \Longrightarrow \Delta, \exists x.\varphi} (\exists'_R) \qquad \frac{\Gamma, \forall x.\varphi, \varphi[t/x] \Longrightarrow \Delta}{\Gamma, \forall x.\varphi \Longrightarrow \Delta} (\forall'_L)$$

$$\frac{\Gamma, s \overset{\circ}{=} t, \varphi[s/x], \varphi[t/x] \Longrightarrow \Delta}{\Gamma, s \overset{\circ}{=} t, \varphi[s/x] \Longrightarrow \Delta} (\text{Subst}'_L)$$

Diese sind im ursprünglichen Sequenzenkalkül **herleitbar** wegen (Kontr_R) und (Kontr_L) oder wegen der Interpretation von Sequenzen als Mengenpaaren. Also ist der Kalkül mit diesen Regeln weiterhin korrekt. Außerdem gilt: Wenn er mit diesen Regeln vollständig ist, dann auch mit den herkömmlichen.

Vorteil: Jetzt lässt sich aus ungültiger Sequenz **generisch** ein Beweisversuch konstruieren, aus dem eine widerlegende Interpretation gebaut werden kann.

Sequenzen von Sätzen

Lemma: Seien Γ, Δ Formelmengen mit $x \notin \text{frei}(\varphi)$ für alle $\varphi \in \Gamma \cup \Delta$.

- a) $\Gamma \Longrightarrow \Delta, \psi$ ist gültig gdw. $\Gamma \Longrightarrow \Delta, \forall x.\psi$ gültig ist.
- b) $\Gamma, \psi \Longrightarrow \Delta$ ist gültig gdw. $\Gamma, \exists x.\psi \Longrightarrow \Delta$ gültig ist.

BEWEIS: Nur (a), Teil (b) analog. Die Aussage gilt offensichtlich, falls $x \notin \text{frei}(\psi)$. Angenommen, $\Gamma \Longrightarrow \Delta, \forall x.\psi$ ist ungültig und $x \in \text{frei}(\psi)$. Dann ex. $\mathcal{I} = (\mathcal{A}, \vartheta)$ mit $\mathcal{A} = (A, \tau)$ und $\mathcal{I} \models \bigwedge \Gamma$ und $\mathcal{I} \not\models \bigvee \Delta \cup \{\forall x.\psi\}$. Insbesondere gibt es ein $a \in A$, so dass $\mathcal{A}, \vartheta[x \mapsto a] \not\models \psi$. Sei $\mathcal{I}' := (\mathcal{A}, \vartheta[x \mapsto a])$. Dann widerlegt $\mathcal{I}'$ die Gültigkeit von $\Gamma \Longrightarrow \Delta, \psi$.

Die Rückrichtung wird genauso bewiesen. □

Aufgrund u.a. dieses Lemmas können wir uns im Vollständigkeitsbeweis auf Sequenzen beschränken, die nur aus Sätzen in positiver Normalform bestehen.

Abzählbarkeit von Termen

Def.: Eine Menge M heißt **höchstens abzählbar unendlich**, wenn es eine **surjektive** Funktion $\mathbb{N} \rightarrow M$ gibt.

Intuitiv: M lässt sich als Liste $m_0, m_1, m_2, \dots$ schreiben, so dass alle Elemente von M irgendwann in dieser Liste vorkommen.

Lemma: (Termabzählung) Sei τ Signatur mit höchstens abzählbar unendlich vielen Funktionssymbolen. Die Menge aller Terme über τ ist ebenfalls höchstens abzählbar unendlich.

Def.: **Grundterm** = Term ohne Variablen

Ein generischer Beweisversuch im Sequenzenkalkül

Sei $\Gamma \Longrightarrow \Delta$ eine Sequenz von τ -Sätzen. Wir konstruieren nun einen **Beweisversuch** im Sequenzenkalkül wie folgt.

Zuerst brauchen wir einen abzählbar unendlichen Vorrat $K = (c_1, c_2, \dots)$ an **Konstantensymbolen**, die nicht in τ vorkommen.

Bem.:

- 1 Es reicht offensichtlich, dass diese nicht in $\Gamma \cup \Delta$ vorkommen.
- 2 Wenn in Δ keine universellen und in Γ keine existentiellen Quantoren vorkommen, dann wird dieser Vorrat überhaupt nicht gebraucht. (Beachte Voraussetzung der positiven Normalform!)

Im folgenden verstehen wir unter “**Grundtermen**” variablen-freie Terme über den Konstantensymbolen in τ und den neuen in K .

Ein generischer Beweisversuch im Sequenzenkalkül

Man schreibt nun alle Unterformeln von Formeln in $\Gamma \cup \Delta$ in eine Prioritäts-Queue Q nach FIFO-Art. Zudem merkt man sich zu jeder Unterformel $\exists x.\psi$ oder $\forall x.\psi$ eine **unendliche Liste** aller Grundterme. Beginnend mit $\Gamma \Longrightarrow \Delta$ macht man nun folgendes.

- ① Wende (Subst'_L) an, solange dies noch zu neuen Formeln im Antezedens führt.
- ② Sei φ die Formel mit der höchsten Priorität in $\Gamma \cup \Delta$, auf die noch eine Regel angewandt werden kann.
 - ① Dupliziere diese Formel mittels (Kontr_L) oder (Kontr_R).
 - ② Wende entsprechende Regel auf eine Kopie davon an. Ist $\varphi = \exists x.\psi \in \Delta$ oder $\varphi = \forall x.\psi \in \Gamma$, dann wähle als Term den ersten aus der entsprechenden Liste. Streiche diesen. Ist $\varphi = \exists x.\psi \in \Gamma$ oder $\varphi = \forall x.\psi \in \Delta$ dann setze vorderste Konstante in K ein. Streiche diese.
- ③ Schiebe φ an das Ende der Prioritäts-Queue.

Pfade im Beweisversuch

Lemma: (Beweisversuch) Sei $\Gamma \Longrightarrow \Delta$ Sequenz, für die nach obiger Anleitung ein Beweisversuch konstruiert wurde. Sei $S_0, S_1, \dots$ ein maximaler Pfad darin (endlich oder unendlich), so dass $S_i = \Gamma_i \Longrightarrow \Delta_i$. Dann gilt für alle i, k gilt: Falls ...

- a) $\exists x. \varphi \in \Delta_i$ bzw. $\forall x. \varphi \in \Gamma_i$, dann ex. j für jedes t mit $\varphi[t/x] \in \Delta_j$ bzw. Γ_j ,
- b) $\varphi \vee \psi \in \Delta_i$ bzw. $\varphi \wedge \psi \in \Gamma_i$, dann ex. j mit $\varphi, \psi \in \Delta_j$ bzw. Γ_j ,
- c) $\varphi \wedge \psi \in \Delta_i$, bzw. $\varphi \vee \psi \in \Gamma_i$, dann ex. j mit $\varphi \in \Delta_j$ bzw. Γ_j , oder $\psi \in \Delta_j$ bzw. Γ_j ,
- d) $\forall x. \varphi \in \Delta_i$ bzw. $\exists x. \varphi \in \Gamma_i$, dann ex. j und c mit $\varphi[c/x] \in \Delta_j$ bzw. Γ_j ,
- e) $s \doteq t \in \Gamma_i$, dann ex. j mit $s \doteq s, t \doteq s \in \Gamma_j$,
- f) $s \doteq t \in \Gamma_i, t \doteq u \in \Gamma_k$, dann ex. j mit $s \doteq u \in \Gamma_j$,
- g) $s \doteq s' \in \Gamma_i$ und $\varphi[s/x] \in \Gamma_k$, dann ex. j mit $\varphi[s'/x] \in \Gamma_j$.
- h) $i \leq k$, dann $\Gamma_i \subseteq \Gamma_k$ und $\Delta_i \subseteq \Delta_k$.
 - i) Γ_i und Δ_i enthalten nur Sätze.

BEWEIS: Übung.

Herbrand-Modelle

Sei $\Pi = S_0, S_1, \dots$ Pfad im Beweisversuch für ungültiges $\Gamma \implies \Delta$. Wir konstruieren nun ein **Herbrand-Modell** $\mathcal{H}^\Pi = (G, \tau)$ wie folgt. O.B.d.A. enthalte τ mindestens ein Konstantensymbol.

- τ besteht aus allen Relations- und Funktionssymbolen, die in Π vorkommen.
- $G = \{t \mid t \text{ Grundterm über } \tau\}$

Die Interpretation der Funktions- und Relationssymbole ist generisch:

- $f^{\mathcal{H}^\Pi}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$,
(Insbesondere $c^{\mathcal{H}^\Pi} = c$ für Konstantensymbole c und allgemein $\llbracket t \rrbracket^{\mathcal{H}^\Pi} = t$ für Grundterme t).
- $(t_1, \dots, t_n) \in R^{\mathcal{H}^\Pi}$ gdw. es ein $S_i = \Gamma_i \implies \Delta_i$ gibt, so dass $R(t_1, \dots, t_n) \in \Gamma_i$.

Faktor-Strukturen modulo einer Kongruenz

Wdh.:

- **Kongruenz** = **Äquivalenz** + **Verträglichkeit** mit Funktionen und Relationen.
- Ist $\sim$ Äquivalenzrelation, so bezeichnet $[x]_{\sim}$ die **Äquivalenzklasse** von x , d.h. $[x]_{\sim} := \{y \mid x \sim y\}$.

Def.: Sei $\mathcal{A} = (A, \tau)$ Struktur und $\sim$ **Kongruenzrelation** auf A .
Definiere den **Faktor** von $\mathcal{A}$ bzgl. $\sim$ als $\mathcal{A}/\sim = (A_{\sim}, \tau)$, wobei

- $A_{\sim} = \{[x]_{\sim} \mid x \in A\}$
- $f^{\mathcal{A}/\sim}([x_1]_{\sim}, \dots, [x_n]_{\sim}) = [f^{\mathcal{A}}(t_1, \dots, t_n)]_{\sim}$
- $([x_1]_{\sim}, \dots, [x_n]_{\sim}) \in R^{\mathcal{A}/\sim}$ gdw. $(x_1, \dots, x_n) \in R^{\mathcal{A}}$

Beachte: Die Faktorstruktur ist **wohldefiniert**. Wegen Kongruenzeigenschaft ist Definition der Funktionen und Relationen unabhängig von Vertretern der Äquivalenzklasse $[x]_{\sim}$.

Das Termmodell

Def.: Sei $\Pi = S_0, S_1, \dots$ Pfad im Beweisversuch für ungültiges $\Gamma \Longrightarrow \Delta$. Für Grundterme s und t definiere

$$s \sim t \quad \text{gdw.} \quad \text{es gibt } i \text{ mit } s \doteq t \in \Gamma_i$$

Lemma: Die Relation $\sim$ ist Kongruenzrelation auf dem Herbrand-Modell $\mathcal{H}^\Pi$.

BEWEIS: Reflexivität, Symmetrie und Transitivität folgen sofort aus dem Beweisversuchs-Lemma (e) und (f). Verträglichkeit mit den Funktions- und Relationssymbolen folgt dann aus (g). □

Im folgenden benutzen wir das **Termmodell** als Faktor des Herbrand-Modells modulo obiger Kongruenzrelation: $\mathcal{H}^\Pi / \sim$.

Eigenschaften des Termmodells

Lemma: (Antezedentien) Sei $\Pi = S_0, S_1, \dots$ Pfad aus Beweisversuch nach obiger Konstruktion und $\mathcal{H}^\Pi/\sim$ dazugehöriges Termmodell. Sei $S_i = \Gamma_i \implies \Delta_i$ und $\Gamma := \bigcup_{i \in \mathbb{N}} \Gamma_i$. Dann gilt $\mathcal{H}^\Pi/\sim \models \varphi$ für alle $\varphi \in \Gamma$.

Beachte: Nach Beweisversuchs-Lemma (i) wird keine Variablenbelegung gebraucht.

BEWEIS: Durch Induktion über den Formelaufbau.

Fall $\varphi = (t_1 \doteq t_2)$: Da $\varphi \in \Gamma$ gilt $t_1 \sim t_2$ und daher $[t_1]_\sim = [t_2]_\sim$ und somit $\mathcal{H}^\Pi/\sim \models t_1 \doteq t_2$.

Fall $\varphi = R(t_1, \dots, t_n)$: Da $\varphi \in \Gamma$ gilt $([t_1]_\sim, \dots, [t_n]_\sim) \in R^{\mathcal{H}^\Pi/\sim}$ und somit $\mathcal{H}^\Pi/\sim \models R(t_1, \dots, t_n)$.

Eigenschaften des Termmodells

Fall $\varphi = \psi_1 \wedge \psi_2$. Da $\varphi \in \Gamma$ gilt nach dem Beweisversuchslemma (b) auch $\psi_1, \psi_2 \in \Gamma$. Zweimalige Anwendung der Hypothese liefert $\mathcal{H}^\Pi/\sim \models \psi_1$ und $\mathcal{H}^\Pi/\sim \models \psi_2$, somit auch $\mathcal{H}^\Pi/\sim \models \varphi$.

Fall $\varphi = \psi_1 \vee \psi_2$ ähnlich mit Beweisversuchslemma (c).

Fall $\varphi = \forall x.\psi$. Das Beweisversuchslemma (a) liefert $\psi[t/x] \in \Gamma$ für jeden Grundterm t . Nach der Hypothese gilt $\mathcal{H}^\Pi/\sim \models \varphi[t/x]$ für jedes solche t . Also gilt auch $\mathcal{H}^\Pi/\sim \models \forall x.\psi$, da es für jedes $t \in G$ offensichtlich ein t' gibt, so dass $[t']_\sim = [t]_\sim$.

Fall $\varphi = \exists x.\psi$. Nach Beweisversuchslemma (d) gibt es c mit $\psi[c/x] \in \Gamma$. Nach der Hypothese gilt $\mathcal{H}^\Pi/\sim \models \psi[c/x]$. Da c Grundterm ist, ist $[c]_\sim \in G_\sim$. Also gilt auch $\mathcal{H}^\Pi/\sim \models \exists x.\psi$. □

Eigenschaften des Termmodells

Lemma: (Sukzedentien) Sei $\Pi = S_0, S_1, \dots$ Pfad aus Beweisversuch nach obiger Konstruktion und $\mathcal{H}^\Pi/\sim$ dazugehöriges Termmodell. Sei $S_i = \Gamma_i \implies \Delta_i$ und $\Gamma := \bigcup_{i \in \mathbb{N}} \Gamma_i$, $\Delta := \bigcup_{i \in \mathbb{N}} \Delta_i$. Falls **kein S_i Axiom** ist, dann gilt $\mathcal{H}^\Pi/\sim \not\models \varphi$ für alle $\varphi \in \Delta$.

BEWEIS: Durch Induktion über den Formelaufbau.

Fall $\varphi = (s \doteq t)$. Angenommen, es gelte $\mathcal{H}^\Pi/\sim \models s \doteq t$. Dann wäre $[s]_\sim = [t]_\sim$, bzw. $s \sim t$. Dies ist aber nur der Fall, wenn es $n \in \mathbb{N}$ und Terme $s_0, \dots, s_n$ gibt, so dass $s_0 = s$, $s_n = t$ und $(s_{i-1} \doteq s_i) \in \Gamma$ für $i = 1, \dots, n$. Nach dem Beweisversuchslemma (f) wäre dann auch $(s \doteq t) \in \Gamma$. Das widerspricht aber der Tatsache, dass Π kein Axiom enthält.

Fall $\varphi = R(t_1, \dots, t_n)$. Ähnlich wie im vorherigen Fall.

Fälle $\varphi = \psi_1 \vee \psi_2$, $\varphi = \psi_1 \wedge \psi_2$, $\varphi = \exists x.\psi$ und $\varphi = \forall x.\psi$: Wie die entsprechenden Fälle im Antezedentien-Lemma mit Beweisversuchslemma (a)–(d). □

Vollständigkeit des Sequenzenkalküls

Thm.: Ist $\Gamma \Longrightarrow \Delta$ gültig, so ist $\Gamma \Longrightarrow \Delta$ beweisbar.

BEWEIS: Angenommen, $\Gamma \Longrightarrow \Delta$ ist nicht beweisbar. Dann liefert der obige Beweisversuch einen endlichen oder unendlichen Pfad Π von Sequenzen, der kein Axiom enthält. Daraus lässt sich das **Termmodell** $\mathcal{H}^\Pi/\sim$ als Faktor des Herbrand-Modells modulo der durch $\doteq$ induzierten Kongruenzrelation generieren.

Nach dem Antezedentien-Lemma erfüllt dies **alle Formeln in Antezedentien** des Pfades, also insbesondere $\mathcal{H}^\Pi/\sim \models \bigwedge \Gamma$.

Nach dem Sukzedentien-Lemma erfüllt dies **keine Formel in einem Sukzedens** des Pfades, also insbesondere $\mathcal{H}^\Pi/\sim \not\models \bigvee \Delta$.

Damit ist dann $\Gamma \Longrightarrow \Delta$ aber nicht gültig.



Schnitt-Elimination

Zur Erinnerung:

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma, \varphi \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \text{ (Cut)}$$

Thm.: Die Regel (Cut) ist **zulässig**.

BEWEIS: Wie bereits gesehen ist (Cut) **korrekt**, d.h. im Sequenzenkalkül **mit** (Cut) lassen sich **nur gültige** Sequenzen beweisen. Der Sequenzenkalkül **ohne** (Cut) ist aber **vollständig**, d.h. darin lässt sich **jede** gültige Sequenz beweisen. Somit gibt es zu jedem Beweis mit (Cut) auch einen ohne. □

Bem.: Dies nennt man auch **semantische** Schnitt-Elimination im Gegensatz zur **syntaktischen**, die wir in der Aussagenlogik kennengelernt haben. Syntaktische gilt auch für FO auf dieselbe Art und Weise.

Der Satz von Löwenheim-Skolem

Thm.: Ist φ erfüllbar, dann gibt es eine Struktur $\mathcal{A} = (A, \tau)$, so dass $\mathcal{A} \models \varphi$ und A ist höchstens **abzählbar unendlich** groß.

BEWEIS: Sei φ erfüllbar, also $\neg\varphi$ nicht allgemeingültig. Dann ist die Sequenz $\varphi \implies \emptyset$ nicht beweisbar. Nach dem Satz über die Vollständigkeit des Sequenzenkalküls ist das induzierte Herbrandmodell modulo entsprechender Kongruenz ein Modell von φ . Dies hat aber höchstens abzählbar unendlich viele Elemente.



Bem.: Der Beweis gilt sogar für höchstens abzählbar unendliche Formelmengen Φ (und sogar für überabzählbare Signaturen).

Kor.: Es gibt keine höchstens abzählbar unendliche Formelmenge Φ , so dass $Mod(\Phi) = \{(\mathbb{R}, \tau)\}$ für beliebiges τ .

Von FO zur Aussagenlogik (und zurück)

Def.: $FO^\forall$ = Menge aller FO-Sätze der Form $\forall x_1 \dots \forall x_n. \varphi$, wobei φ **quantorenfrei**.

Def.: Sei Φ $FO^\forall$ -Menge. O.B.d.A. enthalte zugrundeliegendes τ mindestens ein Konstantensymbol. Definiere **aussagenlogische** Formelmenge

$$AL(\Phi) := \{ al(\varphi[t_1/x_1, \dots, t_n/x_n]) \mid \forall \bar{x}. \varphi \in \Phi, t_1, \dots, t_n \text{ Grundterm} \}$$

wobei

$$al(\varphi \wedge \psi) := al(\varphi) \wedge al(\psi)$$

$$al(s \doteq t) := X_{s \doteq t}$$

$$al(\varphi \vee \psi) := al(\varphi) \vee al(\psi)$$

$$al(R(t_1, \dots, t_n)) := X_{R(t_1, \dots, t_n)}$$

$$al(\neg(\varphi \wedge \psi)) := al(\neg\varphi) \vee al(\neg\psi)$$

$$al(\neg(s \doteq t)) := \neg X_{s \doteq t}$$

$$al(\neg(\varphi \vee \psi)) := al(\neg\varphi) \wedge al(\neg\psi)$$

$$al(\neg R(t_1, \dots, t_n)) := \neg X_{R(t_1, \dots, t_n)}$$

$$al(\varphi \rightarrow \psi) := al(\neg\varphi) \vee al(\psi)$$

$$al(\neg\neg\varphi) := al(\varphi)$$

$$al(\neg(\varphi \rightarrow \psi)) := al(\varphi) \wedge al(\neg\psi)$$

Beispiel

$$\mathbf{Bsp.:} \ \Phi = \{\forall x. R(c) \wedge c \doteq f(c) \wedge (R(x) \rightarrow \neg R(f(x)))\}$$

$$\begin{aligned} AL(\Phi) = \{ & X_{R(c)} \wedge X_{c \doteq f(c)} \wedge (\neg X_{R(c)} \vee \neg X_{R(f(c))}), \\ & X_{R(c)} \wedge X_{c \doteq f(c)} \wedge (\neg X_{R(f(c))} \vee \neg X_{R(f(f(c)))}), \\ & X_{R(c)} \wedge X_{c \doteq f(c)} \wedge (\neg X_{R(f(f(c)))} \vee \neg X_{R(f(f(f(c))))}), \\ & \dots \} \end{aligned}$$

Beachte: hier ist Φ nicht erfüllbar, $AL(\Phi)$ jedoch!

Ziel: Satz von Herbrand, Übertragung der Erfüllbarkeit der Aussagenlogik auf FO.

Problem in diesem Beispiel: $AL(\Phi)$ “vergisst” die Beziehung $c = f(c)$ in jedem erfüllenden (FO-)Modell.

Abschluss

Def.: Sei $AL(\Phi)$ aussagenlogische Formelmenge wie oben. Im folgenden identifizieren wir der Einfachheit halber eine atomare Formel ψ mit der entsprechenden aussagenlogischen Variablen X_ψ .

Eine Menge $AL^*(\Phi)$ heißt **Abschluss** von $AL(\Phi)$, wenn gilt:

- $AL(\Phi) \subseteq AL^*(\Phi)$.
- Für jeden Grundterm t ist $t \doteq t \in AL^*(\Phi)$.
- Ist $\varphi \wedge \psi \in AL^*(\Phi)$ so ist $\varphi, \psi \in AL^*(\Phi)$.
- Ist $\varphi \vee \psi \in AL^*(\Phi)$ so ist $\varphi \in AL^*(\Phi)$ oder $\psi \in AL^*(\Phi)$.
- Ist $\psi[t/x] \in AL^*(\Phi)$ und $t \doteq t' \in AL^*(\Phi)$, so ist auch $\psi[t'/x] \in AL^*(\Phi)$

Satz von Herbrand

Thm.: Sei Φ Menge von $\text{FO}^\forall$ -Sätzen. Dann ist Φ erfüllbar gdw. es einen Abschluss $AL^*(\Phi)$ von $AL(\Phi)$ gibt, der erfüllbar ist.

($\Rightarrow$) Angenommen, Φ ist erfüllbar. Also ex. $\mathcal{A}$ mit $\mathcal{A} \models \varphi$ für alle $\varphi \in \Phi$. Definiere nun Interpretation $\mathcal{I}$ der Variablen:

$$\begin{aligned}\mathcal{I}(s \doteq t) &= \text{tt} \quad \text{gdw.} \quad \llbracket s \rrbracket^{\mathcal{A}} = \llbracket t \rrbracket^{\mathcal{A}} \\ \mathcal{I}(R(t_1, \dots, t_n)) &= \text{tt} \quad \text{gdw.} \quad (\llbracket t_1 \rrbracket^{\mathcal{A}}, \dots, \llbracket t_n \rrbracket^{\mathcal{A}}) \in R^{\mathcal{A}}\end{aligned}$$

Man kann durch Induktion über Formelaufbau zeigen, dass $\mathcal{I} \models \varphi$ für alle $\varphi \in AL(\Phi)$. Danach kann man $AL^*(\Phi)$ konstruieren, indem man zu jeder erfüllten Disjunktion ein erfülltes Disjunkt hinzunimmt und unter Konjunkten und Substitutionen abschließt.

Die Rückrichtung erfordert ein kleines bisschen Vorarbeit.

Herbrand-Strukturen

Um aus einem aussagenlogischen Modell ein prädikatenlogisches zu bauen benutzen wir wieder Herbrand-Modelle modulo der von $\doteq$ induzierten Kongruenz.

Def.: Sei Φ Menge von $\text{FO}^\forall$ -Sätzen und $AL^*(\Phi)$ wie oben. Die **Herbrand-Struktur** (bzgl. der Funktionssymbole) von Φ ist $\mathcal{H}(\Phi) = (G, \tau)$ mit G Menge der Grundterme über τ und

$$f^{\mathcal{H}(\Phi)}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$$

für alle Funktionssymbole f .

Lemma: Sei $AL^*(\Phi)$ wie oben Abschluss von $AL(\Phi)$ und $t_1 \sim t_2$ gdw. $t_1 \doteq t_2 \in AL^*(\Phi)$. Dann ist $\sim$ **Kongruenzrelation** auf der Menge der Grundterme bzgl. aller Funktions- und Relationssymbole in $AL^*(\Phi)$.

BEWEIS: Übung.

Beweis des Satzes von Herbrand

($\Leftarrow$) Ang. es gibt erfüllbaren Abschluss $AL^*(\Phi)$. Dieser habe Modell $\mathcal{I}$. Definiere eine Erweiterung $\mathcal{H}^{\mathcal{I}}(\Phi)$ der Faktor-Herbrand-Struktur $\mathcal{H}(\Phi)/\sim$ wie folgt.

- Universum und Interpretation der Funktionssymbole ist wie in $\mathcal{H}(\Phi)/\sim$.
- Für alle Relationssymbole R gilt

$$([t_1]_{\sim}, \dots, [t_n]_{\sim}) \in R^{\mathcal{H}^{\mathcal{I}}(\Phi)} \text{ gdw. } \mathcal{I} \models R(t_1, \dots, t_n)$$

Beachte: Nach obigem Lemma ist $\sim$ Kongruenzrelation.

Sei nun $\forall \bar{x}. \varphi \in \Phi$, also $al(\varphi[\bar{t}/\bar{x}]) \in AL(\Phi) \subseteq AL^*(\Phi)$ für jedes Tupel $\bar{t}$ von Grundtermen. Durch Induktion über den Formelaufbau zeigt man nun, dass $\mathcal{H}^{\mathcal{I}}(\Phi) \models al(\varphi[\bar{t}/\bar{x}])$ gilt. Da die Elemente des Universums von $\mathcal{H}^{\mathcal{I}}$ Äquivalenzklassen von Grundtermen sind, gilt somit dann auch $\mathcal{H}^{\mathcal{I}} \models \forall \bar{x}. \varphi$. □

Skolemisierung von Formelmengen

Lemma: Sei Ψ Formelmenge. Es gibt Skolem-Normalform $sk(\psi)$ von ψ für jedes $\psi \in \Psi$, so dass Ψ erfüllbar ist, gdw. $sk(\Psi) := \{sk(\psi) \mid \psi \in \Psi\}$ erfüllbar ist.

BEWEIS: Übung.

Beachte: Es gibt auch erfüllbare Mengen, die man durch sukzessive (nicht-clever) Skolemisierung ihrer Elemente in unerfüllbare Mengen überführen kann.

Mithilfe des Satzes von Herbrand lässt sich z.B. der Kompaktheitssatz der Aussagenlogik auf FO übertragen.

Kompaktheit der Prädikatenlogik

Thm.: Sei Φ eine Menge von FO-Formeln. Φ ist **erfüllbar** gdw. **jede endliche Teilmenge** von Φ **erfüllbar** ist.

BEWEIS: “ $\Rightarrow$ ” Trivial. “ $\Leftarrow$ ” Wegen obigem Lemma können wir davon ausgehen, dass Φ Menge von $\text{FO}^\forall$ -Sätzen ist.

Sei nun Φ unerfüllbar. Nach Satz von Herbrand ist somit auch jeder Abschluss von $AL(\Phi)$ unerfüllbar. Sei $AL^*(\Phi)$ einer davon. (Beachte: Diese existieren immer.) Nach dem Kompaktheitssatz der Aussagenlogik gibt es eine endliche Teilmenge $M \subseteq_{fin} AL^*(\Phi)$, die unerfüllbar ist. Betrachte

$$\Psi_M := \{ \forall \bar{x}. \varphi \in \Phi \mid \text{es gibt Grundterme } \bar{t} \text{ mit } al(\varphi[\bar{t}/\bar{x}]) \in M \}$$

Offensichtlich ist $\Psi \subseteq_{fin} \Phi$. Bilde nun den Abschluss M^* von M , wobei alle $\bar{x}$ durch beliebige $\bar{t}$ ersetzt werden. Da $M^* \supseteq M$, ist M^* auch unerfüllbar. Mit dem Satz von Herbrand ist dann aber auch Ψ_M unerfüllbar. □

Aufsteigender Löwenheim-Skolem-Satz

Thm.: Sei φ Satz, der in einem **unendlichen** Modell erfüllt ist. Dann gibt es zu jeder Menge M eine Struktur $\mathcal{A}_M$ mit einem Universum M' , so dass $\mathcal{A}_M \models \varphi$ und $|M'| \geq |M|$.

BEWEIS: Sei M gegeben und sei $\{c_m \mid m \in M\}$ Menge von paarweise verschiedenen Konstantensymbolen, die nicht in φ auftreten. Betrachte die Formelmenge

$$\Phi := \{\varphi\} \cup \{\neg(c_n \doteq c_m) \mid n, m \in M, m \neq n\}$$

Beachte: Der Satz ist bewiesen, wenn gezeigt werden kann, dass Φ erfüllbar ist. Wegen des Kompaktheitssatzes reicht es aus zu zeigen, dass jede endliche Teilmenge erfüllbar ist. Jede Teilmenge, die φ nicht enthält, ist offensichtlich erfüllbar.

Beweis des aufst. Löwenheim-Skolem-Satzes

Betrachte also solche Teilmengen, die φ enthalten. Diese sind gegeben durch eine endliche Teilmenge $N \subseteq_{fin} M$, also als

$$\Phi_N := \{\varphi\} \cup \{\neg(c_n \doteq c_m) \mid n, m \in N, m \neq n\}$$

Nach Voraussetzung hat φ ein unendliches Modell $\mathcal{A}$. Wähle nun in diesem $|N|$ paarweise verschiedene Elemente b_m für jedes $m \in N$. Da $|N| < \infty$ ist dies möglich.

Sei $\mathcal{A}_N$ nun definiert wie $\mathcal{A}$, wobei zusätzlich die Konstante c_m durch das Element b_m interpretiert wird. Offensichtlich ist $\mathcal{A}_N$ Modell von Φ_N . Also ist jedes solche Φ_N erfüllbar und mit dem Kompaktheitssatz dann auch Φ . Sei nun $\mathcal{B}$ ein Modell von Φ . Beachte: $\mathcal{B}$ muss alle c_m , $m \in M$ verschieden interpretieren. Also hat das Universum mindestens die Kardinalität von M . □

Bijektivität und die Potenzmenge

Def.: Eine Abb. $f : A \rightarrow B$ ist

- **surjektiv**, wenn es für jedes $b \in B$ ein $a \in A$ gibt mit $b = f(a)$,
- **injektiv**, wenn für alle $a, a' \in A$ gilt: wenn $a \neq a'$, dann $f(a) \neq f(a')$,
- **bijektiv**, wenn sie surjektiv und injektiv ist.

Def.: Die **Potenzmenge** einer Menge M ist die Menge

$$2^M := \{N \mid N \subseteq M\}.$$

Bsp.: $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Isomorphie und elementare Äquivalenz

Der aufsteigende Löwenheim-Skolem-Satz liefert uns einen ersten Eindruck über die Ausdruckskraft von FO.

Def. $\mathcal{A} = (A, \tau)$ und $\mathcal{B} = (B, \tau)$ sind **isomorph**, $\mathcal{A} \simeq \mathcal{B}$, wenn es eine **bijektive** Abbildung $\iota : A \rightarrow B$ gibt, so dass für alle $a_1, \dots, a_n \in A$ und $f, R \in \tau$:

- $(a_1, \dots, a_n) \in R^{\mathcal{A}}$ gdw. $(\iota(a_1), \dots, \iota(a_n)) \in R^{\mathcal{B}}$,
- $\iota(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(\iota(a_1), \dots, \iota(a_n))$.

Def.: Zwei Strukturen $\mathcal{A}, \mathcal{B}$ sind **elementar äquivalent**, $\mathcal{A} \equiv \mathcal{B}$, wenn für alle FO-Sätze φ gilt:

$$\mathcal{A} \models \varphi \quad \text{gdw.} \quad \mathcal{B} \models \varphi$$

Sprich: Diese können durch keinen FO-Satz voneinander unterschieden werden: $Th(\{\mathcal{A}\}) = Th(\{\mathcal{B}\})$.

Isomorphie und elementare Äquivalenz

Thm.: Wenn $\mathcal{A} \simeq \mathcal{B}$, dann $\mathcal{A} \equiv \mathcal{B}$.

BEWEIS: Übung.

Die Umkehrung gilt jedoch i.A. nicht, wie wir gleich sehen werden. Das Gegenbeispiel braucht jedoch unendliche Strukturen. Im Endlichen gilt die Umkehrung sogar.

Thm.: Seien $\mathcal{A}, \mathcal{B}$ endlich. Wenn $\mathcal{A} \equiv \mathcal{B}$, dann $\mathcal{A} \simeq \mathcal{B}$.

BEWEIS: Übung.

Potenzmengen und surjektive Abbildungen

Lemma: Für eine beliebige Menge A gibt es keine surjektive Abbildung vom Typ $A \rightarrow 2^A$.

BEWEIS: Angenommen $f : A \rightarrow 2^A$ ist surjektiv. Betrachte die Menge $B \subseteq A$, definiert durch $a \in B$ gdw. $a \notin f(a)$. Behauptung: es gibt kein $a \in A$, so dass $f(a) = B$. Denn gäbe es dies, so wäre $a \in f(a)$ gdw. $a \in B$ gdw. $a \notin f(a)$. □

Kor.: Seien $\mathcal{A} = (A, \tau)$ und $\mathcal{B} = (B, \tau)$ Strukturen, so dass B mindestens so groß ist wie 2^A . Dann ist $\mathcal{A} \not\preceq \mathcal{B}$.

Nicht-Isomorphie und elementare Äquivalenz

Thm.: Für jedes $\mathcal{A}$ über einem unendlichen Universum gibt es $\mathcal{B}$, so dass $\mathcal{A} \not\equiv \mathcal{B}$, aber $\mathcal{A} \equiv \mathcal{B}$.

BEWEIS: Sei $\mathcal{A} = (A, \tau)$ unendlich und $\Phi := Th(\{\mathcal{A}\})$.

Offensichtlich ist Φ erfüllbar in einem unendlichen Modell. Sei nun $B := 2^A$. Nach dem aufsteigenden Satz von Löwenheim-Skolem hat Φ auch ein Modell $\mathcal{B}$ mit Universum mindestens so groß wie 2^A . Nach obigem Korollar gilt $\mathcal{A} \not\equiv \mathcal{B}$.

Noch zu zeigen: $\mathcal{A} \equiv \mathcal{B}$. Angenommen, dies ist nicht der Fall.

Dann gibt es FO-Satz φ , so dass genau eines von $\mathcal{A}$, $\mathcal{B}$ Modell von φ ist, die andere Struktur jedoch nicht. O.B.d.A. können wir davon ausgehen, dass $\mathcal{A} \models \varphi$ und $\mathcal{B} \not\models \varphi$ gilt. (Im anderen Fall nehmen wir eben $\neg\varphi$ als FO-Satz, der die beiden unterscheidet.) Dann ist aber $\varphi \in Th(\{\mathcal{A}\})$ und somit $\varphi \in \Phi$ und damit dann auch $\mathcal{B} \models \varphi$.



Modellerweiterungssatz ohne Gleichheit

Wenn Gleichheit nicht in den Formeln vorkommt, dann gilt sogar eine stärkere Variante des aufsteigenden Löwenheim-Skolem-Satzes.

Thm.: Sei φ Satz ohne Gleichheit und $\mathcal{A}$ Modell von φ mit Universum A . Für jedes $B \supseteq A$ gibt es eine Struktur $\mathcal{B}$ mit Universum B , so dass $\mathcal{B} \models \varphi$.

BEWEIS: Übung.

Daraus folgt z.B., dass Gleichheit **nicht definierbar** ist.

Entscheidbarkeit mittels Sequenzenkalkül?

Zur Erinnerung: Das **Erfüllbarkeitsproblem** für die **Aussagenlogik** (und damit auch das Allgemeingültigkeitsproblem) ist in exponentieller Zeit **entscheidbar**. (Naïve Aufzählung aller Interpretationen, DPLL, Resolution, Sequenzenkalkül, etc.)

Es gibt auch Sequenzenkalkül für FO. Ist damit auch das Erfüllbarkeitsproblem für FO entscheidbar? **Nein**, aber wieso?

Bei Aussagenlogik anzuwendende Regel fast kanonisch gegeben, und Prämissen immer kleiner als Konklusionen. $\rightsquigarrow$ Beweisversuch muss irgendwann terminieren.

Nicht so bei FO: Wahl der Terme in $(\exists_R)$ und $(\forall_L)$ vollkommen beliebig! Systematische und terminierende Exploration nicht möglich. Auch kein Abstieg in Größe der Sequenzen gegeben.

Unentscheidbarkeit der Prädikatenlogik

Sequenzenkalkül liefert also keinen Algorithmus, der zu jeder Eingabeformel in FO in endlicher Zeit terminiert und ausgibt, ob diese erfüllbar ist oder nicht. Theoretisch könnte es aber “bessere” bzw. andere Verfahren geben, die dies leisten. Dem ist aber beweisbar nicht so.

Thm.: Es gibt **keinen Algorithmus** für das Erfüllbarkeitsproblem der Prädikatenlogik.

Beweis eigentlich nicht allzu schwer. Hier fehlen uns aber die Voraussetzungen (formaler Begriff der Berechenbarkeit, s. Vorlesung “Formale Sprachen und Komplexität”) dafür.

Beachte: Natürlich kann es solche Algorithmen in Spezialfällen geben, z.B. für

- Fragmente von FO
- bestimmte Strukturklassen

Ein entscheidbares Fragment von FO

Thm.: Sei τ eine Signatur, in der Funktionssymbole mit Stelligkeit ≥ 1 nicht vorkommen. Es gibt einen terminierenden Algorithmus, der zu vorgelegter Formel φ über τ entscheidet, ob diese erfüllbar ist oder nicht.

BEWEIS: Übung. (Hinweis: Satz von Herbrand)

Im folgenden wollen wir noch eine Eigenschaft kennenlernen, mit deren Hilfe sich das Erfüllbarkeitsproblem für ein noch weiter eingeschränktes Fragment ebenfalls zeigen lässt.

Endliche Modelleigenschaft

Def.: Eine Logik $\mathcal{L}$ hat die **endliche Modelleigenschaft** (FMP), falls es für jede erfüllbare Formel $\varphi \in \mathcal{L}$ eine **endliche** Interpretation $\mathcal{I}$ gibt, so dass $\mathcal{I} \models \varphi$.

FMP macht Erfüllbarkeit etwas einfacher. Statt potenziell alle Interpretation zu testen müsste man nur noch alle endlichen testen, um zu entscheiden, ob geg. φ erfüllbar ist oder nicht. Davon gibt es jedoch immer noch unendlich viele.

Bsp.: FO über total geordneten Strukturen hat nicht die FMP:

$$\varphi := \neg \exists x. \forall y. x \dot{=} y \vee y < x$$

besagt, dass es kein größtes Element gibt, welches es in endlichen, total geordneten Strukturen aber immer gibt. Dennoch ist φ erfüllbar.

Kleine Modelleigenschaft

Verschärfung der FMP:

Def.: Sei $f : \mathbb{N} \rightarrow \mathbb{N}$. Eine Logik $\mathcal{L}$ hat die **kleine Modelleigenschaft bzgl. f** (f -SMP), falls jede erfüllbare Formel $\varphi \in \mathcal{L}$ eine **endliche** Interpretation $\mathcal{I}$ mit $\mathcal{I} \models \varphi$ und $|\mathcal{I}| \leq f(|\varphi|)$ hat.

$\mathcal{L}$ hat die **FMP**, falls es ein f gibt, so dass $\mathcal{L}$ die f -SMP hat.

Bem.: Als Größe einer Formel nimmt man typischerweise die Anzahl verschiedener Unterformeln oder ihre syntaktische Länge. Größe einer Interpretation ist typischerweise die Kardinalität des Universums darin.

Def.: Sei $\text{FO}_{\text{Rel}}^{\exists\forall}$ Menge aller Formeln der Form $\exists x_1 \dots \exists x_n. \forall y_1 \dots \forall y_m. \varphi$, wobei φ **quantoren-frei** und **relational**, d.h. ohne Funktionssymbole.

Thm.: $\text{FO}_{\text{Rel}}^{\exists\forall}$ hat die f -SMP, wobei $f(n) = \lceil \frac{n-1}{2} \rceil$.

Substrukturen

Def.: Seien $\mathcal{A}, \mathcal{B}$ τ -Strukturen mit Universen A , bzw. B . Dann ist $\mathcal{B}$ **Substruktur** von $\mathcal{A}$, falls gilt:

- $B \subseteq A$,
- für alle Relationssymbole $R \in \tau$:

$$R^{\mathcal{B}} = R^{\mathcal{A}} \cap \underbrace{B \times \dots \times B}_{st(R)}$$

- für alle Funktionssymbole $f \in \tau$:

$$f^{\mathcal{B}}(a_1, \dots, a_k) = f^{\mathcal{A}}(a_1, \dots, a_k) \in B \quad \text{falls } a_1, \dots, a_k \in B$$

Bsp.: $(\{0, 2, 4, \dots\}, +)$ ist Substruktur von $(\mathbb{N}, +)$,
 $(\{1, 3, 5, \dots\}, +)$ jedoch nicht.

Substrukturen und universelle Formeln

Def.: Eine Formel ist **universell**, wenn sie in positiver Normalform ist und keine existentiellen Quantoren in ihr vorkommen.

Lemma 1: Sei φ universell, $\mathcal{B} = (B, \tau)$ Substruktur von $\mathcal{A}$, β Variablenbelegung mit $\beta(x) \in B$ für alle $x \in \text{frei}(\varphi)$. Dann gilt

$$\text{wenn } \mathcal{A}, \beta \models \varphi \quad \text{dann } \mathcal{B}, \beta \models \varphi$$

BEWEIS: Durch Induktion über den Aufbau von Termen und Formeln. (Übung)

Lemma 2: Sei $\mathcal{A} = (A, \tau)$ relationale Struktur und $B \subseteq A$. Es gibt eine eindeutige Substruktur $\mathcal{B}$ von $\mathcal{A}$, deren Universum B ist.

BEWEIS: Übung.

Beweis der kleinen Modelleigenschaft für $\text{FO}_{\text{Rel}}^{\exists\forall}$

BEWEIS: Beachte, dass wir uns auf Sätze beschränken können, da $\varphi(x) \equiv_{\text{sat}} \exists x.\varphi$ und entsprechendes Eliminieren freier Variablen die Formelgröße höchstens verdoppelt und nicht aus $\text{FO}_{\text{Rel}}^{\exists\forall}$ hinausführt.

Sei $\varphi = \exists x_1 \dots \exists x_n.\varphi'$ erfüllbarer Satz mit $\varphi' = \forall y_1 \dots \forall y_m.\psi$.

Dann ex. $\mathcal{A} = (A, \tau)$, so dass $\mathcal{A} \models \varphi$. Also gibt es $a_1, \dots, a_n \in A$ so dass

$$\mathcal{A}, [x_1 \mapsto a_1, \dots, x_n \mapsto a_n] \models \varphi'$$

Sei $B := \{a_1, \dots, a_n\}$. Da φ relational is, gibt es nach Lemma 2 Substruktur $\mathcal{B}$ von $\mathcal{A}$ mit Universum B . Da φ' universell ist, gilt nach Lemma 1: $\mathcal{B} \models \varphi'$ gdw. $\mathcal{A} \models \varphi'$. Da alle a_i auch in B vorhanden sind, gilt somit auch $\mathcal{B} \models \varphi$.

Beachte: Es kann höchstens $\lceil \frac{n-1}{2} \rceil$ ex. Quantoren in Formel der Länge n geben. □

Model Checking

Das **Auswerteproblem** (oder auch **Model-Checking-Problem**) für FO ist das folgende: Gegeben eine FO-Formel φ und eine passende Interpretation $\mathcal{I}$, entscheide, ob $\mathcal{I} \models \varphi$ gilt oder nicht.

Beachte Unterschied zu Erfüllbarkeit: Hier ist Interpretation als Eingabe gegeben.

Wir betrachten das Model-Checking-Problem nur für endliche Strukturen. Für unendliche ergeben sich Fragen und Hindernisse bzgl. endlicher Repräsentationen.

Thm.: Das Model-Checking-Problem für FO lässt sich in Zeit $\mathcal{O}(m^n)$ entscheiden, wobei n = Größe der Formel, m = Größe der Struktur.

Ein Algorithmus für das Model-Checking-Problem

BEWEIS: Sei $\mathcal{I} = (\mathcal{A}, \beta)$ und $\mathcal{A} = (A, \tau)$. Folgender rekursive Algorithmus löst das Model-Checking-Problem.

```

MC( $\mathcal{A}, \beta, \varphi$ ) =
  case  $\varphi$  of
     $R(t_1, \dots, t_n)$ : return  $(\llbracket t_1 \rrbracket_\beta^{\mathcal{A}}, \dots, \llbracket t_n \rrbracket_\beta^{\mathcal{A}}) \in R^{\mathcal{A}}$ 
     $t_1 \doteq t_2$ :      return  $\llbracket t_1 \rrbracket_\beta^{\mathcal{A}} = \llbracket t_2 \rrbracket_\beta^{\mathcal{A}}$ 
     $\psi_1 \vee \psi_2$ :    return  $\text{MC}(\mathcal{A}, \beta, \psi_1) \vee \text{MC}(\mathcal{A}, \beta, \psi_2)$ 
     $\exists x. \psi$ :          for each  $a \in A$ 
                        if  $\text{MC}(\mathcal{A}, \beta[x \mapsto a], \psi) = \text{tt}$  then return tt
                        return ff
    ...

```

Laufzeitabschätzung ergibt sich daraus, dass im schlimmsten Fall in jeder Unterformel das gesamte Universum durchsucht werden muss. □

SMP und Entscheidbarkeit

Thm.: Sei $\mathcal{L}$ Logik über endlicher Signatur, so dass

- $\mathcal{L}$ die kleine Modelleigenschaft bzgl. einer Funktion f hat, und
- es einen terminierenden Algorithmus für das Model-Checking-Problem für $\mathcal{L}$ auf endlichen Strukturen gibt.

Dann gibt es auch einen terminierenden Algorithmus für das Erfüllbarkeitsproblem für $\mathcal{L}$.

BEWEIS: Folgender Algorithmus löst das Erfüllbarkeitsproblem.

SAT(φ) =

```
eliminiere freie Variablen in  $\varphi$  durch äußere, existentielle Quantifizierung  
for each  $\tau$ -Struktur  $\mathcal{A}$  mit  $|\mathcal{A}| \leq f(|\varphi|)$   
  if MC( $\mathcal{A}, [], \varphi$ ) = tt then return tt  
return ff
```

Korrektheit ergibt sich daraus, dass jedes φ , welches kein Modell der Größe $\leq f(|\varphi|)$ hat, unerfüllbar sein muss. □

Typen

In FO, so wie hier definiert, scheint ein in der Informatik wichtiges Konzept zu fehlen: **Typen**. Beachte: in Strukturen gibt es nur ein Universum A und alle Funktionen haben Typ $A^n \rightarrow A$.

Kann man z.B. auch Struktur $\mathcal{P}$ aller **Laufzeit-Java-Objekte** eines geg. Programms modellieren? (Beachte: FO-Funktion $\neq$ Java-Methoden, sondern modellieren z.B. Verzeigerung im Heap durch Instanzvariablen)

Bsp.: $x.f == y$ gdw. $f^{\mathcal{P}}(x) = y$, bei $x.f.equals(y)$
Modellierung durch Relation R_f möglich

Typen können leicht in FO durch Prädikate (1-st. Relationen) eingeführt werden

Beispiel

zu modellieren: Java-Datentyp `List<Integer>`

- Universum $U = \mathbb{N} \uplus \mathbb{N}^*$ (letzteres bezeichnet alle **Folgen** von Elementen aus $\mathbb{N}$)
- Unterscheidung zwischen Zahl und Liste: 1-st. Relationen $Nat, List$
- 2-st. Relation $R_{first} \subseteq U^2$ zeichnet 1. Listenelement aus
- Methode $get : \mathbb{N}^* \times \mathbb{N} \rightarrow \mathbb{N}$, welche i -tes Element aus Liste extrahiert, kann in FO durch Funktion $f_{get} : U \times U \rightarrow U$ modelliert werden

Verwendung immer mit **Quantorenrelativierung**

$$\forall l. List(l) \rightarrow \left(\forall i. Nat(i) \rightarrow (i > 0 \rightarrow \neg R_{first}(l, f_{get}(l, i))) \right)$$

Sequenzenkalkül in PVS

Der Sequenzenkalkül für FO ist ebenfalls im Theorembeweiser PVS eingebaut. In der Tat: Aussagenlogik darin ist lediglich Fragment von FO.

Um realistischere Beispiele zu modellieren und zu beweisen, ist FO in PVS typisiert. Keine Umwandlung der Formeln etc. nötig. Stattdessen werden Typen explizit angegeben.

wichtige Befehle:

- `inst`: zur Instanziierung ($\exists$ rechts, $\forall$ links)
- `skolem`: zur Einführung von Konstanten ($\forall$ rechts, $\exists$ links)

Ausdruckstärke

Wir haben teilweise einen Eindruck von der **Ausdruckstärke** von FO bekommen, z.B. durch die Begriffe der **elementaren Äquivalenz** und der **Definierbarkeit**.

Im folgenden wollen wir noch eine Technik kennenlernen, mit deren Hilfe man zeigen kann, dass eine Relation oder eine Klasse von Strukturen **nicht FO-definierbar** ist. Beachte: Dies ist eine **universelle** Aussage (‘‘für alle Formeln gilt, dass diese etwas bestimmtes nicht definieren’’), die i.A. schwerer zu beweisen ist als eine existentielle. Insbesondere sollte es klar sein, dass Induktion über den Formelaufbau z.B. dafür nicht geeignet ist.

Zur Vereinfachung betrachten wir nur noch **relationale Strukturen** (ohne Konstanten). Beachte: Funktionen können durch Relationen modelliert und in FO definiert werden, z.B.

$$\forall x. \forall y. \left((\exists z. R_+(x, y, z)) \wedge (\forall z. \forall z'. R_+(x, y, z) \wedge R_+(x, y, z') \rightarrow z \doteq z') \right)$$

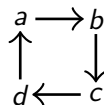
Partielle Isomorphismen

Def.: Seien $\mathcal{A} = (A, \tau)$ und $\mathcal{B} = (B, \tau)$ Strukturen. Ein **partieller Isomorphismus** ist eine partielle, **injektive** Abbildung $\kappa : A \rightarrow B$, so dass für alle R und $a_1, \dots, a_n \in \text{dom}(\kappa)$:

$$(a_1, \dots, a_n) \in R^{\mathcal{A}} \quad \text{gdw.} \quad (\kappa(a_1), \dots, \kappa(a_n)) \in R^{\mathcal{B}}$$

Bsp.: Was sind partielle Isomorphismen zwischen den folgenden Strukturen?

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3$$



Hat part. Iso. **endlichen Domain** $\text{dom}(\kappa) = \{a_1, \dots, a_n\}$, dann schreiben wir ihn auch als Liste $(a_1, \kappa(a_1)), \dots, (a_n, \kappa(a_n))$.

Ehrenfeucht-Fraïssé-Spiele für FO

Def.: Seien $\mathcal{A} = (A, \tau)$, $\mathcal{B} = (B, \tau)$ Strukturen über relationaler Signatur, mit $A \cap B = \emptyset$, $k \in \mathbb{N}$. Das **EF-Spiel** $\mathcal{G}_k^{\mathcal{A}, \mathcal{B}}$ (oder einfach nur $\mathcal{G}_k$) wird zwischen Spielern **S** (**Spoiler**) und **D** (**Duplicator**) folgendermaßen gespielt.

Eine **Partie** π besteht aus k **Runden**. In der i -ten Runde

- wählt **S** ein $a_i \in A$, und danach wählt **D** ein $b_i \in B$, oder es
- wählt **S** ein $b_i \in B$, und danach wählt **D** ein $a_i \in A$.

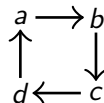
D gewinnt π , falls $(a_1, b_1), \dots, (a_k, b_k)$ partieller Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$ ist. Ansonsten gewinnt **S** die Partie π .

Beispiele

Bsp.: Wer gewinnt welche Partien auf den folgenden Strukturen?

①

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3$$



- ② jeweils $(\mathbb{N}, <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$, $(\mathbb{R}, <)$
- ③ totale Ordnungen mit n , bzw. $n + 1$ Elementen
- ④ balancierter und unbalancierter Baum

Konfigurationen

Man sieht, dass das Gewinnen einer **Partie** in $\mathcal{G}_k^{A,B}$ nicht viel über den **Zusammenhang** zwischen A und B aussagt.

Problem: Spieler können auch **schlechte** Wahl treffen im Sinne, dass sie **gewonnen hätten**, wenn sie **anders gewählt hätten**.

Wir werden “gewinnen können” durch die Existenz von **Strategien** ausdrücken.

Def.: Eine **S-Konfiguration** ist eine Liste $(a_1, b_1), \dots, (a_n, b_n) \in (A \times B)^n$ für ein $n \geq 0$. Eine **D-Konfiguration** ist ein Element aus $(A \times B)^n \times (A \cup B)$ für ein $n \geq 0$. (X -Konfiguration beschreibt eine Situation, in der Spieler X einen Zug macht.)

Strategien

Def.: Eine **Strategie** für Spieler X ist eine Funktion σ , die einer gegebenen X -Konfiguration ein Element aus $A \cup B$ zuordnet.

Sei σ Strategie für Spieler X . Eine Partie $(a_1, b_1), \dots, (a_k, b_k)$ ist **σ -konform**, falls

- $X = \mathbf{S}$ und für alle $i = 1, \dots, k - 1$:

$$\sigma((a_1, b_1), \dots, (a_i, b_i)) = a_{i+1} \quad \text{bzw.}$$

$$\sigma((a_1, b_1), \dots, (a_i, b_i)) = b_{i+1}$$

- $X = \mathbf{D}$ und für alle $i = 1, \dots, k - 1$:

$$\sigma((a_1, b_1), \dots, (a_i, b_i), a_{i+1}) = b_{i+1} \quad \text{bzw.}$$

$$\sigma((a_1, b_1), \dots, (a_i, b_i), b_{i+1}) = a_{i+1}$$

Intuitiv: Konformität bedeutet lediglich, dass man immer so wählt, wie die Strategie(funktion) es vorgibt.

Spiele gewinnen

Def.: Spieler X **gewinnt** das Spiel $\mathcal{G}_k^{\mathcal{A},\mathcal{B}}$, wenn es eine Strategie σ für Spieler X gibt, so dass X **jede σ -konforme Partie** gewinnt.

Intuitiv: Das Spiel gewinnen bedeutet, immer **gewinnen zu können**, egal wie der Gegner spielt.

Thm.: (Determiniertheit) Für alle Strukturen $\mathcal{A}, \mathcal{B}$ und $k \in \mathbb{N}$ gilt:
S gewinnt $\mathcal{G}_k^{\mathcal{A},\mathcal{B}}$ **gdw.** **D** gewinnt $\mathcal{G}_k^{\mathcal{A},\mathcal{B}}$ **nicht**.

BEWEIS: Übung.

Bem.: Richtung “ $\Rightarrow$ ” ist fast trivial, Richtung “ $\Leftarrow$ ” jedoch keineswegs: Aus Nicht-Existenz einer Gewinnstrategie muss Existenz einer Gewinnstrategie für den anderen Spieler gezeigt werden.

Monotonität in der Rundenzahl

Lemma: Seien $\mathcal{A}, \mathcal{B}$ relationale Strukturen, $k \in \mathbb{N}$.

- a) **D** gewinnt $\mathcal{G}_0^{\mathcal{A}, \mathcal{B}}$
- b) Falls **S** das Spiel $\mathcal{G}_k^{\mathcal{A}, \mathcal{B}}$ gewinnt, so auch $\mathcal{G}_{k+1}^{\mathcal{A}, \mathcal{B}}$.
- c) Falls **D** das Spiel $\mathcal{G}_{k+1}^{\mathcal{A}, \mathcal{B}}$ gewinnt, so auch $\mathcal{G}_k^{\mathcal{A}, \mathcal{B}}$.

BEWEIS: (a) $\emptyset$ ist immer ein partieller Isomorphismus.

(b) Angenommen, **S** hat eine Strategie σ für das Spiel $\mathcal{G}_k$. Wir müssen eine **S**-Strategie σ' für das Spiel $\mathcal{G}_{k+1}$ angeben und zeigen, dass er jede σ' -konforme Partie gewinnt:

$$\sigma'((a_1, b_1), \dots, (a_i, b_i)) = \begin{cases} \sigma((a_1, b_1), \dots, (a_{i-1}, b_{i-1})) & , \text{ falls } i < k \\ \sigma((a_1, b_1), \dots, (a_{k-1}, b_{k-1})) & , \text{ falls } i = k \end{cases}$$

Nach Voraussetzung ist $(a_1, b_1), \dots, (a_k, b_k)$ kein part. Iso. Also dann auch $(a_1, b_1), \dots, (a_k, b_k), (a_k, x)$ bzw.

$(a_1, b_1), \dots, (a_k, b_k), (x, b_k)$ für beliebiges x nicht.

(c) Übung.



Ziel: Ausdrucksstärke

Wir wollen zeigen, dass gewisse Klassen $\mathcal{K}$ von Strukturen nicht FO-definierbar sind, d.h. dass es keinen FO-Satz φ gibt, so dass $\text{Mod}(\varphi) = \mathcal{K}$.

Erster Ansatz: Finde $\mathcal{A}, \mathcal{B}$, so dass $\mathcal{A} \in \mathcal{K}$, $\mathcal{B} \notin \mathcal{K}$, aber $\mathcal{A} \equiv \mathcal{B}$.

Nach den Sätzen über Isomorphie und elementare Äquivalenz kann dies aber nur sein, wenn entweder

- $\mathcal{K}$ nicht unter Isomorphie abgeschlossen ist, oder
- $\mathcal{A}$ und $\mathcal{B}$ beide unendlich sind.

Frage: Kann man auch zeigen, dass **unter Isomorphie abgeschlossene Klassen endlicher Strukturen** nicht in FO definierbar sind, z.B. die Klasse aller endlichen, zusammenhängenden Graphen? Ja!

Quantorentiefe

Def.: Die **Quantorentiefe** einer Formel φ ist folgendermaßen definiert.

$$qt(s \doteq t) = qt(R(t_1, \dots, t_n)) = 0$$

$$qt(\neg\varphi) = qt(\varphi)$$

$$qt(\varphi \wedge \psi) = qt(\varphi \vee \psi) = \max\{qt(\varphi), qt(\psi)\}$$

$$qt(\exists x.\varphi) = qt(\forall x.\varphi) = 1 + qt(\varphi)$$

Def.: Seien $\mathcal{A}, \mathcal{B}$ relationale Strukturen. Wir definieren $\mathcal{A} \equiv_k \mathcal{B}$ gdw. für alle FO-Sätze φ mit $qt(\varphi) \leq k$ gilt:

$$\mathcal{A} \models \varphi \quad \text{gdw.} \quad \mathcal{B} \models \varphi$$

Soll heißen: $\mathcal{A}$ und $\mathcal{B}$ können nicht durch einen Satz mit Quantorentiefe höchstens k unterschieden werden.

Generalisierte Spiele

Def.: Seien $\mathcal{A} = (A, \tau), \mathcal{B} = (B, \tau)$ relationale Strukturen, $k \in \mathbb{N}$, $n \leq k$ und $\bar{a} = (a_1, \dots, a_n) \in A^n$, $\bar{b} = (b_1, \dots, b_n) \in B^n$. Schreibe $(\bar{a}, \bar{b})$ für $(a_1, b_1), \dots, (a_n, b_n)$.

Das **generalisierte Spiel** $\mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b})$ wird gespielt wie das Spiel $\mathcal{G}_k^{\mathcal{A}, \mathcal{B}}$, angefangen in der $(n+1)$ -ten Runde, wobei man annimmt, dass in den Runden 1 bis n bereits $(a_1, b_1), \dots, (a_n, b_n)$ gewählt wurden.

Beachte: Dies ermöglicht es uns, Beweise über Spiele **induktiv** zu führen. Z.B. lässt sich so die Existenz einer Gewinnstrategie im Spiel $\mathcal{G}_k$ nach Wahl von a, b in der 1. Runde auf die Existenz einer Gewinnstrategie in $\mathcal{G}_{k-1}(a, b)$ zurückführen.

Satz von Ehrenfeucht und Fraïssé

Thm.: Für alle Strukturen $\mathcal{A}, \mathcal{B}$ und alle $k \in \mathbb{N}$ gilt:

$$\mathbf{D} \text{ gewinnt } \mathcal{G}_k^{\mathcal{A}, \mathcal{B}} \quad \text{gdw.} \quad \mathcal{A} \equiv_k \mathcal{B}$$

Weder “ $\Rightarrow$ ” noch “ $\Leftarrow$ ” lassen sich so durch Induktion über k z.B. zeigen. Problem: freie Variablen. Lösung: **generalisierte Spiele**. Es sollte klar sein, dass folgender Satz den obigen impliziert.

Thm.: Für alle Strukturen $\mathcal{A} = (A, \tau)$, $\mathcal{B} = (B, \tau)$ und alle $k \in \mathbb{N}$, $n \leq k$, $\bar{a} \in A^n$, $\bar{b} \in B^n$ und $\bar{x} = (x_1, \dots, x_n)$ gilt:

$$\mathbf{D} \text{ gewinnt } \mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b}) \quad \text{gdw.} \quad \text{für alle } \varphi(\bar{x}) \text{ mit } qt(\varphi) \leq k - n : \\ \mathcal{A}, \bar{a} \models \varphi(\bar{x}) \text{ gdw. } \mathcal{B}, \bar{b} \models \varphi(\bar{x})$$

Beweis des Satzes von Ehrenfeucht-Fraïssé

“ $\Rightarrow$ ” Durch Kontraposition. Angenommen, es gibt $\varphi(\bar{x})$ mit $qt(\varphi) \leq k - n$, so dass nicht $\mathcal{A}, \bar{a} \models \varphi(\bar{x})$ gdw. $\mathcal{B}, \bar{b} \models \varphi(\bar{x})$. Wir konstruieren nun eine Gewinnstrategie für **S** in $\mathcal{G}_{k-n}(\bar{a}, \bar{b})$ per Induktion über $k - n$. Es sollte klar sein, dass damit **D** nicht $\mathcal{G}_{k-n}(\bar{a}, \bar{b})$ gewinnen kann.

Induktionsanfang, $k - n = 0$: Dann ist $\varphi(\bar{x})$ boolesche Kombination aus atomaren Formeln der Form $x_i \doteq x_j$ oder $R(x_{i_1}, \dots, x_{i_m})$. Nach Voraussetzung ist (o.B.d.A.) $\mathcal{A}, \bar{a} \models \varphi(\bar{x})$ und $\mathcal{B}, \bar{b} \not\models \varphi(\bar{x})$. Man vergewissert sich (z.B. durch Induktion über den Aufbau von φ), dass $(\bar{a}, \bar{b})$ kein part. Iso. zwischen $\mathcal{A}$ und $\mathcal{B}$ ist. Somit gewinnt **S** aber $\mathcal{G}_0(\bar{a}, \bar{b})$.

Beweis des Satzes von Ehrenfeucht-Fraïssé

Induktionsschritt, sei $k - n > 0$. Nach Voraussetzung gilt nicht $\mathcal{A}, \bar{a} \models \varphi(\bar{x})$ gdw. $\mathcal{B}, \bar{b} \models \varphi(\bar{x})$. Aufgrund von Variablenumbenennung, Symmetrie zwischen $\mathcal{A}$ und $\mathcal{B}$ in der Aussage, der Äquivalenz $\forall x. \psi \iff \neg \exists x. \neg \psi$ und einigen Überlegungen bzgl. der booleschen Operatoren kann man annehmen, dass $\varphi = \exists x_{n+1}. \psi(x_1, \dots, x_{n+1})$ und $\mathcal{A}, \bar{a} \models \varphi$ und $\mathcal{B}, \bar{b} \not\models \varphi$. D.h. es gibt $a \in A$, so dass

- $\mathcal{A}, (\bar{a}, a) \models \psi(x_1, \dots, x_{n+1})$ und
- für alle $b \in B$ gilt: $\mathcal{B}, (\bar{b}, b) \not\models \psi(x_1, \dots, x_{n+1})$.

Die Gewinnstrategie für **S** besteht nun daraus, zuerst in $\mathcal{A}$ das Element a zu wählen. Darauf antwortet **D** mit einem $b \in B$. Nach der Induktionshypothese gewinnt **S** das Spiel $\mathcal{G}_{k-(n+1)}((\bar{a}, a), (\bar{b}, b))$, also somit auch $\mathcal{G}_{k-n}(\bar{a}, \bar{b})$.

Isomorphietypen

Die Umkehrung verlangt wieder etwas Vorarbeit.

Def.: Sei $\mathcal{A} = (A, \tau)$ Struktur, $k \in \mathbb{N}$, $n \leq k$, $\bar{x} = (x_1, \dots, x_n)$.
Definiere für jedes $\bar{a} = (a_1, \dots, a_n) \in A^n$ eine Formel $\varphi_{k-n}^{\mathcal{A}, \bar{a}}$ wie folgt.

$$\begin{aligned} \varphi_0^{\mathcal{A}, \bar{a}}(\bar{x}) &:= \left(\bigwedge_{a_i = a_j} x_i \dot{=} x_j \right) \wedge \left(\bigwedge_{a_i \neq a_j} \neg(x_i \dot{=} x_j) \right) \wedge \\ &\quad \bigwedge_{R \in \tau} \left(\bigwedge_{(a_{i_1}, \dots, a_{i_m}) \in R^{\mathcal{A}}} R(x_{i_1}, \dots, x_{i_m}) \wedge \bigwedge_{(a_{i_1}, \dots, a_{i_m}) \notin R^{\mathcal{A}}} \neg R(x_{i_1}, \dots, x_{i_m}) \right) \\ \varphi_{k-n}^{\mathcal{A}, \bar{a}}(\bar{x}) &:= \bigwedge_{a \in A} \exists x_{n+1} \cdot \varphi_{k-n-1}^{\mathcal{A}, (\bar{a}, a)} \wedge \forall x_{n+1} \cdot \bigvee_{a \in A} \varphi_{k-n-1}^{\mathcal{A}, (\bar{a}, a)} \end{aligned}$$

Wohldefiniertheit der Isomorphietypen

Beachte: Im Grunde handelt es sich in der Definition von $\varphi_m^{\mathcal{A}, \bar{a}}$ für $m > 0$ um **unendliche** Kon- und Disjunktionen. Diese sind jedoch in Wirklichkeit **nur endlich**.

Lemma: Sei $\mathcal{A} = (A, \tau)$ und $\bar{x}$ gegeben. Für alle $n, m \geq 0$ ist die Menge

$$\{ \varphi_m^{\mathcal{A}, \bar{a}}(\bar{x}) \mid \bar{a} \in A^n \}$$

endlich.

BEWEIS: Übung.

Hinweis: Beachte, dass $\bar{a}$ selbst in $\varphi_m^{\mathcal{A}, \bar{a}}$ **nicht** vorkommt und dass $\bar{x}$ fest ist.

Isomorphietypen und EF-Spiele

Lemma: Sei $k \in \mathbb{N}$, $n \leq k$, $\mathcal{A} = (A, \tau)$, $\bar{a} \in A^n$, $\mathcal{B} = (B, \tau)$, $\bar{b} \in B^n$. Dann gilt:

$$\mathbf{D} \text{ gewinnt } \mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b}) \quad \text{gdw.} \quad \mathcal{B}, \bar{b} \models \varphi_{k-n}^{\mathcal{A}, \bar{a}}$$

BEWEIS: Per Induktion über $k - n$. Sei $k - n = 0$. Dann ist $\mathcal{B}, \bar{b} \models \varphi_0^{\mathcal{A}, \bar{a}}$ gdw.

- für alle $1 \leq i, j \leq n$: $b_i = b_j$ gdw. $a_i = a_j$, und
- für alle $1 \leq i_1, \dots, i_m \leq n$: $(b_{i_1}, \dots, b_{i_m}) \in R^{\mathcal{B}}$ gdw. $(a_{i_1}, \dots, a_{i_m}) \in R^{\mathcal{A}}$.

Dies ist der Fall gdw. $(\bar{a}, \bar{b})$ part. Iso. zwischen $\mathcal{A}$ und $\mathcal{B}$ ist, bzw. gdw. $\mathbf{D}$ das Spiel $\mathcal{G}_0^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b})$ gewinnt.

Isomorphietypen und EF-Spiele

Sei $k - n > 0$. Angenommen $\mathcal{B}, \bar{b} \models \varphi_{k-n}^{\mathcal{A}, \bar{a}}$. Dann existiert

- für jedes $a \in A$ ein $b \in B$ und
- für jedes $b \in B$ ein $a \in A$

so dass $\mathcal{B}, (\bar{b}, b) \models \varphi_{k-n-1}^{\mathcal{A}, (\bar{a}, a)}$. Eröffnet **S** nun mit $a \in A$, so kann **D** mit entsprechendem $b \in B$ und umgekehrt antworten. Nach Hypothese gewinnt **D** das Restspiel $\mathcal{G}_{k-n-1}^{\mathcal{A}, \mathcal{B}}((\bar{a}, a), (\bar{b}, b))$ und somit auch $\mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b})$.

Die Umkehrung gilt genauso.



Beweis des Satzes von Ehrenfeucht-Fraïssé

zur Erinnerung: Sind $\mathcal{A}, \bar{a}$ und $\mathcal{B}, \bar{b}$ nicht durch eine **Formel** der Quantorentiefe $\leq k - n$ zu unterscheiden, dann gewinnt **D** das Spiel $\mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b})$.

BEWEIS: Durch Kontraposition. Angenommen, **D** gewinnt $\mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{B}}(\bar{a}, \bar{b})$ **nicht**. Nach obigem Lemma gilt dann $\mathcal{B}, \bar{b} \not\models \varphi_{k-n}^{\mathcal{A}, \bar{a}}$. Man vergewissert sich leicht, dass außerdem folgendes gilt:

- $qt(\varphi_{k-n}^{\mathcal{A}, \bar{a}}) = k - n$ (einfach nachrechnen)
- $\mathcal{A}, \bar{a} \models \varphi_{k-n}^{\mathcal{A}, \bar{a}}$ (folgt z.B. aus obigem Lemma und der Tatsache, dass **D** per Copy-Cat-Strategie immer das Spiel $\mathcal{G}_{k-n}^{\mathcal{A}, \mathcal{A}}(\bar{a}, \bar{a})$ gewinnen kann)

Somit ist es nicht der Fall, dass $\mathcal{A}, \bar{a}$ und $\mathcal{B}, \bar{b}$ nicht durch Formeln der Quantorentiefe $\leq k - n$ zu unterscheiden sind. □

Nicht-Definierbarkeit von Strukturklassen

Den Satz von Ehrenfeucht-Fraïssé kann man nun folgendermaßen anwenden, um die Nicht-Definierbarkeit einer Klasse von Strukturen zu zeigen.

Thm.: Sei $\mathfrak{K}$ Klasse von Strukturen, so dass es für jedes $k \in \mathbb{N}$ Strukturen $\mathcal{A}_k, \mathcal{B}_k$ gibt mit

- $\mathcal{A}_k \in \mathfrak{K}$,
- $\mathcal{B}_k \notin \mathfrak{K}$,
- $\mathbf{D}$ gewinnt $\mathcal{G}_k^{\mathcal{A}, \mathcal{B}}$

Dann gibt es keinen FO-Satz φ mit $Mod(\varphi) = \mathfrak{K}$.

BEWEIS: Angenommen, es gibt φ mit $Mod(\varphi) = \mathfrak{K}$. Dieses hätte eine feste Quantorentiefe $qt(\varphi) = k$. Da $\mathcal{A}_k \in \mathfrak{K}$ gilt somit $\mathcal{A}_k \models \varphi$. Nach Voraussetzung gewinnt $\mathbf{D}$ das Spiel $\mathcal{G}_k^{\mathcal{A}, \mathcal{B}}$, und nach dem Satz von Ehrenfeucht-Fraïssé gilt somit $\mathcal{A}_k \equiv_k \mathcal{B}_k$ und damit dann auch $\mathcal{B}_k \models \varphi$. Somit wäre aber $\mathcal{B}_k \in \mathfrak{K} = Mod(\varphi)$, was der Voraussetzung $\mathcal{B}_k \notin \mathfrak{K}$ widerspricht. □

Zusammenhängende Graphen

Ziel: Die Klasse aller **zusammenhängender**, ungerichteter **Graphen** ist **nicht FO-definierbar**.

Da ungerichtete Graphen FO-definierbar sind, brauchen wir uns nur noch auf den Zusammenhang zu konzentrieren.

Def.: Für $k \in \mathbb{N}$ definiere:

- $\mathfrak{K}_{con} := \{ G = (V, E) \mid G \text{ ist zusammenhängender Graph} \}$
- $\mathcal{A}_k = \text{Zykel der Länge } 2^k$
- $\mathcal{B}_k = \text{zwei disjunkte Kopien von } \mathcal{A}_k$

Offensichtlich gilt für alle $k \in \mathbb{N}$: $\mathcal{A}_k \in \mathfrak{K}_{con}$ und $\mathcal{B}_k \notin \mathfrak{K}_{con}$.

Def.: $\delta(x, y) = \text{Distanz}$ von x zu y (Länge des kürzesten Weges, evtl. ∞)

Zusammenhängende Graphen

Lemma: Für alle $k \in \mathbb{N}$ gewinnt **D** das Spiel $\mathcal{G}_k^{\mathcal{A}_k, \mathcal{B}_k}$.

BEWEIS: Gewinnstrategie für **D**: Seien im i -ten Zug bereits $a_1, \dots, a_{i-1}$ und $b_1, \dots, b_{i-1}$ gewählt. Wähle nun (eines von) a_i und b_i so, dass für alle $1 \leq j, h \leq i$ gilt:

- $\delta(a_j, a_h) = \delta(b_j, b_h)$ oder
- $\delta(a_j, a_h), \delta(b_j, b_h) \geq 2^{k-i+1}$

Klar ist, dass dies in Runde 1 problemlos möglich ist.

Angenommen, bis in die i -te Runde war dies möglich. Dann wählt **S** ein Element in der $(i+1)$ -ten Runde. Sei dies ein $a_i \in \mathcal{A}_k$. (Der andere Fall ist aus Symmetriegründen ähnlich.) Sei a_j dasjenige Element in $\mathcal{A}_k$, welches bereits ausgewählt wurde und **geringste Distanz** zu a_i hat.

Zusammenhängende Graphen

Fall $\delta(a_i, a_j) \geq 2^{k-i}$. Nach Voraussetzung ist der Abstand zweier bereits ausgewählter $b, b' \in \mathcal{B}_k$ entweder mindestens $2^{k-(i-1)+1}$ oder gleich dem Abstand der entsprechenden Elemente in $\mathcal{A}_k$. So lässt sich leicht ein b_i finden, welches zu allen bereits gewählten einen Abstand von mindestens $2^{k-(i-1)+1}/2 = 2^{k-i+1}$ hat.

Fall $\delta(a_i, a_j) < 2^{k-i}$. Dann muss sich auch ein b_i finden lassen, so dass $\delta(b_i, b_j) = \delta(a_i, a_j)$ und außerdem $\delta(b_i, b_h) = \delta(a_i, a_h)$ oder $\delta(b_i, b_h), \delta(a_i, a_h) \geq 2^{k-i+1}$ für alle $h < i$.

Nach k Zügen gilt also für alle $1 \leq i, j \leq k$: $\delta(a_i, a_j) = \delta(b_i, b_j)$ oder $\delta(a_i, a_j), \delta(b_i, b_j) \geq 2$. Daraus folgt

- $a_i = a_j$ gdw. $b_i = b_j$ und
- $(a_i, a_j) \in E^{\mathcal{A}_k}$ gdw. $(b_i, b_j) \in E^{\mathcal{B}_k}$

was bedeutet, dass $(\bar{a}, \bar{b})$ part. Iso. ist.



Undefinierbarkeitsresultate

Kor.: Es gibt keinen FO-Satz φ mit $Mod(\varphi) = \mathcal{R}_{con}$.

Kor.: Es gibt keine FO-Formel $\varphi(x, y)$ über der Signatur $\tau = (E)$, welche Erreichbarkeit in Graphen definiert, also

$$G, v, w \models \varphi(x, y) \quad \text{gdw.} \quad w \text{ ist von } v \text{ aus erreichbar in } G$$

BEWEIS: Dann wäre $Mod(\forall x. \forall y. \varphi(x, y)) = \mathcal{R}_{con}$. □

Kor.: Sei R zweistellige Relation. Ihre reflexiv-transitive, bzw. transitive Hülle R^* bzw. R^+ ist nicht FO-definierbar.

BEWEIS: Angenommen, es gäbe $\varphi_{R^+}(x, y)$ mit $\mathfrak{A}, a, b \models \varphi_{R^+}(x, y)$ gdw. $(a, b) \in (R^{\mathfrak{A}})^+$. Reflexiv-transitive Hülle würde dann definiert durch $\varphi_{R^*}(x, y) = (x \doteq y) \vee \varphi_{R^+}(x, y)$. Dann würde φ_{E^*} Erreichbarkeit in Graphen definieren. □

Weitere undefinierbarkeitsresultate

Mithilfe des Satzes von Ehrenfeucht-Fraïssé lassen sich viele Klassen als nicht FO-definierbar identifizieren, z.B.

- alle Strukturen gerader Kardinalität
- alle Strukturen einer Größe n mit $n \equiv 0 \pmod k$ für festes k
- alle endlichen Strukturen
- alle balancierten Bäume (Bäume sind FO-definierbar!)
- korrekte XML-Dokumente
- korrekt verzeigte Strukturen in einem Java-Heap (z.B. Listen)
- ...

XML-Dokumente modellieren

Sei T eine **endliche** Menge von **Tag-Namen**. Wir modellieren XML-Dokumente als Strukturen über der relationalen Signatur

$$\tau_{\text{XML}} = \{<\} \cup \{Open_t, Close_t \mid t \in T\}$$

wobei $<$ 2-stellig und die anderen Relationen 1-st. sind

Wir **abstrahieren** von konkreten Inhalten und interessieren uns nur für die **Struktur** eines XML-Dokuments.

Ein XML-Dokument ist somit eine endliche Liste von öffnenden und schließenden Tags.

Beispiel

Das XML-Dokument

```
<library>
  <books>
    <book>
      <id> 17 </id>
      <title> Everything to Know About Bears </title>
      <author> Michael Scott </author>
      <year> 2009 </year>
    </book>
  </books>
  <users>
    <user>
      <name> Dwight Schrute </name>
      <possesses> 17 </possesses>
    </user>
  </users>
</library>
```

abstrahieren wir zu der 22-elementigen τ_{XML} Struktur,

- deren Elemente eine lineare Ordnung bzgl. $<$ bilden
- deren 1. Element nur das Prädikat $Open_{library}$ erfüllt,
- deren 2. Element nur das Prädikat $Open_{books}$ erfüllt,
- ...
- deren 5. Element nur das Prädikat $Close_{id}$ erfüllt,
- ...

XML-Dokumente

Def.: Die Klasse $\mathfrak{K}_{\text{XML}}$ aller gültig-(modelliert-)en XML-Dokumente ist die **kleinste Klasse** $\mathfrak{K}$, bestehend aus endlichen, linear geordneten τ_{XML} -Strukturen, für die gilt:

- Ist t Tag-Name, $n \geq 0$ und $d_1, \dots, d_n \in \mathfrak{K}$, so ist $\text{Open}_t d_1 \dots d_n \text{Close}_t \in \mathfrak{K}$.

Beachte: Somit ist $\mathfrak{K}_{\text{XML}}$ **induktiv** definiert. Induktionsanfang ($n = 0$) und -schritt ($n > 0$) sind in einem abgehandelt.

FO-Undefinierbarkeit von $\mathcal{R}_{\text{XML}}$

Thm.: Die Klasse $\mathcal{R}_{\text{XML}}$ ist nicht FO-definierbar.

BEWEIS: Sei t ein fest gewählter Tag-Name. Für jedes $k \in \mathbb{N}$ definiere Strukturen $\mathcal{A}_k, \mathcal{B}_k$ wie folgt:

- $\mathcal{A}_k = \underbrace{Open_t \dots Open_t}_{2^k \text{ mal}} \underbrace{Close_t \dots Close_t}_{2^k \text{ mal}}$
- $\mathcal{B}_k = \underbrace{Open_t \dots Open_t}_{2^k \text{ mal}} \underbrace{Close_t \dots Close_t}_{2^{k+1} \text{ mal}}$

Für alle $k \in \mathbb{N}$ gilt:

- $\mathcal{A}_k \in \mathcal{R}_{\text{XML}}$
- $\mathcal{B}_k \notin \mathcal{R}_{\text{XML}}$
- $\mathbf{D}$ gewinnt $\mathcal{G}_k^{\mathcal{A}_k, \mathcal{B}_k}$

Nach dem Satz über die Nicht-Definierbarkeit von Strukturklassen ist $\mathcal{R}_{\text{XML}}$ somit nicht FO-definierbar. □

Die Peano-Axiome

Eine historisch und in Bezug auf die Informatik wichtige Struktur ist die **Arithmetik** $\mathcal{N} := (\mathbb{N}, 0, s, +, *)$ der natürlichen Zahlen.

Dedekind entwarf **Axiome** für diese Struktur, aus denen sich dann alle wahren Aussagen über natürliche Zahlen herleiten lassen sollten (vgl. Vollständigkeit); Peano hat diese dann formalisiert

- 1 0 ist natürliche Zahl
- 2 jede natürliche Zahl hat einen **eindeutigen Nachfolger**
- 3 0 ist **nicht Nachfolger** einer natürlichen Zahl
- 4 keine zwei **verschiedenen Zahlen** haben **denselben Nachfolger**
- 5 $\mathbb{N}$ ist die **kleinste Menge**, die 0 **enthält** und unter Nachfolgern **abgeschlossen** ist

Die Peano-Axiome für Addition und Multiplikation

- ⑥ 0 ist **neutrales** Element der **Addition**
- ⑦ die **Summe** aus n und dem **Nachfolger** von m ist gleich dem **Nachfolger** der **Summe** aus n und m
- ⑧ 0 ist **absorbierend** für die **Multiplikation**
- ⑨ das **Produkt** aus n und dem **Nachfolger** von m ist gleich der **Summe** aus n und dem **Produkt** aus n und m

Formalisierung der Peano-Axiome

Sei $\tau = (0, s, +, *)$ mit 0 Konstante, s einstellig. 1. Axiom hat sich erübrigt.

- ② jede natürliche Zahl hat einen eindeutigen Nachfolger

$$\forall x. \exists y. y \doteq s(x)$$

Beachte: Eindeutigkeit durch Modellierung als Funktion bereits gegeben.

- ③ 0 ist nicht Nachfolger einer natürlichen Zahl

$$\forall x. \neg(0 \doteq s(x))$$

- ④ keine zwei verschiedenen Zahlen haben denselben Nachfolger

$$\forall x. \forall y. s(x) \doteq s(y) \rightarrow x \doteq y$$

Formalisierung der Peano-Axiome

- ⑥ 0 ist **neutrales** Element der **Addition**

$$\forall x. x \doteq x + 0$$

- ⑦ die **Summe** aus n und dem **Nachfolger** von m ist gleich dem **Nachfolger** der **Summe** aus n und m

$$\forall x. \forall y. x + s(y) \doteq s(x + y)$$

- ⑧ 0 ist **absorbierend** für die **Multiplikation**

$$\forall x. 0 \doteq x * 0$$

- ⑨ das **Produkt** aus n und dem **Nachfolger** von m ist gleich der **Summe** aus n und dem **Produkt** aus n und m

$$\forall x. \forall y. x * s(y) \doteq x + (x * y)$$

Das 5. Peano-Axiom

- 5 $\mathbb{N}$ ist die kleinste Menge, die 0 enthält und unter Nachfolgern abgeschlossen ist

Das 5. Axiom lässt sich nicht so einfach in FO formalisieren, da in ihr über **Mengen** quantifiziert wird. Zur Erinnerung: “first-order” = Quantifizierung nur über **Elemente** des Universums.

äquivalente Formulierung (in der Prädikatenlogik **zweiter** Stufe):

$$\forall P. \left(P(0) \wedge \forall x. (P(x) \rightarrow P(s(x))) \rightarrow \forall x. P(x) \right)$$

auch bekannt als **Induktionsaxiom**

kann in FO-Sätze umgewandelt werden:

Peano-Axiome $\Phi_{Peano} = \text{FO-Sätze (1)–(4),(6)–(9)} + \text{abzählbar unendlich viele Instanzen von (5) mit allen möglichen Ersetzungen von } P \text{ durch eine Formel } \psi(y)$

Die Modellklasse von Φ_{Peano}

Es sollte klar sein, dass $\mathcal{N} \in \text{Mod}(\Phi_{Peano})$. Diese Klasse enthält jedoch auch “unerwünschte” Strukturen.

Thm.: Φ_{Peano} hat ein Modell, welches **nicht isomorph** zu $\mathcal{N}$ ist.

BEWEIS: Folgt sofort aus dem aufsteigenden Satz von Löwenheim-Skolem. □

Das so erhaltene, sogenannte **Nicht-Standardmodell der Arithmetik** ist jedoch überabzählbar groß. Der folgende Satz von Skolem verstärkt diese Tatsache noch.

Thm.: Φ_{Peano} hat ein abzählbar unendlich großes Modell, welches nicht isomorph zu $\mathcal{N}$ ist.

Beweis des Satzes von Skolem

BEWEIS: Ist $n \in \mathbb{N}$, so schreiben wir $\underline{n}$ für $\underbrace{s(s(\dots s((0))))}_{n \text{ mal}}$. Sei c neues Konstantensymbol. Für $k \in \mathbb{N}$ sei $\mathcal{N}_k := (\mathbb{N}, 0, s, +, *, k)$ die Erweiterung von $\mathcal{N}$, in der die neue Konstante c durch das Element k interpretiert wird.

Betrachte die Menge

$$\Phi := \Phi_{Peano} \cup \{\neg(c \doteq \underline{n}) \mid n \in \mathbb{N}\}$$

Jede endliche Teilmenge Ψ von Φ ist erfüllbar, z.B. in $\mathcal{N}_k$, wobei $k = \min\{n \mid \neg(c \doteq \underline{n}) \notin \Psi\}$. Nach dem Kompaktheitssatz ist Φ erfüllbar. Der Satz von Löwenheim-Skolem besagt, dass es auch ein höchstens abzählbar unendliches $\mathcal{A}$ gibt, so dass $\mathcal{A} \models \Phi$.

Beweis des Satzes von Skolem

Wir zeigen zunächst, dass es kein $k \in \mathbb{N}$ gibt, so dass $\mathcal{N}_k \simeq \mathcal{A}$. Angenommen, es gäbe solch ein k und einen Isomorphismus $\kappa : \mathcal{N}_k \rightarrow \mathcal{A}$. Dann muss für alle $n \in \mathbb{N}$ gelte:

$$\kappa(n) = \kappa(\underline{n}^{\mathcal{N}}) = \underline{n}^{\mathcal{A}}$$

denn sonst wäre κ nicht verträglich mit den Funktionssymbolen 0 und s. Insbesondere gilt auch $\kappa(k) = \underline{k}^{\mathcal{A}}$. Andererseits ist $k = c^{\mathcal{N}_k}$ und somit auch $\kappa(k) = c^{\mathcal{A}}$. Dies steht aber im Widerspruch zu der Annahme, dass $\mathcal{A} \models \Phi$, denn $\neg(c \doteq \underline{k}) \in \Phi$.

Beweis des Satzes von Skolem

Nun entstehe $\mathcal{A}'$ aus $\mathcal{A}$ dadurch, dass man lediglich die Interpretation von c verwirft. Folgendes gilt:

- ① $\mathcal{A}'$ ist höchstens abzählbar unendlich groß.
- ② $\mathcal{A}' \models \Phi_{\text{Peano}}$, denn $\Phi_{\text{Peano}} \subseteq \Phi$ und $\mathcal{A}'$ unterscheidet sich von $\mathcal{A}$ lediglich in der Interpretation von c , welches in Φ_{Peano} aber nicht vorkommt.
- ③ $\mathcal{A}' \not\cong \mathcal{N}$. Angenommen, es gäbe Isomorphismus $\kappa : \mathcal{A}' \rightarrow \mathcal{N}$. Dann gibt es a , so dass $a = c^{\mathcal{A}}$, und κ wäre auch Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{N}_{\kappa(a)}$. □

Satz von Dedekind

Thm.: Jedes Modell von Φ_{Peano} zusammen mit 5. Peano-Axiom

$$\forall P. \left(P(0) \wedge \forall x. (P(x) \rightarrow P(s(x))) \rightarrow \forall x. P(x) \right)$$

(formuliert in der Prädikatenlogik zweiter Stufe) ist isomorph zu $\mathcal{N}$.

Struktur eines Nicht-Standardmodells

Sei $\mathcal{M}$ ein Nicht-Standardmodell der Arithmetik mit Universum M . Mit der kanonischen Einbettung $\kappa : \mathbb{N} \rightarrow M$ mit $\kappa(n) = (\underline{n})^{\mathcal{M}}$ lässt sich $\mathbb{N}$ als Teilmenge von M identifizieren.

Elemente aus M , die nicht im Bild der Einbettung κ liegen, heißen **nicht-standard**.

Struktur eines Nicht-Standardmodells

Doch wie sieht das Modell $\mathcal{M}$ (bzgl. der Einbettung aus)?

- ① Die Kleiner-Relation ist definierbar.
- ② Die Arithmetik beweist, dass $<$ eine linear Ordnung ist mit 0 als kleinstem Element.

Also ist z.B. $<^{\mathcal{M}}$ auch eine lineare Ordnung in M .

- ③ Für jedes $k \in \mathbb{N}$ gilt nun

$$\mathcal{M} \models \forall x. x < \underline{k} \rightarrow x \doteq \underline{0} \vee x \doteq \underline{1} \vee \dots \vee x \doteq \underline{k-1}$$

da diese Formeln in der Arithmetik beweisbar sind.

- ④ Sei a ein nicht-standard Element. Für alle $k \in \mathbb{N}$ gilt nun

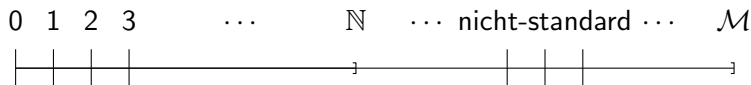
$$M, [x \mapsto a] \models \neg(x \doteq \underline{k})$$

Also muss mit obigem Punkt gelten:

$$M, [x \mapsto a] \models x > \underline{k}$$

Struktur eines Nicht-Standardmodells

Ingesamt erhalten wir folgendes Bild:



Nicht-standard Zahlen können helfen über $\mathbb{N}$ zu argumentieren:

Lemma Sei $\varphi(x)$ eine Formel und a eine nicht-standard Zahl in $\mathcal{M}$. Dann sind äquivalent:

- ① $\mathcal{M}, [x \mapsto a] \models \varphi(x)$
- ② es gibt unendliche viele $k \in \mathbb{N}$ mit $\mathbb{N} \models \varphi(\underline{k})$.

Unentscheidbarkeit der Arithmetik

Def.: $\tau_{ar} = (0, 1, <, +, *)$

Thm.: Es gibt keinen Algorithmus, der zu vorgegebenem τ_{ar} -Satz φ entscheidet, ob dieser in $\mathcal{N}$ gilt.

Wie beim Satz über die Unentscheidbarkeit von FO i.A. fehlen uns wiederum die Grundlagen, um dies zu beweisen. Das Prinzip ist aber einfach: Man kennt ein anderes Problem, für das es beweisbar keinen Algorithmus gibt. Dann zeigt man, dass sich jede Instanz dieses Problems auf einen τ_{ar} -Satz abbilden lässt. Damit hätte man aus einem Algorithmus für die Arithmetik auch einen Algorithmus für das andere Problem.

Die Goldbach-Vermutung

Gäbe es einen solchen Algorithmus, so wären einige mathematische Probleme vielleicht schon gelöst, z.B. die **Goldbach-Vermutung**.

Jede gerade Zahl größer als 2 kann als Summe zweier Primzahlen geschrieben werden.

Beachte: Dies ist eine **universelle** Aussage. Mithilfe von Computern hat man jedoch noch kein **Gegenbeispiel** unter 10^{18} gefunden.

Formalisierung:

$$2 := 1 + 1$$

$$\textit{Teilt}(x, y) := \exists z. x * z \doteq y$$

$$\textit{Gerade}(y) := \textit{Teilt}(2, y)$$

$$\textit{Prim}(y) := \neg \exists x. \neg(x \doteq 1) \wedge \neg(x \doteq y) \wedge \textit{Teilt}(x, y)$$

$$\textit{Goldbach} := \forall x. \textit{Gerade}(x) \wedge 2 < x \rightarrow$$

$$\exists y. \exists z. \textit{Prim}(y) \wedge \textit{Prim}(z) \wedge x \doteq y + z$$

Entscheidbarkeit von Fragmenten der Arithmetik

Zur Unentscheidbarkeit der Arithmetik sind sowohl Addition als auch Multiplikation nötig.

Def.: $\tau_{ar}^+ = (0, 1, <, +)$, $\tau_{ar}^* = (0, 1, <, *)$

Thm.: Es gibt jeweils einen Algorithmus, der zu vorgelegtem

- τ_{ar}^+ -Satz,
- τ_{ar}^* -Satz,

entscheidet, ob dieser in $\mathcal{N}$ erfüllt ist.

Beweis jeweils nicht trivial.

Bem.: Bei τ_{ar}^+ spricht man auch von **Presburger-Arithmetik**.

Hilberts zweites Problem

1900 stellte der damals führende Mathematiker Hilbert 23 Probleme auf, die es in den nächsten 100 Jahren in der Mathematik zu lösen galt. Das 2. Problem (wie es heute verstanden wird) fragte nach einem Beweis der **Konsistenz** der Peano-Arithmetik.

Def.: Eine Formelmenge Φ ist konsistent, wenn es keine Formel φ gibt so, dass sowohl $\Phi \models \varphi$ als auch $\Phi \models \neg\varphi$.

Allgemeines Problem mit der Lösung von Hilberts 2. Problem:
Beweis der Konsistenz müsste ja auch wiederum formalisiert sein.

Konsistenz der Peano-Arithmetik lässt sich in gewissen anderen Systemen zeigen, z.B. Zermelo-Fraenkel-Mengentheorie. Gödels 2. Unvollständigkeitssatz besagt, dass sich die Konsistenz der Peano-Arithmetik nicht in irgendeinem Beweissystem zeigen kann, dessen Regeln und Axiome selbst in irgendeiner Form in der Arithmetik formalisiert werden können.

Gödels 1. Unvollständigkeitssatz

*Jedes (in gewissem Sinne sinnvolle) konsistente
Beweissystem für die Arithmetik ist unvollständig.*

Unvollständigkeit bedeutet, dass es einen Satz φ gibt, so dass weder φ noch $\neg\varphi$ beweisbar ist.

Beachte Einschränkung auf “sinnvolle” Beweissysteme. Es gibt natürlich auch konsistente und vollständige Beweissysteme für die Arithmetik, z.B. das, welches $Th(\mathcal{N})$ als Axiome und keine Regeln enthält. Solch ein System ist aber sinnlos, weil man nicht mechanisch entscheiden kann, ob eine vorgelegte Formel Axiom in dem System ist.

Konsequenz: Versuch, natürliche Zahlen mittels Logik zu definieren, kann zu Inkonsistenz führen.

Beweisskizze

Der Beweis des 1. Unvollständigkeitssatzes zerfällt in zwei Schritte.

- 1 Arithmetisierung der Syntax
- 2 Diagonalisierung

Arithmetisierung:

- 1 Jeder **Formel** φ wird eine eindeutige Zahl $\ulcorner \varphi \urcorner$ zugeordnet (die sogenannte **Gödelnummer**), so dass $\ulcorner \varphi \urcorner$ aus φ und andererseits φ auch aus $\ulcorner \varphi \urcorner$ berechnet werden kann. Analog für **Terme**.
- 2 Jedem **Beweis** P wird genauso eine Gödelzahl $\ulcorner P \urcorner$ zugeordnet. (Beachte: Ein Beweis kann z.B. als Liste von Regelanwendungen auf gewisse Formeln gegeben sein; Listen von Zahlen sind wiederum als Zahlen kodierbar.)

Beide Abbildungen können sogar bijektiv gestaltet werden.

Arithmetisierung

Durch die “Gödelisierung” von Formeln und Beweisen wird die Frage, ob ein gegebener Beweis ein Beweis für eine gegebene Formel ist, zu einer binären **Relation auf zwei Zahlen**.

$IsProof(x, y)$ gdw. P mit $\ulcorner P \urcorner = x$ ist Beweis von φ mit $y = \ulcorner \varphi \urcorner$

Noch besser: Die **Beweisbarkeit** einer Formel wird zu einem Prädikat auf Zahlen:

$$Provable(y) := \exists x. IsProof(x, y)$$

Def.: Wir schreiben $\vdash \varphi$, falls φ in der betrachteten Theorie beweisbar ist.

Arithmetisierung

Lemma 1: Für alle ψ gilt:

- Falls $\vdash \psi$, dann $\vdash \text{Provable}(\ulcorner \psi \urcorner)$.
- Falls $\vdash \neg \psi$, dann $\vdash \neg \text{Provable}(\ulcorner \psi \urcorner)$.

Intuition: Wenn ψ beweisbar ist, so gibt es einen Beweis P . Dieser hat die Gödelnummer $\ulcorner P \urcorner$, welche die geforderte Existenz bezeugt.

Eigenschaften der Arithmetisierung

Bei geeigneter Arithmetisierung gelten folgende Eigenschaften.

Fakt: Es gibt eine Formel S , so dass für jede Formel φ , jede Variable x , jeden Term t gilt:

$$\vdash \forall y. S(\underline{\ulcorner \varphi \urcorner}, \underline{\ulcorner x \urcorner}, \underline{\ulcorner t \urcorner}, y) \leftrightarrow y \doteq \underline{\ulcorner \varphi[t/x] \urcorner}$$

D.h. Substitution ist darstellbar.

Fakt: Es gibt eine Formel T , so dass für jede Zahl $k \in \mathbb{N}$ gilt:

$$\vdash \forall y. T(\underline{k}, y) \leftrightarrow y \doteq \underline{\ulcorner k \urcorner}$$

D.h. eine Zahl kann in die Arithmetisierung ihrer Darstellung umgewandelt werden.

Fixpunktsatz

Lemma 2 (Fixpunktsatz): Für jede Formel $\varphi(x)$ gibt es einen Satz ψ , so dass $\vdash \psi \leftrightarrow \varphi(\ulcorner \psi \urcorner)$.

Beweis. Setze $\sigma(x) := \exists y. \exists z. S(x, \ulcorner x \urcorner, y, z) \wedge T(x, z) \wedge \varphi(z)$.
D.h. für alle Formeln ξ gilt:

$$\begin{aligned} \vdash & \quad \sigma(\ulcorner \xi \urcorner) \\ \leftrightarrow & \quad \exists z. S\left(x, \ulcorner x \urcorner, y, \ulcorner \ulcorner \xi \urcorner \urcorner\right) \wedge \varphi(z) \\ \leftrightarrow & \quad \varphi(\ulcorner \xi[\ulcorner \xi \urcorner/x] \urcorner) \end{aligned}$$

Im Speziellen für $\psi := \sigma(\ulcorner \sigma \urcorner)$ gilt

$$\vdash \sigma(\ulcorner \sigma \urcorner) \leftrightarrow \ulcorner \sigma[\ulcorner \sigma \urcorner/x] \urcorner$$

Ergo $\vdash \psi \leftrightarrow \varphi(\ulcorner \psi \urcorner)$.



Beweis von Gödels 1. Unvollständigkeitssatz

Betrachte die Formel $\varphi(x) := \neg \text{Provable}(x)$ (Diagonalisierung).

Nach Lemma 2 hat diese einen Fixpunkt ψ . Nun gilt:

$$\vdash \neg \psi \xRightarrow{\text{Lemma 1}} \vdash \neg \text{Provable}(\ulcorner \psi \urcorner) \xRightarrow{\text{Lemma 2}} \vdash \psi$$

und andererseits

$$\vdash \psi \xRightarrow{\text{Lemma 1}} \vdash \text{Provable}(\ulcorner \psi \urcorner) \xRightarrow{\text{Lemma 2}} \vdash \neg \psi$$

Also kann weder ψ noch $\neg \psi$ beweisbar sein, da die zugrundeliegende Theorie als konsistent angenommen wurde. □

Unabhängige Sätze

Nach dem 1. Unvollständigkeitssatz muss es also in jeder Theorie, die die Arithmetik umfasst, Sätze geben, die in dieser Theorie weder beweisbar noch widerlegbar sind.

Beispiele davon wurden gefunden:

- Das **Auswahlaxiom** in Zermelo-Fraenkel-Mengentheorie.
- Die **Kontinuums-Hypothese** (Hilberts 1. Problem) in Zermelo-Fraenkel-Mengentheorie mit Auswahlaxiom (ZFC).

Jede überabzählbare Obermenge der natürlichen Zahlen ist so mächtig wie die reellen Zahlen.

- **Kruskal's Baumsatz:**

Die homeomorphe Einbettung endlicher Bäume, die mit einer Wohl-Quasiordnung beschriftet sind, ist eine Wohl-Quasiordnung.

Ist beweisbar in ZFC aber weder beweisbar noch widerlegbar in Peano-Arithmetik.

Gödel 2. Unvollständigkeitssatz

Die Konsistenz der Peano-Arithmetik lässt sich nicht mit Methoden zeigen, die wiederum in der Peano-Arithmetik formalisierbar sind.

Dies wird im Prinzip dadurch gezeigt, dass man den Beweis des 1. Unvollständigkeitssatzes in dem entsprechenden Beweissystem selbst formuliert.