Einführung in die Logik

Jürgen Koslowski
unter Mitwirkung von Thorsten Palm
basierend auf Materialien von Roland Meyer

Theoretical Computer Science
Technische Universität Braunschweig

SS 2019

https://www.tcs.cs.tu-bs.de/teaching/Logik_SS_2019.html

Kapitel 0
Überblick

Teil 1: Aussagenlogik

Ziel ist die Formalisierung des korrekten Schließens, d.h., aus einer Menge Γ als richtig angenommener Prämissen auf korrekte Weise Schlüsse A zu ziehen, so dass diese automatisch richtig sind, wenn das für die Prämissen gilt; Schreibweise $\Gamma \models A$.

Diese Schlußregeln sollen unabhängig vom jeweiligen konkreten Inhalt der zugrundeliegenden Aussagen gültig sein.

Wir verwenden Methoden/Ergebnisse aus drei Bereichen der Mathematik.
Hinsichtlich der Syntax, d.h., dem korrekten Aufbau von Formeln:

- formale Sprachen, um von unserer natürlichen Sprache zu abstrahieren;
- Funktionale Algebra, speziell das Rekursionstheorem;

Hinsichtlich der Semantik, d.h., der Interpretation der Formeln:

- Ordnungstheorie, da die Menge $\mathbb{B} = \{0, 1\}$ der Wahrheitswerte auf natürliche Weise geordnet ist, was sich auf die Menge der aussagenlogischen Formeln überträgt.

Teil 2: Prädikatenlogik

Hier soll dann die genauere Analyse spezifischer mathematischer Strukturen ermöglicht werden, die mittels einer Signatur Σ aus formalen Funktions- und Relationssymbolen beschrieben werden können.

Syntaktisch ersetzt man die atomaren Formeln der Aussagenlogik durch Aussagen darüber, ob für eine gegeben Variablenmenge die Terme in den Σ-Funktionssymbolen formal in den Σ-Relationen zueinander stehen.

Erst dann kommen die aussagenlogischen Junktoren zum Einsatz, ergänzt durch weitere einstellige Junktoren, die aus den Variablen mit Hilfe sog. Quantoren $\forall$ (für alle) und $\exists$ (es gibt) gebildet werden, und diese Variablen binden (Stichwort: Quantifizierung).

Die Semantik spielt sich dann in Σ-Strukturen ab, d.h., Mengen mit einer Instanziierung der Funktions- und Relationssymbole aus Σ.

Teil 1
Aussagenlogik

Kapitel 1
Syntax

Das Alphabet der Logik

Das Alphabet der Aussagenlogik verwendet drei Sorten von Symbolen:

- Ein hinreichend großer (oft abzählbar unendlicher) Vorrat $\mathcal{A}$ von Aussagen-Variablen oder atomaren Formeln, um in jedem konkreten Fall von den eigentlichen Aussagen abstrahieren zu können;
- Abstraktionen der Bindewörter „und“, „oder“, „nicht“ etc. der natürlichen Sprache mittels einer endlichen Menge $\mathcal{J}$ sog. Junktoren mit Namen gemäß ihrer intendierten Semantik (s.u):

$\wedge$	für ‚und‘, „Konjunktion“	$\top$	für ‚wahr‘
$\vee$	für ‚oder‘, „Disjunktion“	$\bot$	für ‚falsch‘
$\rightarrow$	für ‚[wenn...], dann’	$\leftrightarrow$	für ‚genau dann wenn‘
$\neg$	für ‚nicht‘	...	

- Klammern $($ und $)$ zum Auflösen eventueller Mehrdeutigkeiten.

Deren (disjunkte!) Vereinigung $\mathcal{J}[\mathcal{A}]$ bildet das Alphabet der Logik.

Die formale Sprache der Logik

Definition

Die formale Sprache der Aussagenlogik ist die kleinste Menge $\mathcal{F}[\mathcal{A}]$ von Wörtern über dem Alphabet $\mathcal{J}[\mathcal{A}]$ mit folgenden Abschlußeigenschaften:

- $\mathcal{A} \cup \{\bot, \top\} \subseteq \mathcal{F}[\mathcal{A}]$;
- wenn $A \in \mathcal{F}[\mathcal{A}]$, dann $\neg A \in \mathcal{F}[\mathcal{A}]$;
- wenn $A, B \in \mathcal{F}[\mathcal{A}]$, dann $(\!(A \star B)\!) \in \mathcal{F}[\mathcal{A}]$ mit $\star \in \{\wedge, \vee, \to, \leftrightarrow\}$.

Die Elemente von $\mathcal{F}[\mathcal{A}]$ heißen Formeln; diejenigen ohne Junktor kann man auch molekular nennen (im Unterschied zu den atomaren Formeln in $\mathcal{A}$).

Dies wird in der Informatik gelegentlich auch mit Hilfe einer „Grammatik“ in Backus-Naur-Form, kurz BNF ausgedrückt:

$$F ::= p \mid \bot \mid \top \mid \neg F \mid (\!(F \star F)\!) \quad \text{für} \quad p \in \mathcal{A} \text{ und } \star \in \{\wedge, \vee, \to, \leftrightarrow\}$$

Algebra 1

Die Menge $\mathcal{J}[\mathcal{A}]^*$ aller Wörter über $\mathcal{J}[\mathcal{A}]$, d.h. die disjunkte Vereinigung

$$\mathcal{J}[\mathcal{A}]^* := \sum\{\, \mathcal{J}[\mathcal{A}]^n \,:\, n \in \mathbb{N} \,\}$$

aller Mengen von Wörtern fester Länge, ist ein Monoid bzgl. Konkatenation (assoziativ) mit dem leeren Word ε als neutralem Element.

Um Eigenschaften von Formeln zu beweisen kann man versuchen, die Struktur des Monoids $\mathcal{J}[\mathcal{A}]^*$ auszunutzen, nämlich:

Algebra-Fakt

Jede Abbildung $\mathcal{J}[\mathcal{A}] \xrightarrow{\kappa} M$ läßt sich eindeutig zu einem Monoid-Homomorphismus $\mathcal{J}[\mathcal{A}]^* \xrightarrow{\bar{\kappa}} M$ fortsetzen.

Lemma

Jede Formel hat gleich viele öffnende wie schließende Klammern.

1. Beweis

Die Menge $\mathbb{Z}$ der ganzen Zahlen ist ein Monoid bzgl. der Addition $+$ mit neutralem Element 0. Es handelt sich sogar um eine Gruppe, denn jedes Element n hat ein Inverses $-n$. Setze

$$\mathcal{J}[\mathcal{A}] \xrightarrow{\delta} \mathbb{Z} \quad , \quad x \longmapsto \begin{cases} 1 & \text{falls } x = (; \\ -1 & \text{falls } x =), \\ 0 & \text{sonst} \end{cases}$$

Dann mißt $\bar{\delta}$ die Differenz zwischen öffnenden und schließenden Klammern.

Indem man Formeln in nichtleere Wörter zerlegt und ihren Aufbau beachtet läßt sich zeigen, dass $\bar{\delta}$ alle Formeln auf 0 abbildet. □

Aber $\bar{\delta}$ bildet auch viele andere Wörter auf 0 ab, z.B. $)\neg(\wedge !?$

Strukturelle Induktion

2. Beweis, nimmt den Aufbau der Formeln gleich ernst

Die Behauptung ist korrekt für die Elemente von $\mathcal{A} \cup \{\bot, \top\}$.

Jede andere Formel $A \in \mathcal{F}[\mathcal{A}]$ ist länger und folglich durch eine der 5 Abschlußoperationen aus einfacheren Formeln entstanden. Es genügt also zu zeigen, dass diese Operationen jeweils dieselbe Anzahl von öffnenden wie schließenden Klammern zu denen hinzufügen, die bereits in den Argumenten enthalten sind. Aber das ist in allen 5 Fällen klar.

Achtung: Die Menge der Formeln trägt selber eine algebraische Struktur: einfache Formeln kombinieren sich eindeutig(!) zu komplizierteren. Daher wollen wir die Junktorenmenge $\mathcal{J}$ von nun an als Signatur betrachten, also zusammen mit einer Abbildung $\mathcal{J} \xrightarrow{\mathbf{ar}} \mathbb{N} = \{0, 1, 2, \dots\}$, und zwar

$$\mathbf{ar}(\bot) = \mathbf{ar}(\top) = 0 \ , \ \mathbf{ar}(\neg) = 1 \ ; \ \mathbf{ar}(\star) = 2 \text{ für } \star \in \{\wedge, \vee, \to, \leftrightarrow\}$$

Signaturen, Terme und Strukturen (Algebra-Fakten)

In einer Signatur $\mathcal{S} \xrightarrow{\mathbf{ar}} \mathbb{N}$ dient $f \in \mathcal{S}$ als formales Funktionssymbol.

- Über jeder Menge $\mathcal{V}$ sog. Variabler können wir rekursiv die Menge $\mathbf{Term}(\mathcal{S}, \mathcal{V})$ der syntaktischen $\mathcal{S}$-Terme bilden, in BNF etwa:

$$t ::= v \mid f\,(\!(\, t_0, \ldots, t_{\mathbf{ar}(f)-1} \,)\!) \quad \text{mit} \quad v \in \mathcal{V} \quad \text{und} \quad f \in \mathcal{J}$$

- Über jeder nichtleeren Menge X kann man andererseits $f \in \mathcal{S}$ als konkrete Funktion $X^{\mathbf{ar}(@)} \xrightarrow{I(@)} X$ der entsprechenden Stelligkeit interpretieren. I.A. gibt es viele solche Interpretationen. Ein Paar aus Trägermenge und Interpretation $\langle X, I \rangle$ heißt $\mathcal{S}$-Algebra.
- $\mathbf{Term}(\mathcal{S}, \mathcal{V})$ wird selber kanonisch zu einer $\mathcal{S}$-Algebra vermöge

$$\bar{f}(t_0, \ldots, t_{\mathbf{ar}(f)-1}) := f\,(\!(\, t_0, \ldots, t_{\mathbf{ar}(f)-1} \,)\!)$$

- Rekursionssatz[1]: Jede Abbildung $\mathcal{V} \xrightarrow{\varphi} X$ läßt sich eindeutig zu einem $\mathcal{S}$-Homomorphismus $\mathbf{Term}(\mathcal{S}, \mathcal{V}) \xrightarrow{\hat{\varphi}} \langle X, I \rangle$ fortsetzen mit

$$\hat{\varphi}\left(\bar{f}(t_0, \ldots, t_{\mathbf{ar}(f)-1})\right) = \bar{f}\left(\hat{\varphi}(t_0), \ldots, \hat{\varphi}(t_{\mathbf{ar}(f)-1})\right)$$

[1] subsumiert Algebra-Fakt von Folie 9

Logik aus algebraischer Sicht

Beobachtung

$\mathcal{F}[\mathcal{A}]$ ist isomorph zu $\mathbf{Term}(\mathcal{J},\mathcal{A})$; der Unterschied besteht in der Verwendung der Infix-Schreibweise für Formeln mit binären Junktoren $\star$, im Gegensatz zur Präfix-Schreibweise für Terme:

$$(\!(A \star B)\!) \quad \text{anstatt} \quad \star\,(\!(A, B)\!)$$

Die kanonische $\mathcal{J}$-Algebrastruktur auf $\mathcal{F}[\mathcal{A}]$ ist gegeben durch

$$\begin{aligned}
(\mathcal{F}[\mathcal{A}])^0 &\xrightarrow{\bar{\bot}} \mathcal{F}[\mathcal{A}]; & \bullet &\longmapsto \bot \\
(\mathcal{F}[\mathcal{A}])^0 &\xrightarrow{\bar{\top}} \mathcal{F}[\mathcal{A}]; & \bullet &\longmapsto \top \\
(\mathcal{F}[\mathcal{A}])^1 &\xrightarrow{\bar{\neg}} \mathcal{F}[\mathcal{A}]; & A &\longmapsto \neg A \\
(\mathcal{F}[\mathcal{A}])^2 &\xrightarrow{\bar{\star}} \mathcal{F}[\mathcal{A}]; & \langle A, B\rangle &\longmapsto (\!(A \star B)\!)
\end{aligned}$$

Wir verwenden ab jetzt $@ \in \mathcal{J}$ statt $\bar{@}$ für die kanonischen Operationen $(\mathcal{F}[\mathcal{A}])^{\mathbf{ar}(@)} \longrightarrow \mathcal{F}[\mathcal{A}]$ und ersetzen $(\!($ und $)\!)$ durch $($ bzw. $)$.

$\mathcal{J}$-Algebra

Alle wesentlichen Konstruktionen auf der $\mathcal{J}$-Algebra $\mathcal{F}[\mathcal{A}]$ werden nun mit Hilfe des Rekursionssatzes vorgenommen.

Beispiel

Länge $|A|$ = Anzahl aller $\mathcal{J}[\mathcal{A}]$-Symbole in A: Verwende

- die konstante Abbildung $\mathcal{A} \xrightarrow{1} \mathbb{N}$;
- die folgenden Interpretationen von $\mathcal{J}$ in $\mathbb{N}$:

$$\begin{aligned}
\mathbb{N}^0 &\xrightarrow{I(\bot)} \mathbb{N}; & \bullet &\longmapsto 1\\
\mathbb{N}^0 &\xrightarrow{I(\top)} \mathbb{N}; & \bullet &\longmapsto 1\\
\mathbb{N}^1 &\xrightarrow{I(\neg)} \mathbb{N}; & n &\longmapsto n+1\\
\mathbb{N}^2 &\xrightarrow{I(\star)} \mathbb{N}; & \langle n, m\rangle &\longmapsto n+m+3
\end{aligned}$$

Nun ist $\mathcal{F}[\mathcal{A}] \xrightarrow{||} \mathbb{N}$ die eindeutige Fortsetzung von $\mathcal{A} \xrightarrow{1} \mathbb{N}$ zu einem $\mathcal{J}$-Homomorphismus nach $\langle \mathbb{N}, I\rangle$.

Beispiel (nochmal Klammerdifferenz $\bar{\delta}(A)$, s.o.)

- $\mathcal{A} \xrightarrow{\delta} \mathbb{Z}$ ist konstant mit Wert 0;
- Interpretiere $\mathcal{J}$ in $\mathbb{Z}$ wie folgt:

$$\begin{aligned}
\mathbb{Z}^0 &\xrightarrow{I(\bot)} \mathbb{Z}; & \bullet &\longmapsto 0\\
\mathbb{Z}^0 &\xrightarrow{I(\top)} \mathbb{Z}; & \bullet &\longmapsto 0\\
\mathbb{Z}^1 &\xrightarrow{I(\neg)} \mathbb{Z}; & n &\longmapsto n\\
\mathbb{Z}^2 &\xrightarrow{I(\star)} \mathbb{Z}; & \langle n, m\rangle &\longmapsto n + m
\end{aligned}$$

Nun ist die eindeutige Fortsetzung $\mathcal{F}[\mathcal{A}] \xrightarrow{\bar{\delta}} \mathbb{Z}$ von $\mathcal{A} \xrightarrow{1} \mathbb{Z}$ zu einem $\mathcal{J}$-Homomorphismus nach $\langle \mathbb{Z}, I\rangle$ ebenfalls konstant mit Wert 0.

Substitution

Für Formeln $A, B \in \mathcal{F}[\mathcal{A}]$ und ein Atom $q \in \mathcal{A}$ bezeichne $A[q/B]$ die Formel, die durch simultanes Ersetzen jedes Auftretens von q in A durch B entsteht. Genauer:

Definition

$\mathcal{F}[\mathcal{A}] \xrightarrow{[p/B]} \mathcal{F}[\mathcal{A}]$ ist die durch den Rekursionssatz eindeutig bestimmte Fortsetzung der Abbildung

$$\mathcal{A} \xrightarrow{f} \mathcal{F}[\mathcal{A}], \qquad q \longmapsto \begin{cases} B & \text{falls } q = p \\ q & \text{falls } q \neq p \end{cases}$$

bzgl. der kanonischen $\mathcal{J}$-Algebra-Struktur auf $\mathcal{F}[\mathcal{A}]$.

Klammerersparnisregeln

Um Klammern einzusparen, verabreden wir folgende

Bindungskonventionen

- Junktoren niedrigerer Stelligkeit binden stärker als solche höherer Stelligkeit.
- $\wedge$ und $\vee$ binden gleich stark, aber stärker als $\rightarrow$ und $\leftrightarrow$.
- $\rightarrow$ und $\leftrightarrow$ binden gleich stark.
- binäre Junktoren assoziieren nach rechts, d.h., $A \star B \star C$ ist als $A \star (B \star C)$ zu interpretieren (anders als auf alten Folien!). Für $(A \star B) \star C$ gib es keine Vereinfachung.

Achtung: Im Rahmen der Semantik werden wir später sehen, dass die binären Operatoren $\wedge$, $\vee$ und $\leftrightarrow$ auf Formeln modulo Äquivalenz tatsächlich assoziativ sein werden; für $\rightarrow$ ist dies aber nicht der Fall!

Kapitel 2
Semantik

Der Wahrheitsbereich $\mathbb{B} = \{0, 1\}$

Als Wahrheitswerte wollen wie 1 für „wahr“ und 0 für „falsch“ verwenden.

Die Wahrheitswerte unserer atomaren Formeln sollten beliebig wählbar sein:

Definition

Eine Abbildung $\mathcal{A} \xrightarrow{\varphi} \mathbb{B}$ heißt Belegung. Ihre eindeutige Fortsetzung bzgl. der kanonischen Interpretation von $\mathcal{J}$ in $\mathbb{B}$ (wir lassen I weg)

$$\begin{array}{llll}
\mathbb{B}^0 \xrightarrow{\bot} \mathbb{B}; & \bullet \longmapsto 0 & \mathbb{B}^2 \xrightarrow{\wedge} \mathbb{B}; & \langle x, y\rangle \longmapsto \inf\{x, y\} \\
\mathbb{B}^0 \xrightarrow{\top} \mathbb{B}; & \bullet \longmapsto 1 & \mathbb{B}^2 \xrightarrow{\vee} \mathbb{B}; & \langle x, y\rangle \longmapsto \sup\{x, y\} \\
\mathbb{B}^1 \xrightarrow{\neg} \mathbb{B}; & x \longmapsto 1 - x & \mathbb{B}^2 \xrightarrow{\rightarrow} \mathbb{B}; & \langle x, y\rangle \longmapsto \chi_{\leq}\langle x, y\rangle \\
 & & \mathbb{B}^2 \xrightarrow{\leftrightarrow} \mathbb{B}; & \langle x, y\rangle \longmapsto \chi_{=}\langle x, y\rangle
\end{array}$$

bezeichnen wir mit $\mathcal{A} \xrightarrow{\hat{\varphi}} \mathbb{B}$ und nennen sie Bewertung.

χ_R steht hier für die charakteristische Funktion der Menge $R \subseteq \mathbb{B} \times \mathbb{B}$.

Wahrheitstablellen

Die kanonische Interpretation von $\mathcal{J}$ in $\mathbb{B}$ läßt sich alternativ mittels Wahrheitstabellen darstellen:

$\bot$
0

$\top$
1

	$\neg$
0	1
1	0

		$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

Beispiel (Finde $\hat{\varphi}(\neg(p \wedge q) \rightarrow r)$ falls $\varphi(p) = 1$ und $\varphi(q) = \varphi(r) = 0$)

$$\underbrace{\underbrace{\neg\underbrace{(\underbrace{p}_{1} \wedge \underbrace{q}_{0})}_{0}}_{1} \rightarrow \underbrace{r}_{0}}_{0}$$

oder in „flacher“ Notation $\underset{1}{\neg}\,(\,\underset{1}{p}\,\underset{0}{\wedge}\,\underset{0}{q}\,)\,\underset{\mathbf{0}}{\rightarrow}\,\underset{0}{r}$

Boole'sche Funktionen

Für jede Formel A kann man fragen, welche Werte $\hat{\varphi}(A)$ annimmt, wenn φ alle Belegungen durchläuft. Da A nur endlich viele Atome enthält, etwa n, erhalten wir eine Funktion $\mathbb{B}^n \xrightarrow{f_A} \mathbb{B}$, die sich tabellarisch angeben läßt:

Beispiel

p	q	r	p	$\vee$	q	$\rightarrow$	$(q$	$\leftrightarrow$	$r)$	$\wedge$	$\neg$	$(p$	$\vee$	$\neg$	$r)$
0	0	0	0			**1**		1		0	0		1	1	
0	0	1	0			**1**		0		0	1		0	0	
0	1	0	1			**0**		0		0	0		1	1	
0	1	1	1			**1**		1		1	1		0	0	
1	0	0	1			**0**		1		0	0		1	1	
1	0	1	1			**0**		0		0	0		1	0	
1	1	0	1			**0**		0		0	0		1	1	
1	1	1	1			**0**		1		0	0		1	0	

Logische Folgerung $\models$, Erfüllbar- und Allgemeingültigkeit

Definition

- A (bzw. Γ) heißt erfüllbar, wenn eine Belegung φ existiert mit $\hat{\varphi}(A) = 1$ (für jedes $A \in \Gamma$).
- Die Erfüllungsrelation ist gegeben durch $@ \subseteq \mathbb{B}^{\mathcal{A}} \times \mathcal{F}[\mathcal{A}]$. Die zugehörige ▸ Polarität induziert je einen ▸ Hüllenoperator $\models(\ )$ auf $\mathbb{B}^{\mathcal{A}}$ und $(\ )^{\models}$ auf $\mathcal{F}[\mathcal{A}]$. Schreib- bzw. Sprechweise: $\Gamma \models A$ für $A \in \Gamma^{\models}$; A folgt logisch aus Γ; die Elemente von Γ heißen Prämissen.
- A heißt allgemeingültig/Tautologie, wenn jede Belegung A erfüllt. Schreibweise: $\models A$ für $A \in \emptyset^{\models} \left(= @^{\circ}\left(\mathbb{B}^{\mathcal{A}}\right)\right)$.

Ob A erfüllbar oder allgemeingültig ist, entspricht der Existenz von Einsen, bzw. keinen Nullen, in der relevanten Spalte der Boole'schen Funktion f_A.

Beobachtung.

A ist genau dann allgemeingültig, wenn $\neg A$ nicht erfüllbar ist. □

Charakterisierung von Unerfüllbarkeit

Lemma

Folgende Bedingungen sind für eine Formelmenge Γ *äquivalent:*

(0) Γ *ist unerfüllbar.*

(1) $\Gamma \models A$ *für alle Formeln* A.

(2) $\Gamma \models \bot$.

(3) *Es gibt eine Formel* B *mit* $\Gamma \models B$ *und* $\Gamma \models \neg B$.

Beweis.

(0) $\Rightarrow$ (1): Klar, da A keine Bedingungen erfüllen muß.

(1) $\Rightarrow$ (2), (3): Trivial.

(2), (3) $\Rightarrow$ (0): Keine Belegung erfüllt $\bot$ bzw. B und $\neg B$. $\square$

Das semantische Deduktionstheorem

Prämissen lassen sich nach Bedarf zwischen externer Relation $\models$ und internem Junktor $\to$ verschieben:

Lemma

$\Gamma \cup \{B\} \models A$ *genau dann wenn* $\Gamma \models B \to A$.

Beweis.

($\Rightarrow$): Erfüllt φ die Menge Γ, folgt aus $\hat{\varphi}(B) = 1$ nach Voraussetzung $\hat{\varphi}(A) = 1$, oder es gilt $\hat{\varphi}(B) \leq \hat{\varphi}(A)$. Beides impliziert $\hat{\varphi}(B \to A) = 1$.

($\Leftarrow$): Mit $\Gamma \cup \{B\}$ erfüllt ψ auch Γ und $\{B\}$, nach Voraussetzung also $B \to A$. Aber $\hat{\psi}(B) = \hat{\psi}(B \to A) = 1$ erzwingt $\hat{\psi}(A) = 1$. □

Aufgrund der Expansivität des Hüllenoperators $(\ )^{\models}$ folgt somit

Korollar

Für alle Formeln A, B gilt: $B, B \to A \models A$.

Der Kompaktheitssatz (KPS)

Alle bisher eingeführten Begriffe sind entscheidbar, solange die Formelmengen endlich sind: dann kommen nur endlich viele Atome vor und man kann eine endliche Wahrheitstabelle aufstellen.

Der folgende zentrale Satz besagt, dass man sich im Wesentlichen auf endliche Formelmengen beschränken kann:

Definition

Γ heißt endlich erfüllbar, wenn jede endliche Teilmenge von Γ erfüllbar ist.

Satz (Kompaktheitssatz)

Γ ist genau dann erfüllbar, wenn Γ endlich erfüllbar ist.

Die Notwendigkeit ist trivial, ebenso die Hinlänglichkeit, falls $\mathcal{A}$ endlich ist (Kontraposition). Vor dem Beweis der Hinlänglichkeit für unendliches $\mathcal{A}$ betrachten wir erst eine „Anwendung“ und einige Konsequenzen des KPS.

Ein Matching-Problem

Beispiel

Für eine Funktion $M \xrightarrow{T} P_f(F)$ ist eine injektive Auswahlfunktion gesucht, d.h., $M \xrightarrow{e} F$ mit $e(m) \in T(m)$ für alle $m \in M$.

Aufgrund des KPS garantiert die Lösbarkeit für endliche Mengen M die Lösbarkeit auch für unendliches M.

Als Atome verwenden wir Symbole $p_{m,f}$, $\langle m, f \rangle \in M \times F$.

Γ besteht aus drei Komponenten, die verschiedene Aspekt der Problemstellung umsetzen ($m, m' \in M$, $f, f' \in F$):

- Auswahleigenschaft: $H_m := \bigvee_{f \in T(m)} p_{m,f}$
- Funktionalität: $I_{m;f,f'} := p_{m,f} \to \neg p_{m,f'}$ mit $f \neq f'$;
- Injektivität: $J_{f;m,m'} := p_{m,f} \to \neg p_{m',f}$ mit $m \neq m'$.

Beispiel (Fortsetzung)

Die Existenz einer Γ erfüllenden Belegung folgt nach KPS aus der Erfüllbarkeit jeder endlichen Teilmenge.

Für endliches $\Gamma_0 \subseteq \Gamma$ setze

$$M_* := \{\, m \in M \,:\, m \text{ tritt als Index in einer Formel von } \Gamma_0 \text{ auf } \}$$

Es gibt vier Möglichkeiten, wie $m \in M_*$ zustande kommen kann, via H_m, via $I_{m;f,f'}$, via $J_{f;m,m'}$ und via $J_{f;m',m}$.

M_* als endliche Menge erlaubt eine Lösung des Matching-Problems: Einschränkung der Konstruktion von Γ auf $m \in M_*$ liefert eine endliche Formelmenge Γ_*. Und jede Γ_* erfüllende Belegung erfüllt auch $\Gamma_0 \subseteq \Gamma_*$.

Varianten des Kompaktheitssatzes

Korollar (wird auch oft als KPS bezeichnet).

$\Gamma \models A$ genau dann wenn $\Gamma_0 \models A$ für eine endliche Teilmenge $\Gamma_0 \subseteq \Gamma$.

Beweis.

$\Gamma \models A$ gdw. $\Gamma \cup \{\neg A\}$ unerfüllbar

gdw. $\Gamma \cup \{\neg A\}$ hat eine endliche unerfüllbare Teilmenge Γ_1

gdw. Γ hat eine endliche Teilmenge Γ_0 mit $\Gamma_0 \cup \{\neg A\}$ unerfüllbar

gdw. $\Gamma_0 \models A$ für eine endliche Teilmenge $\Gamma_0 \subseteq \Gamma$ $\square$

Korollar (KPS für $\neg\Gamma$).

Für eine Formelmenge Γ sind folgende Aussagen äquivalent:

(a) Jede Belegung erfüllt mindestens eine Formel $B \in \Gamma$.

(b) Es gibt $B_i \in \Gamma$, $i < n$, so dass $B_0 \vee \cdots \vee B_{n-1}$ allgemeingültig ist.

Zum KPS-Beweis

Lemma

Für jede Formelmenge Γ *und jede Formel* A *gilt: ist* Γ *endlich erfüllbar, so auch* $\Gamma \cup \{A\}$ *oder* $\Gamma \cup \{\neg A\}$ *.*

Beweis.

Nach Voraussetzung enthält jede unerfüllbare endliche Teilmenge von $\Gamma \cup \{A\}$ bzw. $\Gamma \cup \{\neg A\}$ die Formel A bzw. $\neg A$.

Annahme: $\Gamma \cup \{A\}$ nicht endlich erfüllbar, also $\Gamma_0 \cup \{A\}$ nicht erfüllbar für eine endliche Teilmenge $\Gamma_0 \subseteq \Gamma$.

zu zeigen: $\Gamma \cup \{\neg A\}$ ist endlich erfüllbar. Betrachte $\Gamma_1 \subseteq \Gamma$ endlich. Nach Voraussetzung hat $\Gamma_0 \cup \Gamma_1$ eine erfüllende Belegung φ . Aufgrund der Annahme gilt nun $\hat{\varphi}(\neg A) = 1$. □

Jede Belegung φ erfüllt „die Hälfte“ aller Formeln, nämlich immer genau eine der Formeln A und $\neg A$. Die tatsächlich erfüllte Formel bezeichnen wir mit ${}^{\varphi}A$. Entsprechend schreiben wir ${}^{\varphi}\Gamma = \{ {}^{\varphi}A : A \in \Gamma \}$ für die von φ erfüllten Varianten der Formeln einer Menge Γ. Beachte: $|{}^{\varphi}\Gamma| = |\Gamma|$.

Definition

Unter einem Literal versteht man eine Formel aus $\mathcal{A} \cup \neg\mathcal{A}$.

Beobachtung

Für jede Belegung φ ist ${}^{\varphi}\mathcal{A}$ eine maximale erfüllbare Literalmenge, denn jedes Atom p oder seine Negation gehört zu ${}^{\varphi}\mathcal{A}$, aber nicht beide.

Umgekehrt bestimmt jede maximale erfüllbare Litreralmenge $\mathcal{L}$ genau eine sie erfüllende Belegung $\varphi_{\mathcal{L}}$:

$$\varphi_{\mathcal{L}}(p) = \begin{cases} 1 & \text{falls } p \in \mathcal{L} \\ 0 & \text{falls } \neg p \in \mathcal{L} \end{cases}$$

Beweis (KPS, Hinlänglichkeit).

$\mathcal{A}$ sei abzählbar[a] unendlich und Γ endlich erfüllbar.

Ziel: Finde eine maximale erfüllbare Literalmenge $\mathcal{L}_*$, so dass $\Gamma \cup \mathcal{L}_*$ endlich erfüllbar ist, denn die zugehörige Belegung φ_* erfüllt dann auch Γ:

Ist $\mathcal{A}_B$ die endliche Atom-Menge von $B \in \Gamma$, so hat $\{B\} \cup {}^{\varphi_*}\mathcal{A}_B \subseteq \Gamma \cup \mathcal{L}_*$ eine erfüllende Belegung φ_B, und diese stimmt auf $\mathcal{A}_B$ mit φ_* überein, folglich auch auf B, also gilt $\hat{\varphi}_*(B) = 1$.

Konstruktion von $\mathcal{L}_*$: Für eine Aufzählung p_i, $i \in \mathbb{N}$, von $\mathcal{A}$ setze

$$\mathcal{L}_0 = \emptyset \quad , \quad \mathcal{L}_{n+1} = \begin{cases} \mathcal{L}_n \cup \{p_n\} & \text{falls } \Gamma \cup \mathcal{L}_n \cup \{p_n\} \text{ endlich erfüllbar} \\ \mathcal{L} \cup \{\neg p_n\} & \text{sonst} \end{cases}$$

Wegen des Lemmas ist jede der Mengen $\Gamma \cup \mathcal{L}_n$ endlich erfüllbar. Dasselbe gilt für $\mathcal{L}_* = \bigcup\{ \mathcal{L}_n : n \in \mathbb{N} \}$, da jede endliche Teilmenge bereits in einem $\mathcal{L}_k$ und das Atom p_n in $\mathcal{L}_{n+1}$ enthalten ist. □

[a] Im überabzählbaren Fall braucht man eine transfinite Konstruktion für $\mathcal{L}_*$.

Die kanonische Ordnung und Äquivalenz auf $\mathcal{F}[\mathcal{A}]$

Lemma

Eine kanonische Quasi-Ordnung $B \sqsubseteq A$ *auf* $\mathcal{F}[\mathcal{A}]$ *wird durch*

$$\begin{aligned} \{B\} \models A \quad & \textit{gdw.} \quad \hat{\varphi}(B) = 1 \quad \textit{impliziert} \quad \hat{\varphi}(A) = 1 \quad \textit{für alle} \quad \varphi \in \mathbb{B}^{\mathcal{A}} \\ & \textit{gdw.} \quad \hat{\varphi}(B) \leq \hat{\varphi}(A) \quad \textit{für alle} \quad \varphi \in \mathbb{B}^{\mathcal{A}} \\ & \textit{gdw.} \quad \hat{\varphi}(B \to A) = 1 \quad \textit{für alle} \quad \varphi \in \mathbb{B}^{\mathcal{A}} \end{aligned}$$

definiert. Wir betrachten sie als Externalisierung des Junktors $\to$. □

Definition

$\models\!\!\!=$ sei die von $\sqsubseteq$ induzierte ÄR, die Externalisierung des Junktors $\leftrightarrow$.

Die kanonische Quasi-Ordnung auf $\mathcal{F}[\mathcal{A}]$ mit $\models$ zu bezeichnen kann Missverständnisse begünstigen. Wir wenden $\models\!\!\!=$ nie auf Formelmengen an.

Die $\mathcal{J}$-Algebra der $\mathcal{F}[\mathcal{A}]$-Äquivalenzklassen

Semantisch interessieren uns nur noch Formeln modulo $\models\!\!\models$, also die $\mathcal{J}$-Algebra $\mathcal{F}[\mathcal{A}]/\models\!\!\models$ der Äquivalenzklassen.

Aber warum bilden die Ä-Klassen überhaupt eine $\mathcal{J}$-Algebra?

Satz

$\models\!\!\models$ *ist eine Kongruenzrelation, d.h., aus* $A \models\!\!\models B$ *und* $C \models\!\!\models D$ *folgt*

- $\neg A \models\!\!\models \neg B$;
- $A \star C \models\!\!\models B \star D$

Beweis.

In den HA war untersucht worden, wie sich die kanonischen Operationen auf $\mathcal{F}[\mathcal{A}]$ mit der kanonischen Ordnung vertragen. Exemplarisch: wenn $A \sqsubseteq B$ und $C \sqsubseteq D$, dann auch $A \wedge C \sqsubseteq B \wedge D$. Nach Voraussetzung gilt aber auch $A \sqsupseteq B$ und $C \sqsupseteq D$, also $A \wedge C \sqsupseteq B \wedge D$, d.h., $A \wedge C \models\!\!\models B \wedge D$. $\square$

Folgende Rechenregeln reflektieren das Verhalten der kanonischen Interpretation der Junktoren in $\mathbb{B}$, siehe Folien 18, 19.
Man kann sie leicht mittels Wahrheitstabellen nachweisen:

Satz (HA)

- $\neg$ *ist selbstinvers, d.h.,* $\neg\neg A \models\!\!\!\models A$.
- $\wedge$ *und* $\vee$ *sind*
  - *idempotent, d.h.,* $A \wedge A \models\!\!\!\models A \models\!\!\!\models A \vee A$.
  - *assoziativ, d.h.,* $(A \star B) \star C \models\!\!\!\models A \star B \star C$ *für* $\star \in \{\wedge, \vee\}$.
  - *kommutativ, d.h.,* $A \star B \models\!\!\!\models B \star A$ *für* $\star \in \{\wedge, \vee\}$.
  - *mit neutralem Element* $\top$ *bzw.* $\bot$ *, d.h.,* $A \wedge \top \models\!\!\!\models A \models\!\!\!\models A \vee \bot$.
- $\bot$ *und* $\top$ *sind absorbierend bzgl.* $\wedge$ *bzw.* $\vee$ *, d.h.,* $A \wedge \bot \models\!\!\!\models \bot$ *und* $A \vee \top \models\!\!\!\models \top$.
- *es gelten die Absorbtionsregeln*

$$A \wedge (A \vee B) \models\!\!\!\models A \quad \text{und} \quad A \vee (A \wedge B) \models\!\!\!\models A \qquad \square$$

Notationelle Konvention + weitere Rechenregeln

Die Assoziativität von $\wedge$ und $\vee$ rechtfertigt folgende Schreibweise:

Notation

$$\bigwedge_{i<0} A_i := \top \ , \quad \bigwedge_{i<n+1} A_i := \Big(\bigwedge_{i<n} A_i\Big) \wedge A_n \quad \text{, und dual mit } \bigvee \text{ für } \vee$$

Satz (HA)

1. *Es gelten die De Morgan'schen Regeln:*

$$\neg \bigwedge_{i<n} A_i \dashv\vdash \bigvee_{i<n} \neg A_i \qquad \textit{sowie} \qquad \neg \bigvee_{i<n} A_i \dashv\vdash \bigwedge_{i<n} \neg A_i$$

2. *Es gelten die Distributivgesetze:*

$$A \wedge \bigvee_{i<n} B_i \dashv\vdash \bigvee_{i<n} (A \wedge B_i) \qquad \textit{sowie} \qquad A \vee \bigwedge_{i<n} B_i \dashv\vdash \bigwedge_{i<n} (A \vee B_i)$$

Funktional vollständige Junktorenmengen

Im Hinblick auf die Wahrheitstablellen 19 stellen wir fest, dass es 2^{2^n} n-stellige Boole'sche Funktionen 20 gibt.

Wie die De Morganschen Regeln zeigen, sind die durch $\mathcal{J}$ spezifizierten Funktionen redundant: neben $\vee$ können z.B. auch $\rightarrow$ und $\leftrightarrow$ eliminiert werden, ohne die Ausdrucksfähigkeit zu mindern.

Definition

Eine Menge $\mathcal{I}$ von Junktorsymbolen mit vorgegebener Semantik (= Wahrheitstabelle) heißt funktional vollständig, falls jede Boole'sche Funktion $\mathbb{B}^n \longrightarrow \mathbb{B}$ als f_A für geeignetes $A \in \mathbf{Term}(\mathcal{K}, \mathcal{A})$ dargestellt werden kann.

Satz (HA)

$\mathcal{J}$ ist funktional vollständig. □

Ist $\mathcal{I}$ funktional vollständig, so auch jede Junktor-Menge $\mathcal{I}'$, deren Junktoren alle Junktoren aus $\mathcal{I}$ simulieren können.

Post'scher Vollständigkeitssatz

Für $\mathcal{A}_0 \subseteq \mathcal{A}$ endlich heißt $A \in \mathcal{F}[\mathcal{A}_0]$

- $\bot$ / $\top$-erhaltend, falls $\hat{\varphi}(A) = 0/1$ für jede Belegung φ, die auf $\mathcal{A}_0$ den Wert $0/1$ annimmt;
- monoton, falls $\hat{\varphi}(A) \leq \hat{\psi}(A)$ für alle Belegungen φ und ψ, die $\varphi(p) \leq \psi(p)$ für alle $p \in \mathcal{A}_0$ erfüllen;
- linear, falls für jedes Atom $p \in \mathcal{A}_0$ und jede Belegung φ
  - entweder $\hat{\varphi}(A[p/\neg p]) = \hat{\varphi}(A)$ (dann heißt p Dummy-Variable);
  - oder $\hat{\varphi}(A[p/\neg p]) = 1 - \hat{\varphi}(A)$,
- selbst-dual, falls $\hat{\varphi}(A) = 1 - \hat{\varphi}(A[p/\neg p : p \in \mathcal{A}_0]$ für jede Belegung φ.

Satz (Post'scher Vollständigkeitssatz)

Eine Junktormenge $\mathcal{K}$ ist vollständig, wenn $\mathbf{Term}(\mathcal{K}, \mathcal{A})$ *je eine Formel enthält, die eine der obigen Eigenschaften nicht hat.* □

Kapitel 3
Deduktion allgemein

Wozu Deduktion?

Bisher konnten wir die Erfüllbarkeit einer Formel oder einer Formelmenge nur mit semantischen Mitteln überprüfen. Wegen $\Gamma \models A$ gdw. $\Gamma \cup \{\neg A\}$ unerfüllbar schließt das den Nachweis korrekter Schlussfolgerungen mit ein.

Mit wachsender Atom-Zahl nimmt der Aufwand, Wahrheitstabellen zu erstellen, exponentiell zu, stößt also bald an Grenzen.

Nach hinreichend vielen Beispielen wird man aber feststellen, dass man bestimmte korrekte Schlüsse allein anhand der Form, also der Syntax, ihrer Prämissen und der Schlussfolgerung erkennen und so den Aufwand einer semantischen Überprüfung vermeiden kann. Auf diese Weise erhält man verschiedene sog. deduktive Systeme.

Idealerweise sollten die logische Folgerelation $\models$ mit der Herleitungsrelation $\vdash$ eines deduktiven Systems übereinstimmen.

Deduktive Systeme sind aber nicht auf den Bereich der Logik beschränkt.

Schlussregeln und Theoreme

Definition

Ein deduktives System $\mathcal{K} = \langle \mathcal{F}, \mathcal{R} \rangle$ ($\mathcal{K}$ für Kalkül) besteht aus

- einer Menge $\mathcal{F}$ von sog. Formeln;
- einer Menge $\mathcal{R} \subseteq \mathcal{F}^* \times \mathcal{F}$ sog. Schlussregeln, oder kurz Regeln.

Alternative Schreibweise für Regeln (mit Prämissen A_i und Konklusion B):

$$\frac{A_0, A_1, \ldots, A_{k-1}}{B} \qquad \text{anstatt} \qquad \langle A_0, A_1, \ldots, A_{k-1}; B \rangle \in \mathcal{R}$$

Die Menge $\mathbf{Ax}(\mathcal{K})$ der Axiome besteht aus den Konklusionen von Regeln ohne Prämissen, also mit $k = 0$. Ihr Abschluss unter den Regeln bildet die Menge $\mathbf{Thm}(\mathcal{K})$ der Theoreme.

Regeln werden oft in Schemata zusammengefasst, mit Formel-Variablen.

Erste Beispiele

Beispiel (Ein deduktives System für partielle Syntax)

Mit der eingeschränkten Junktormenge $\mathcal{J}_0 = \{\neg, \to\}$ und den Klammern $(\!($ und $)\!)$ das Alphabet $\mathcal{J}_0[\mathcal{A}]$. Das deduktive System $\mathcal{K}_{\text{syn}} = \langle \mathcal{F}_{\text{syn}}, \mathcal{R}_{\text{syn}} \rangle$ verwendet als Formelmenge ganz $\mathcal{J}_0[\mathcal{A}]^*$ und

$$\begin{aligned}\mathcal{R}_{\text{syn}} := \mathcal{A} &\cup \{ \langle A, \neg A \rangle \,:\, A \in \mathcal{J}_0[\mathcal{A}]^* \} \\ &\cup \{ \langle A, B; (\!(A \to B)\!) \rangle \,:\, A, B \in \mathcal{J}_0[\mathcal{A}]^* \}\end{aligned}$$

oder als Regelschemata mit

$$\frac{}{v}\ (\nu) \quad (v \in \mathcal{A}) \quad , \quad \frac{A}{\neg A}\ (\neg) \quad \text{und} \quad \frac{A \quad B}{(\!(\, A \to B \,)\!)}\ (\to)$$

Die Atome (Elemente aus $\mathcal{A}$) sind die Axiome, während die Theoreme die aus dem Syntax-Kapitel bekannten Aussageformen, d.h., Formeln in den Junktoren $\neg$ und $\to$ sind.

Beispiel (Ein deduktives System $\mathcal{K}_{\mathrm{Ar}} = \langle \mathcal{F}_{\mathrm{Ar}}, \mathcal{R}_{\mathrm{Ar}} \rangle$ für die Arithmetik)

Setze $\mathcal{F}_{\mathrm{Ar}} := \mathbb{Q}$, die Menge der rationalen Zahlen. $\mathcal{R}_{\mathrm{Ar}}$ liefern folgende Schemata

$$\frac{}{1}\ (1) \quad , \quad \frac{x \quad y}{xy}\ (\times) \quad \text{und} \quad \frac{x \quad y}{x - y}\ (-)$$

Hierbei durchlaufen x und y alle rationalen Zahlen. Man mache sich klar, dass die Theoreme genau die ganzen Zahlen sind. Z.B. -2 erhält man mit

$$\dfrac{\dfrac{\dfrac{\dfrac{}{1}\ (1) \quad \dfrac{}{1}\ (1)}{0}\ (-) \quad \dfrac{}{1}\ (1)}{-1}\ (-) \quad \dfrac{}{1}\ (1)}{-2}\ (-)$$

Man kann diese Kombination von Regeln als eine Art gerichteten „Baum“ verstehen, mit Axiomen als Blättern und den „Bruchstrichen“ der Regeln als Knoten mit $k \in \mathbb{N}$ Eingabe-Kanten und genau einer Ausgabe-Kante. Alternativ sind die Regeln Kanten eines sog. „Multigraphen“.

Herleitungen (auch Beweise genannt)

Definition

Eine Herleitung einer Formel A im deduktiven System $\mathcal{K} = \langle \mathcal{F}, \mathcal{R} \rangle$ ist ein Wort $\langle A_i : i < n \rangle \in \mathcal{F}^*$ mit

- $A_{n-1} = A$
- zu jedem $j < n$ gibt es eine Indexfolge $i \in (j-1)^*$ derart, dass $\langle \langle A_{i_k} : k < t \rangle ; A_j \rangle$ eine Schlussregel ist; i heißt Begründung für A_j.

$A \in \mathcal{F}$ heißt herleitbar, wenn es eine Herleitung von A gibt.

Beispiel

Eine mögliche Herleitung von -42 im obigen deduktiven System $\mathcal{K}_{\mathrm{Ar}}$ ist

$$\langle 1,\, 0,\, -1,\, -2,\, 4,\, -6,\, 36,\, -42 \rangle$$

Der entsprechende Baum, der -42 im Regelabschluss des Axioms 1 verortet, hat 71 Knoten und der Teilbaum für -2 tritt neunmal darin auf.

Satz

Eine Formel ist genau dann ein Theorem, wenn sie herleitbar ist.

Beweis.

Die Hinlänglichkeit folgt mittels Induktion über die Länge der Herleitung, die Notwendigkeit mittels Induktion über den Aufbau von Theoremen. □

Obiges Beispiel zeigt, wie viel kürzer Herleitungen sein können, verglichen mit der expliziten Angabe des Regel-Abschlusses ausgehend von bestimmten Axiomen. Sie enthalten viel weniger Redundanz.

Definition

Unter einer expliziten Herleitung versteht man eine vertikale Auflistung der Folgenglieder mit ihrer Nummer und ihrer Begründung, samt Kurzname der verwendeten Regel.

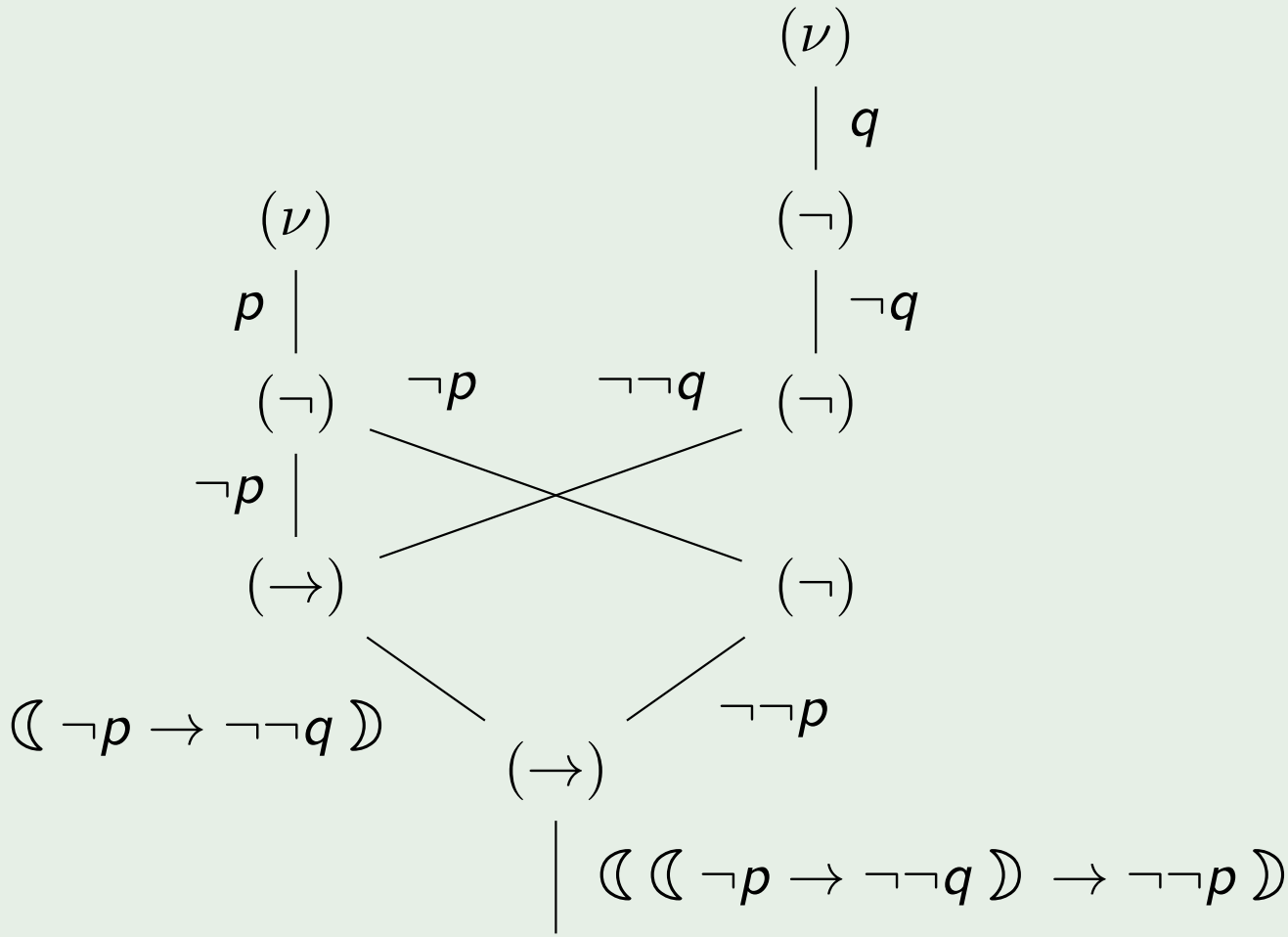
Beispiel

Explizite Herleitung von $(\!(\, (\!(\, \neg p \to \neg\neg q \,)\!) \to \neg\neg p \,)\!)$ in $\mathcal{K}_{\mathrm{syn}}$:

0. p	(ν)
1. $\neg p$	$(\neg), 0$
2. q	(ν)
3. $\neg q$	$(\neg), 2$
4. $\neg\neg q$	$(\neg), 3$
5. $(\!(\neg p \to \neg\neg q)\!)$	$(\to), 1, 4$
6. $\neg\neg p$	$(\neg), 2$
7. $(\!(\!(\neg p \to \neg\neg q)\!) \to \neg\neg p)\!)$	$(\to), 5, 6.$

Dies läßt sich graphisch aufbereiten mit Regelnamen als Knoten und Formeln als Ein- und Ausgaben; die Schrittnummern können dann entfallen.

Beispiel (Herleitungsgraph; Richtung von oben nach unten)



Ein Baum entsteht nur, wenn jede Formel außer der Wurzel genau einmal in einer Begründung auftritt. Sonst sind Knoten aufzuspalten:

Beispiel (Herleitungsbaum, „Bruchstriche“ als Knoten, Kanten implizit)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p}\,(\nu)}{\neg p}\,(\neg) \qquad \dfrac{\dfrac{\dfrac{}{q}\,(\nu)}{\neg q}\,(\neg)}{\neg\neg q}\,(\neg)}{(\!(\, \neg p \to \neg\neg p \,)\!)}\,(\to) \qquad \dfrac{\dfrac{\dfrac{}{p}\,(\nu)}{\neg p}\,(\neg)}{\neg\neg p}\,(\neg)}{(\!(\, (\!(\, \neg p \to \neg\neg q \,)\!) \to \neg\neg p \,)\!)}\,(\to)$$

Ein Herleitungsbaum läßt die Struktur der Herleitung deutlicher erkennen und ist vertikal kompakter, aber zum Preis von deutlich mehr Knoten, wie das Beispiel der Herleitung von -42 in $\mathcal{K}_{\mathrm{Ar}}$ oben zeigt.

Erweiterung des Herleitungsbegriffs: Ableitungen

Definition

Eine Ableitung einer Formel A im deduktiven System $\mathcal{K} = \langle \mathcal{F}, \mathcal{R} \rangle$ aus einer Formelmenge Γ ist ein Wort $\langle A_i : i < n \rangle \in \mathcal{F}^*$ mit

- $A_{n-1} = A$
- für jedes $j < n$ hat A_j entweder eine Begründung $i \in (j-1)^*$ wie bei einer Herleitung, oder $A_j \in \Gamma$.

A heißt aus Γ ableitbar ($\Gamma \vdash_{\mathcal{K}} A$), wenn eine solche Ableitung existiert.

Die notationellen Konventionen orientieren sich an denen für $\models$.

Satz (HA)

Ein deduktives System $\mathcal{K} = \langle \mathcal{F}, \mathcal{R} \rangle$ induziert einen Hüllenoperator vermöge

$$\Gamma^{\vdash_{\mathcal{K}}} := \{ A \in \mathcal{F} : \Gamma \vdash_{\mathcal{K}} A \}$$

Dessen Fixpunkte heißen deduktiv abgeschlossene Mengen.

Der Beweis des folgenden Satzes ist viel einfacher als der Beweis seines semantischen Gegenstücks:

Satz (Kompkatheitssatz, syntaktisch (HA))

Eine Formel $A \in \mathcal{F}$ ist aus $\Gamma \subseteq \mathcal{F}$ genau dann ableitbar, wenn sie aus einer endlichen Teilmenge $\Gamma_0 \subseteq \Gamma$ ableitbar ist.

Kapitel 4
Deduktion in der Aussagenlogik

Ziel

Wir wollen ein deduktives System $\mathcal{K}_0 = \langle \mathcal{F}_0, \mathcal{R}_0 \rangle$ einführen, für das die Relation $\vdash_{\mathcal{K}_0}$ mit $\models$ übereinstimmt. Vereinfachend setzen wir $\vdash := \vdash_{\mathcal{K}_0}$.

Die Formelmenge $\mathcal{F}_0$ besteht aus den Aussageformen über der vollständigen Junktorenmenge $\mathcal{J}_0 = \{\neg, \to\}$, während $\mathcal{R}_0$ durch vier Schemata gegeben ist (beachte die Klammervereinfachungen!):

- $$\frac{A \quad A \to B}{B} \ (MP)$$ Abtrennungsregel oder modus ponens
- $$\frac{}{B \to A \to B} \ (\text{Ax1})$$
- $$\frac{}{(A \to B \to C) \to (A \to B) \to A \to C} \ (\text{Ax2})$$
- $$\frac{}{(\neg B \to \neg A) \to (A \to B)} \ (\text{Ax3})$$

Lemma

Für jede Formel $A \in \mathcal{F}_0$ gilt:

$$\vdash A \to A \qquad \text{(Th1)}$$

Beweis.

Wir geben eine explizite Herleitung:

0.	$A \to A \to A$	Ax1
1.	$A \to (A \to A) \to A$	Ax1
2.	$(A \to (A \to A) \to A) \to (A \to A \to A) \to A \to A$	Ax2
3.	$(A \to A \to A) \to A \to A$	MP, 1,2
4.	$A \to A$	MP, 0,3 $\square$

Achtung: Die Klammerersparnisregeln für $\to$ können die Lesbarkeit zunächst beeinträchtigen. Dagegen hilft nur Routine.

Das syntaktische Deduktionstheorem

Der Nutzen von $\mathcal{K}_0$ beruht wesentlich auf dem

Satz (Deduktionstheorem)

$\Gamma \cup \{A\} \vdash B$ *genau dann wenn* $\Gamma \vdash A \to B$.

Beweis.

($\Leftarrow$) Aus $\Gamma \cup \{A\}$ lassen sich A und $A \to B$ ableiten, also auch B .

($\Rightarrow$) Induktion über alle aus $\Gamma \cup \{A\}$ ableitbaren Formeln B :

- $B \in \mathbf{Ax} \cup \Gamma$: Wende (MP) an auf B und das Axiom $B \to A \to B$.
- B ist Konklusion von aus $\Gamma \cup \{A\}$ ableitbaren Prämissen C und $C \to B$: Nach IV sind dann auch $A \to C$ und $A \to C \to B$ aus Γ ableitbar. 2-malige Anwendung von (MP) auf die Instanz $(A \to C \to B) \to (A \to C) \to A \to B$ von (Ax2) liefert $A \to B$.
- $B = A$: obiges Lemma. □

Sieben weitere Tautologie-Schemata

Lemma

$$\vdash \neg\neg A \to A \qquad \text{(Th2)}$$

Beweis (unter Verwendung des Deduktionstheorems).

0. $\neg\neg A$	Ann.
1. $\neg\neg A \to \neg\neg\neg\neg A \to \neg\neg A$	Ax1
2. $\neg\neg\neg\neg A \to \neg\neg A$	MP, 0,1
3. $(\neg\neg\neg\neg A \to \neg\neg A) \to \neg A \to \neg\neg\neg A$	Ax3
4. $\neg A \to \neg\neg\neg A$	MP, 2,3
5. $(\neg A \to \neg\neg\neg A) \to \neg\neg A \to A$	Ax3
6. $\neg\neg A \to A$	MP, 4,5
7. A	MP, 0,6) $\square$

Lemma

(a) $\vdash \neg B \to B \to A$ (Th3)

(b) $\vdash B \to \neg\neg B$ (Th4)

Beweis (unter Verwendung des Deduktionstheorems).

(a)

0. $\neg B$	Ann.
1. $\neg B \to \neg A \to \neg B$	Ax1
2. $\neg A \to \neg B$	MP, 0,1
3. $(\neg A \to \neg B) \to B \to A$	Ax3
4. $B \to A$	MP, 2,3

(b)

0. $\neg\neg\neg B \to \neg B$	Th2
1. $(\neg\neg\neg B \to \neg B) \to B \to \neg\neg B$	Ax3
2. $B \to \neg\neg B$	MP, 0,1

□

Lemma

$$\vdash (A \to B) \to \neg B \to \neg A \qquad \text{(Th5)}$$

Beweis.

0.	$A \to B$	Ann.
1.	$\neg\neg A$	Ann.
2.	$\neg\neg A \to A$	Th2
3.	A	MP, 1,2
4.	B	MP, 3,0
5.	$B \to \neg\neg B$	Th4
6.	$\neg\neg B$	MP, 4,5
7.	$\neg\neg A \to \neg\neg B$	DT, 2–7
8.	$(\neg\neg A \to \neg\neg B) \to \neg B \to \neg A$	Ax1
9.	$\neg B \to \neg A$	MP, 7,8
10.	$(A \to B) \to \neg B \to \neg A$	DT, 0–9

□

Lemma

$$\vdash A \to \neg B \to \neg(A \to B) \qquad \text{(Th6)}$$

Beweis.

0.	A	Ann.
1.	$\quad A \to B$	Ann.
2.	$\quad B$	MP, 0,1
3.	$(A \to B) \to B$	DT, 2–3
4.	$((A \to B) \to B) \to \neg B \to \neg(A \to B)$	Th5
5.	$\neg B \to \neg(A \to B)$	MP, 3,4
6.	$A \to \neg B \to \neg(A \to B)$	DT, 0–5

□

Lemma

$$\vdash (A \to B) \to (A \to \neg B) \to \neg A \qquad \text{(Th7)}$$

Beweis.

0.	$A \to B$	Ann.
1.	$A \to \neg B$	Ann.
2.	A	Ann.
3.	B	MP, 2,0
4.	$\neg B$	MP, 2,1
5.	$\neg B \to B \to \neg(A \to A)$	Th3
6.	$B \to \neg(A \to A)$	MP, 4,5
7.	$\neg(A \to A)$	MP, 3,7
8.	$A \to \neg(A \to A)$	DT, 2–7
9.	$A \to A$	Th1
10.	$(A \to A) \to \neg\neg(A \to A)$	Th4
11.	$\neg\neg(A \to A)$	MP, 9,10
12.	$(A \to \neg(A \to A)) \to (\neg\neg(A \to A) \to \neg A)$	Th5
13.	$\neg\neg(A \to A) \to \neg A$	MP, 8,12
14.	$\neg A$	MP 11,13
15.	$(A \to \neg B) \to \neg A$	DT, 2–14
16.	$(A \to B) \to (A \to \neg B) \to \neg A$	DT, 1–15

□

Lemma

$$\vdash (B \to A) \to (\neg B \to A) \to A \qquad \text{(Th8)}$$

Beweis.

0.	$B \to A$	Ann.
1.	$(B \to A) \to \neg A \to \neg B$	Th5
2.	$\neg A \to \neg B$	MP, 0,1
3.	$\neg B \to A$	Ann.
4.	$(\neg B \to A) \to \neg\, A \to \neg\neg B$	Th5
5.	$\neg\, A \to \neg\neg B$	MP, 3,4
6.	$(\neg A \to \neg B) \to (\neg A \to \neg\neg B) \to \neg\neg A$	Th7
7.	$(\neg A \to \neg\neg B) \to \neg\neg A$	MP, 2,6
8.	$\neg\neg A$	MP, 5,7
9.	$\neg\neg A \to A$	Th2
10.	A	MP, 8,9
11.	$(\neg B \to A) \to A$	DT, 3–10
12.	$(B \to A) \to (\neg B \to A) \to A$	DT, 0–11

□

Zusammenfassung

Künftig dürfen wir neben den ursprünglichen Regeln von $\mathcal{K}_0$ (MP, Ax1, Ax2, Ax3) und dem syntaktischen Deduktionstheorem auch die Tautologie-Schemata (Th1) – (Th8) in Ableitungen verwenden:

- (Th1) $\vdash A \to A$
- (Th2) $\vdash \neg\neg A \to A$
- (Th3) $\neg B \to B \to A$
- (Th4) $\vdash B \to \neg\neg B$
- (Th5) $(A \to B) \to (\neg B \to \neg A)$
- (Th6) $\vdash A \to \neg B \to \neg(A \to B)$
- (Th7) $(A \to B) \to (A \to \neg B) \to \neg A$
- (Th8) $(B \to A) \to (\neg B \to A) \to A$

Definition

Eine Menge $\Gamma \subseteq \mathcal{F}_0$ heißt widersprüchlich oder inkonsistent, wenn eine Formel $B \in \mathcal{F}_0$ mit $\Gamma \vdash B$ und $\Gamma \vdash \neg B$ existiert.

0-Korrektheit und 0-Vollständigkeit von $\mathcal{K}_0$, Vorarbeiten

Satz

Eine Formel ist genau dann Theorem von $\mathcal{K}_0$, wenn sie eine Tautologie ist.

Die Notwendigkeit (0-Korrektheit des Kalküls) ist leicht (HA). Der Beweis der Hinlänglichkeit (0-Vollständigkeit) erfordert einige Vorarbeit.

Lemma

Für eine Teilmenge $\mathcal{A}_0$ von Atomen, eine Formel $A \in \mathcal{F}_0[\mathcal{A}_0]$ (in den Junktoren $\neg$ und $\to$) und eine Belegung $\varphi \in \mathbb{B}^{\mathcal{A}}$ gilt ${}^{\varphi}\mathcal{A}_0 \vdash {}^{\varphi}A$.

Beweis. (Struturelle Induktion über A)

- A atomar impliziert $A = p \in \mathcal{A}_0$, also ${}^{\varphi}A \in {}^{\varphi}\mathcal{A}_0$.
- $A = \neg B$ und B ist aus ${}^{\varphi}\mathcal{A}_0$ herleitbar.
  - $\hat{\varphi}(B) = 0$ impliziert ${}^{\varphi}B = \neg B = A = {}^{\varphi}A$; fertig.
  - $\hat{\varphi}(B) = 1$ impliziert ${}^{\varphi}B = B$ und ${}^{\varphi}A = \neg A = \neg\neg B$. Damit genügt es, $B \vdash \neg\neg B$ nachzuweisen, was mittels MP aus (Th4) folgt.

Beweis. (Fortsetzung)

- $A = B \to C$ und sowohl ${}^{\varphi}B$ als auch ${}^{\varphi}C$ sind herleitbar.
  - $\hat{\varphi}(C) = 1$ impliziert ${}^{\varphi}C = C$ und ${}^{\varphi}A = B \to C$. Damit genügt es, $C \vdash B \to C$ nachzuweisen, was sofort aus Ax1 folgt.
  - $\hat{\varphi}(B) = 0$ impliziert ${}^{\varphi}B = \neg B$ und ${}^{\varphi}A = B \to C$. Damit genügt es, $\neg B \vdash B \to C$ nachzuweisen, was sofort aus (Th3) folgt.
  - $\hat{\varphi}(C) = 0$ und $\hat{\varphi}(B) = 1$ impliziert ${}^{\varphi}C = \neg C$, ${}^{\varphi}B = B$ und ${}^{\varphi}A = \neg(B \to C)$. Damit genügt es, $\{B, \neg C\} \vdash \neg(B \to C)$ nachzuweisen, und das folgt aus (Th6). □

Lemma

Mit $\Gamma \cup B \vdash A$ *und* $\Gamma \cup \{\neg B\} \vdash A$ *gilt auch* $\Gamma \vdash A$.

Beweis.

DT liefert $\Gamma \vdash B \to A$ sowie $\Gamma \vdash \neg B \to A$. Aber $\{B \to A, \neg B \to A\} \vdash A$ folgt nach zweimaliger Anwendung von (MP) aus (Th8). □

0-Vollständigkeit von $\mathcal{K}_0$

Beweis.

A sei eine Tautologie, in der n Atome auftreten, etwa $\{ p_i : i < n \}$. Nach dem ersten Lemma gilt für jede Belegung φ

$$ {}^{\varphi}\{ p_i : i < n \} \vdash {}^{\varphi}A = A \qquad (\star) $$

Das zweite Lemma erlaubt es, induktiv die Atome p_i, $i < n$, auf der linken Seite zu entfernen, bis $\vdash A$ übrigbleibt: Wähle φ beliebig und setze

$$ \varphi_k(p_j) = \begin{cases} \varphi(p_i) & \text{falls } i < k \\ 1 - \varphi(p_i) & \text{falls } i \geq k \end{cases} \quad \text{für} \quad k < n $$

All diese $k+1$ Belegungen erfüllen $(\star)$. Da sich ${}^{\varphi_{k-1}}\{ p_i : i < n \}$ und ${}^{\varphi_k}\{ p_i : i < n \}$ an genau einer Stelle unterscheiden, folgt nach dem zweiten Lemma ${}^{\varphi}\{ p_i : i < k \} \vdash A$ für alle $k < n$, speziell $k = 0$. □

Korrektheit und Vollständigkeit von $\mathcal{K}_0$

Satz

A ist genau dann in $\mathcal{K}_0$ aus Γ ableitbar, wenn A logisch aus Γ folgt.

Beweis.

Im Folgenden sei $\Gamma_0 = \{ A_i : i < n \}$ eine endliche Teilmenge von Γ.

$$
\begin{aligned}
\Gamma \vdash B \quad & \text{gdw.} \quad \text{es gibt } \Gamma_0 \subseteq \Gamma \text{ mit } \Gamma_0 \vdash B \\
& \text{gdw.} \quad \text{es gibt } \Gamma_0 \subseteq \Gamma \text{ mit } \vdash A_0 \to A_2 \to \ldots \to A_{n-1} \to B \\
& \text{gdw.} \quad \text{es gibt } \Gamma_0 \subseteq \Gamma \text{ mit } \models A_0 \to A_2 \to \ldots \to A_{n-1} \to B \\
& \text{gdw.} \quad \text{es gibt } \Gamma_0 \subseteq \Gamma \text{ mit } \Gamma_0 \models B \\
& \text{gdw.} \quad \Gamma \models B
\end{aligned}
$$

□

Hier wurden auf der semantischen und der syntaktischen Seite jeweils die entsprechenden Kompaktheitssätze und Deduktionstheoreme angewendet, und „in der Mitte“ die prämissenfreie Variante des Satzes.

Bemerkungen

- Der wesentliche Punkt des obigen Beweises ist die Verfügbarkeit des syntaktischen Deduktionstheorems (DT) für den Kalkül $\mathcal{K}_0$.
- Für andere Kalküle $\mathcal{K}$ mit dem Junktor $\rightarrow$ stellt sich die Frage, ob sie das Deduktionstheorem $\Gamma \vdash_{\mathcal{K}} A \rightarrow B$ gdw. $\Gamma \cup \{A\} \vdash_{\mathcal{K}} B$ erfüllen.
- Man kann zeigen, dass aus der Gültigkeit des DT die Schemata (MP), (Ax1) und (Ax2) herleitbar sind. Das Schema (Ax3), das nicht im Beweis des DT für $\mathcal{K}_0$ verwendet wurde, kann hingegen auch durch andere Schemata ersetzt werden (z.B. Varianten des modus tollens).
- Deduktive Systeme der Logik, die wie $\mathcal{K}_0$ möglichst wenige Schlußregeln verwenden, werden Hilbert[2]-Kalküle genannt. $\mathcal{K}_0$ selbst geht auf Łukasiewicz[3] zurück, und stellt eine Vereinfachung des bahnbrechenden Systems von Frege[4] dar.

[2] David Hilbert (1862–1943)
[3] Jan Łukasiewicz (1878–1956), auch Erfinder der sog. „polnischen Notation“
[4] Gottlob Frege (1848–1925)

Andere deduktive Systeme: natürliche Deduktion

Die herausgehobene Bedeutung des Junktors $\to$ und die Auswahl der Axiomschemata in Hilbert-Kalkülen gelten nicht universell als Vorteile: was zeichnet (Ax2) aus, wenn $A \to A$ aufwändig hergeleitet werden muß?

▸ Dagegen haben Kalküle des ▸ natürlichen Schließens keine Axiome. Ihre Einführungs- und Eliminationsregeln für die einzelnen Junktoren in $\mathcal{J}$ sollen fundamentale Wahrheiten über diese ausdrücken (Jaśkowski[5] und unabhängig Gentzen[6], 1934). Das Symbol $\vdash$ wandelt seine Rolle von einer externen Relation zu einem Bestandteil der Syntax: die Formeln von $\mathcal{K}_{\mathrm{nat}}$ sind sog. Sequenzen $B_0, \ldots, B_{n-1} \vdash A$, und die Ableitbarkeit von A aus den B_i, $i < n$, meint nun, dass obige Sequenz ein Theorem von $\mathcal{K}_{\mathrm{nat}}$ ist. Dieses System ermöglicht eine sehr effiziente Konstruktion von Beweisen in intuitionistischer Logik, die im Gegensatz zur klassischen Logik die Eliminierung doppelter Negation nicht zuläßt.

[5] Stanisław Jaśkowski (1906–1965)
[6] Gerhard Gentzen (1909–1945)

Andere deduktive Systeme: Gentzen-Kalkül, siehe Skript

Gentzens ▸ zweites System war ursprünglich als technisches Hilfmittel zum Beweis der Konsistenz der Prädikatenlogik gedacht.

Es verwendet als Formeln(!) symmetrischen Sequenzen $\Gamma \vdash \Delta$, bei denen links und rechts endliche Folgen von Formeln aus $\mathcal{F}[\mathcal{A}]$ stehen dürfen. Eine solche Sequenz ist korrekt, wenn $\bigwedge \Gamma \to \bigvee \Delta$ allgemeingültig ist.

Prämissen, wie sie uns bisher interessierten, werden durch die Seqenzen schon abgedeckt. Betrachtet man dagegen das Problem, ob eine einzelne Sequenz $\Gamma \vdash \Delta$ aus einer Menge $\mathfrak{S}$ von Sequenzen folgt, so stellt sich heraus, dass der Gentzen-Kalkül in diesem erweiterten Sinne zwar korrekt, aber nicht vollständig ist. Dieses Problem kann durch Einbeziehung der sog. Schnittregel behoben werden:

$$\frac{\Gamma_0, A \vdash \Delta_0 \qquad \Gamma_1 \vdash A, \Delta_1}{\Gamma_0, \Gamma_1 \vdash \Delta_0, \Delta_1}$$

Kapitel 5
Algorithmen für die Aussagenlogik

Übersicht

Zum Nachweis von $\Gamma \models A$ kann man anstelle von $\Gamma \vdash A$ natürlich auch die Nichterfüllbarkeit von $\Gamma \cup \{\neg A\}$ überprüfen. Aufgrund des KPS läßt sich selbst bei unendlichem Γ in endlich vielen Schritten feststellen, dass $\Gamma \cup \{\neg A\}$ nicht erfüllt werden kann, im Gegensatz zur Erfüllbarkeit. Daher heißt das Problem der Unerfüllbarkeit semi-entscheidbbar.

Wir stellen drei Algorithmen vor, mit deren Hilfe die Nichterfüllbarkeit von Formeln bzw. Formelmengen mit syntaktischen Mitteln häufig schneller gezeigt werden kann, als mittels Wahrheitstabellen (brute force). Im ungünstigsten Fall ist ihre Laufzeit aber immer noch exponentiell.

Während semantische Tableaus auf beliebige Formelmengen anwendbar ist, erfordert der Davis-Putnam Algorithmus Formeln in Negations-Normalform (NNF), während die Resolutionsmethode Formeln in konjunktiver Normalform (KNF) benötigt. Insofern werden wir kurz auf diese und ähnliche Normalformen eingehen.

Semantische Tableaus, Vorüberlegungen

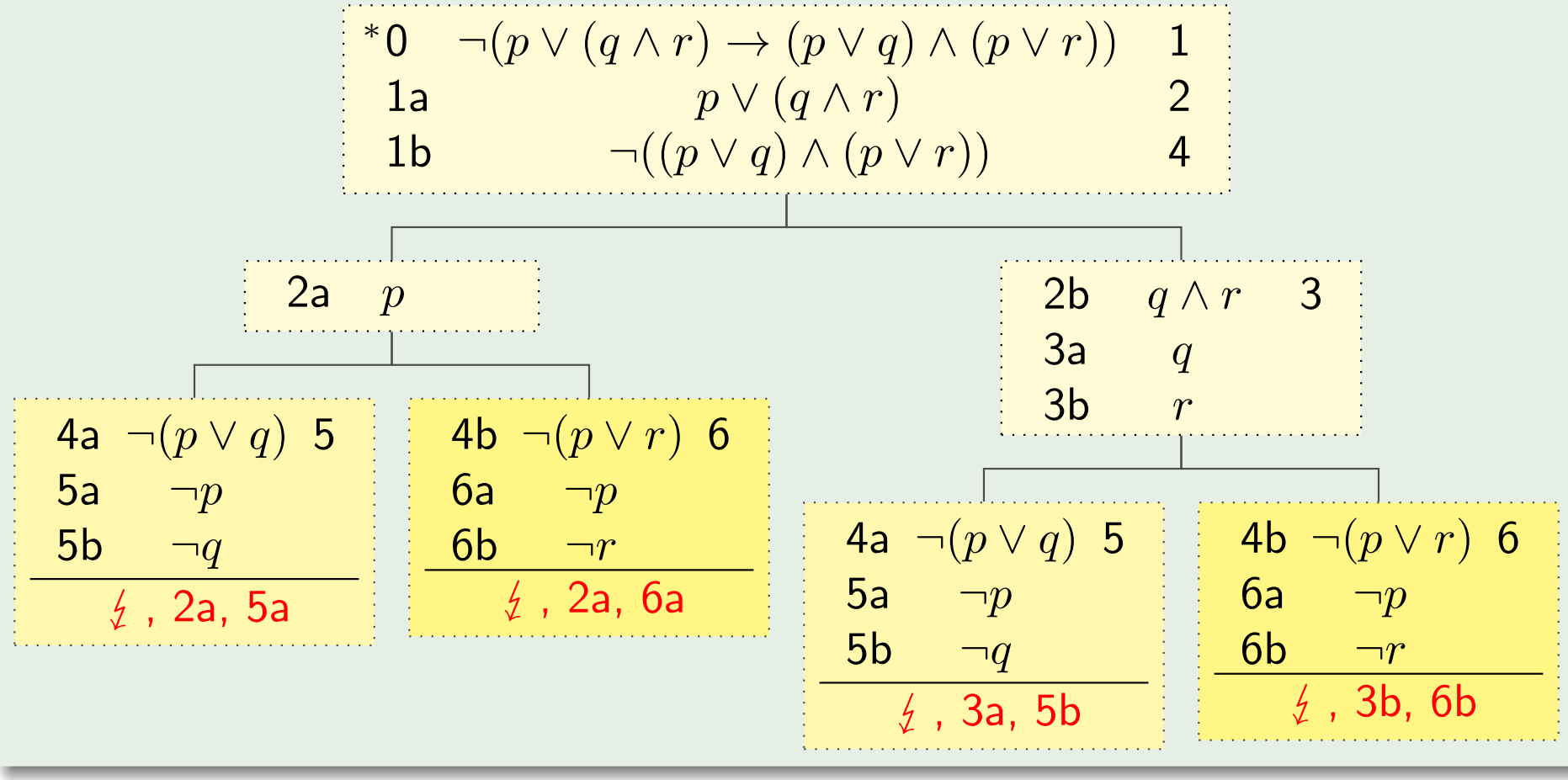
Wir klassifizieren Formeln über $\mathcal{J}_1 = \{\neg, \wedge, \vee, \rightarrow\}$ als

- Literale, also Atome in $\mathcal{A}$ oder deren Negationen;
- doppelte Negationen;
- bis auf Äquivalenz binäre Konjunktionen, genannt α-Formeln;
- bis auf Äquivalenz binäre Disjunktionen, genannt β-Formeln.

Strategie: Ersetze die Formeln in $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$ durch einfachere Formeln, bis Literale erreicht sind. α- und β-Formeln liefern die beiden Argumente der äquivalenten Kon- bzw. Disjunktion; doppelte Negationen werden entfernt.

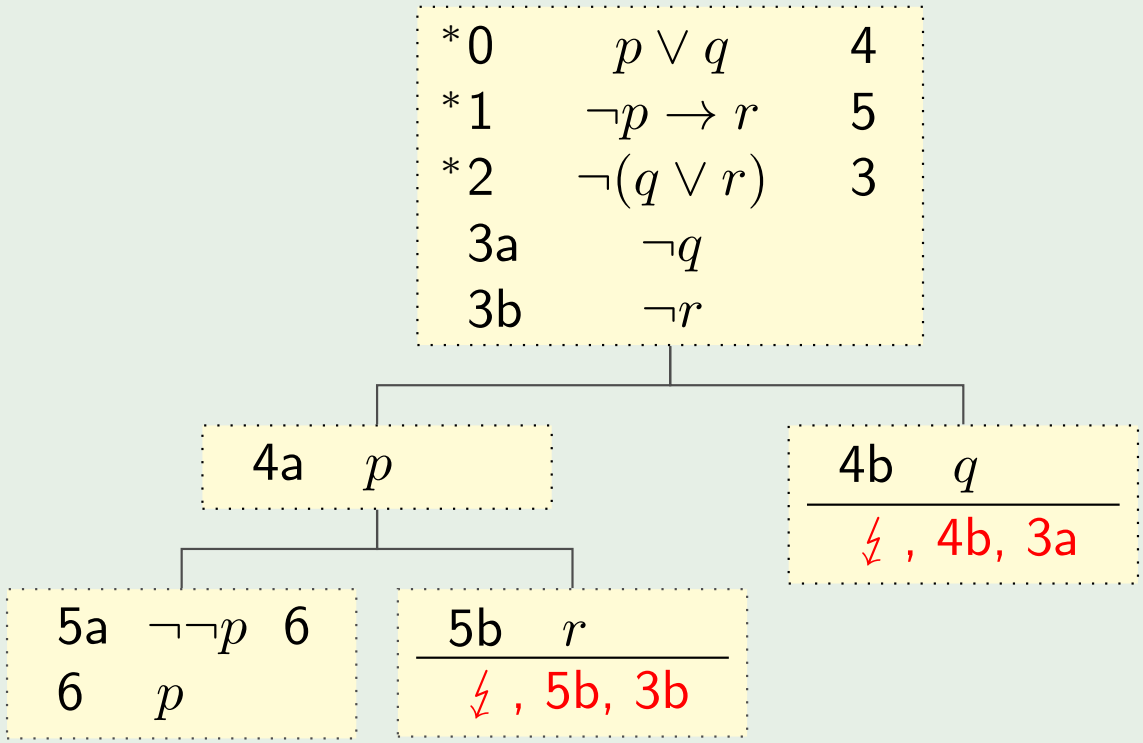
Disjunktionen führen dabei zu Fallunterscheidungen hinsichtlich der zu untersuchenden Formelmenge, die sich durch binäre Verzweigungen in einer Baumstruktur darstellen lassen, mit Formelmengen als Knoten. Genau die Zweige ohne widersprüchliche Literale in der Vereinigung ihrer Knoten-Mengen werden den möglichen erfüllenden Belegungen entsprechen.

Beispiel ($\Gamma = \{\neg(p \vee (q \wedge r) \to (p \vee q) \wedge (p \vee r))\}$ ist nicht erfüllbar)



Die optionalen linken/rechten Label zeigen die Reihenfolge der Entstehung/ Abarbeitung (nicht-deterministisch!). Die Arbeit in den linken bzw. rechten beiden unteren Knoten kann parallel erfolgen bzw. kopiert werden; allerdings ergeben sich anderere Widersprüche.

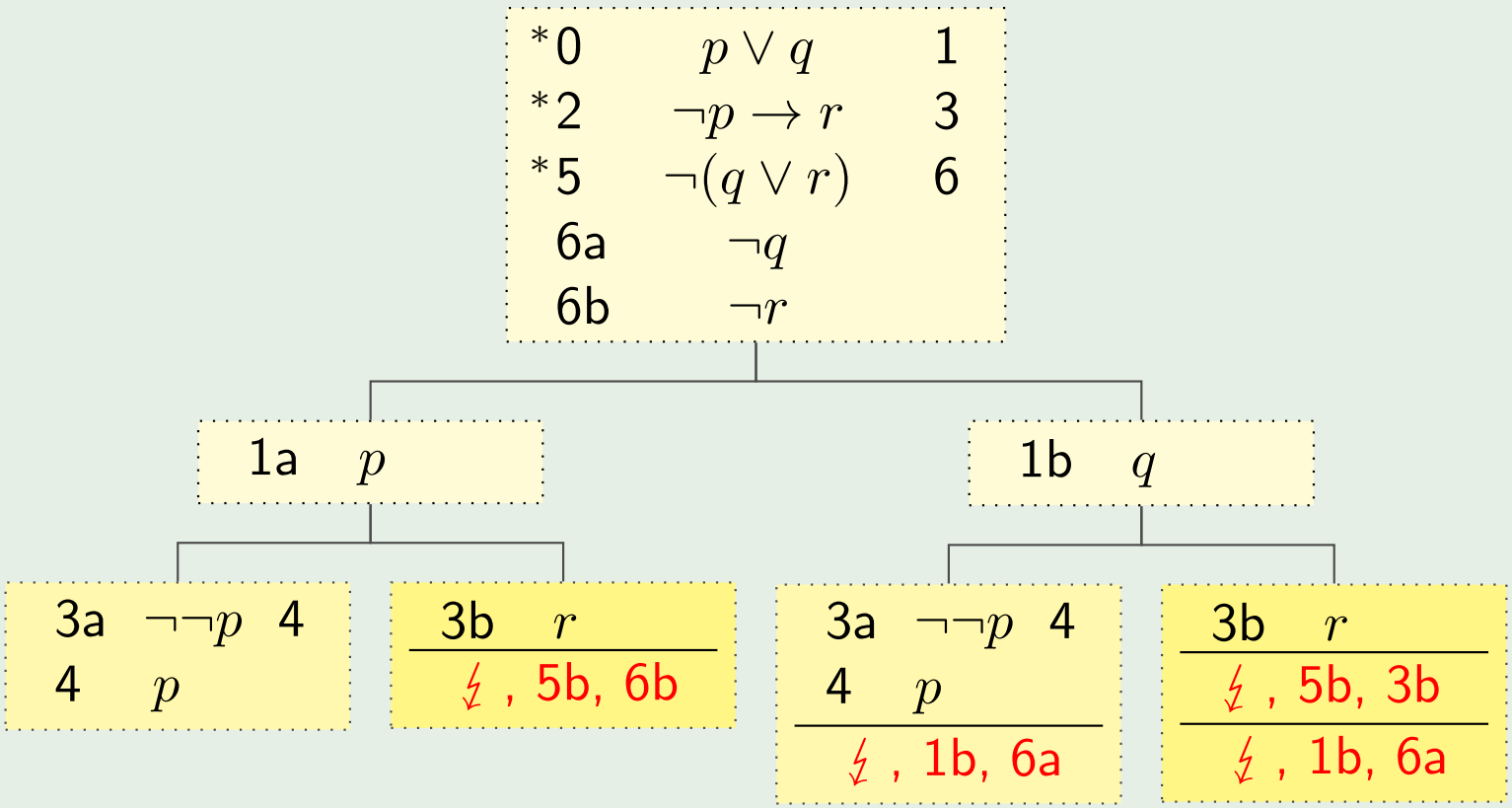
Beispiel ($\Gamma = \{A_0 = p \vee q, A_1 = \neg p \to r, A_2 = \neg(p \vee r)\}$ ist erfüllbar)



Entlang des widerspruchsfreien linken Astes macht die Belegung $p \longmapsto 1$, $q \longmapsto 0$, $r \longmapsto 0$ die Literale (Einträge 6, 3a und 3b), und damit Γ wahr.

Alternativ kann man A_1 und A_2 erst dann der Wurzelmenge hinzufügen, wenn die Vorgängerformel vollständig abgearbeitet ist. Das liefert

Beispiel ($\Gamma = \{p \vee q, \neg p \to r, \neg(p \vee r)\}$ ist erfüllbar, Alternative)



Hier wurden die Komponenten von α- und Doppelnegations-Formeln ihrer lokalen Knotenmenge hinzugefügt; nur β-Formeln entfalten „Fernwirkung“. Zwar wird der Widerspruch zwischen 1b und 6a später erkannt als in der vorigen Variante, aber bei unendlichem Γ hat diese Variante Vorteile.

Die Notation für die syntaktisch(!) definierten Zerlegungsschritte lehnt sich an jene für die Schlußreglen deduktiver Systeme an. Die kleineren Komponenten unter dem „Bruchstrich“ landen bei doppelter Negation und für α-Formeln in selben Knoten-Menge des Baumes wie die Ursprungsformel und werden ggf. untereinander geschrieben:

$$\frac{\neg\neg A}{A} \quad , \quad \frac{A \wedge B}{\begin{array}{c} A \\ B \end{array}} \quad , \quad \frac{\neg(A \vee B)}{\begin{array}{c} \neg A \\ \neg B \end{array}} \quad , \quad \frac{\neg(A \to B)}{\begin{array}{c} A \\ \neg B \end{array}}$$

- ▷ Sind die Komponenten wahr, so auch die Ursprungsformel.

Bei den fernwirkenden β-Formeln deutet ein senkrechter Strich zwischen den beiden Alternativen im „Nenner“ die Verzweigung an, die zunächst an jedem Blatt vorzunehmen ist:

$$\frac{A \vee B}{A \,|\, B} \quad , \quad \frac{\neg(A \wedge B)}{\neg A \,|\, \neg B} \quad , \quad \frac{A \to B}{\neg A \,|\, B}$$

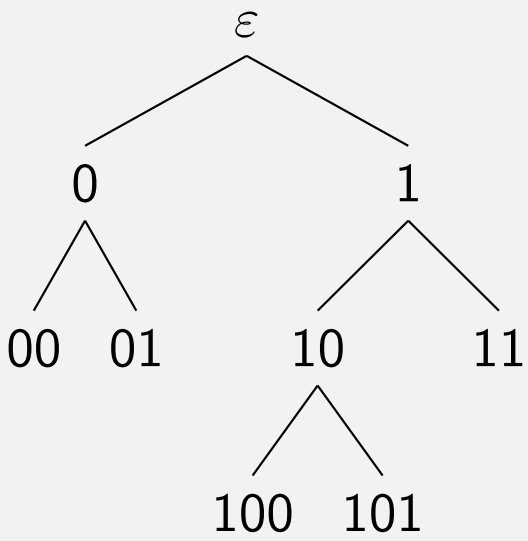
- ▷ Ist mindestens eine Komponente wahr, so auch die Ursprungsformel.

Gerade binäre Bäume

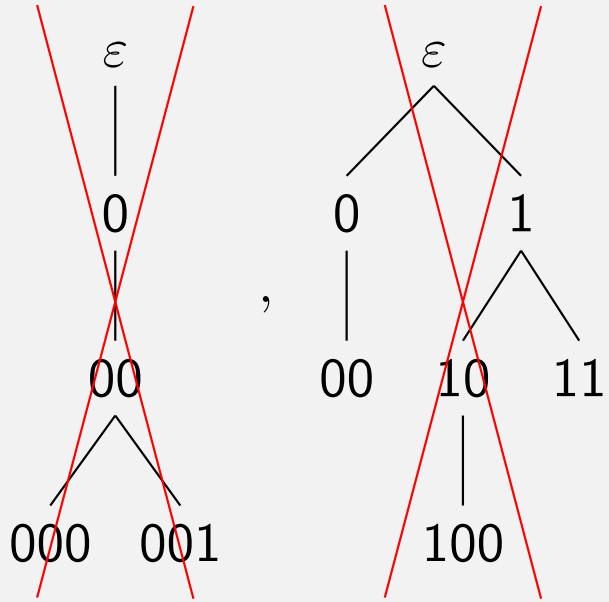
Definition

Ein gerader binärer Baum ist eine präfix-abgeschlossene Menge $\mathcal{B} \subseteq \{0,1\}^*$ binärer Wörter, so dass aus $w \in \mathcal{B}$ folgt: $w0 \in \mathcal{B}$ gdw. $w1 \in \mathcal{B}$.

Die Elemente von $\mathcal{B}$ fungieren gleichzeitig als Knoten und als Wegweiser von der Wurzel ε zum entsprechenden Knoten, etwa



aber



Die Gegenbeispiele erfüllen als binäre Bäume $w1 \in \mathcal{B}$ impliziert $w0 \in \mathcal{B}$.

Definition

Ein Tableau für $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$ ist Abbildung $\{0,1\}^* \xrightarrow{\tau} \mathfrak{P}(\mathcal{F}[\mathcal{A}])$, so dass

- das Urbild der Formelmengen $\neq \emptyset$ ist ein gerader binärer Baum $\mathcal{B}(\tau)$;
- $\Gamma \subseteq \tau(\varepsilon)$;
- jede auftretende Formel $A \in \tau(w)$
  - gehört entweder zu Γ, falls $w = \varepsilon$,
  - oder ist Komponente einer der ersten vier Regeln mit Prämisse in $\tau(w)$,
  - oder ist Komponente einer der letzten drei Regeln mit Prämisse in $\tau(u)$ für ein echtes Präfix u von w.

Ein Ast Θ von $\mathcal{B}(\tau)$ (maximale lineare Präfix-geordnete Teilmenge) heißt

- vollständig, falls $\bigcup \tau[\Theta]$ bzgl. Regelanwendung invariant ist;
- abgeschlossen, falls $\bigcup \tau[\Theta]$ eine Formel und ihre Negation enthält; andernfalls heißt Θ offen.

Ein Tableau heißt abgeschlossen, falls jeder Ast abgeschlossen ist.

Die Existenz vollständiger Tableaus

Lemma

Jedes Tableau τ kann vervollständigt werden.

Beweis.

Setze $\tau_0 := \tau$ und definiere τ_{k+1} durch Anwendung einer passenden Regel auf jedes Nicht-Literal in τ_k. Dann gilt $\tau_k(w) \subseteq \tau_{k+1}(w)$ für alle $w \in \{0,1\}^*$ und $k \in \mathbb{N}$. Vereinigung liefert ein vollständiges Tableau τ_∞:

$$\tau_\infty(w) := \bigcup \{ \tau_k(w) \,:\, k \in \mathbb{N} \}$$

□

Korollar

Zu jeder Formelmenge Γ existiert ein vollständiges Tableau.

Beweis.

Starte mit $\gamma_0(\varepsilon) = \Gamma$ und $\gamma_0(w) = \emptyset$ für $w \in \{0,1\}^+$. □

Lemma (Hintikka)

Für vollständige Tableau-Astmengen gilt: „erfüllbar“=„offen“.

Beweis.

„$\subseteq$“ ist klar. Umgekehrt sei Θ offen. φ möge genau die Atome p mit $\neg p \in \bigcup \tau[\Theta]$ auf 0 abbilden. Induktion über die Länge der Formeln in $\bigcup \tau[\Theta]$ und die Abhängigkeit des Wahrheitswerts der Ursprungsformel von denen der Komponenten in den Regeln zeigt $\bigcup \tau[\Theta] \subseteq \hat{\varphi}^{-1}[\{1\}]$. □

Die ursprüngliche Tableau-Methode markiert Knoten nicht notwendig gerader binärer Bäume mit einzelnen Formeln, statt mit Formelmengen. Sie geht auf Beth[7] und (unabhängig) Hintikka[8] zurück (um 1955). Smullyans[9] Vereinfachung (1968, 1995) machte sie populär.

[7] Evert Willem Beth (1908–1964)
[8] Jaakko Hintikka (1929–2015)
[9] Raymond Merrill Smullyan (1919–2017)

Unerfüllbarkeit via Tableaus

Satz

Eine Formelmenge Γ ist genau dann unerfüllbar, wenn sie ein abgeschlossenes Tableau besitzt.

Beweis.

In einem vollständigen Tableau τ für Γ ist Γ in allen Astmengen enthalten. Damit sind diese unerfüllbar, und nach Hintikkas Lemma abgeschlossen.

Erfüllt φ umgekehrt Γ, so wegen der α-Regeln auch $\tau_\infty(\varepsilon)$ für jedes Tableau τ für Γ. **Ann.**: $\tau(w) \neq \emptyset$ und φ erfüllt $\bigcup\{\, \tau_\infty(u) : u \leq w \,\}$. Ist $\tau_\infty(wi)$, $i < 2$ leer, bestimmt w einen offenen Ast.
Sonst ist genau(!) je ein $A_i \in \tau_\infty(wi)$ Komponente einer β-Regel mit Prämisse in $\tau_\infty(u)$ für ein $u \leq w$. Also existiert $i < 2$ mit $\hat{\varphi}(A_i) = 1$.
Jedes Element von $\tau_\infty(wi)$ entsteht durch α-Regeln in endlich vielen Schritten aus A_i. Also erfüllt φ auch $\bigcup\{\, \tau_\infty(u) : u \leq wi \,\}$. Induktion über $|w|$ zeigt nun, dass nicht alle Äste von τ_∞ abgeschlossen sind. □

Algorithmus zur Konstruktion von Tableaus

Um für eine abzählbare Menge $\Gamma = \{ A_i : i \in \mathbb{N} \}$ ein Tableau zu konstruieren, dessen abgeschlossene Äste als solche markiert und dessen offene Äste vollständig sind, gibt es diverse Strategien, z.B.,

0. Für $\{ A_i : i < k \}$ sei υ_k ein nicht abgeschlossenes solches Tableau.
1. Konstruiere ein Tableau υ_{k+1} für $\{ A_i : i < k+1 \}$ wie folgt:
   - 1.0. Konstruiere ein Tableau σ_k für A_k in endlich vielen Schritten.
   - 1.1. Kombiniere υ_k und σ_k zu υ_{k+1}:
     - 1.1.0. Vereinige die Wurzelmengen:

$$\upsilon_{k+1}(\varepsilon) := \upsilon_k(\varepsilon) \cup \sigma_k(\varepsilon)$$

     - 1.1.1. Hänge die beiden Unterbäume von σ_k mit Wurzel 0 bzw. 1 an jedes Blatt eines offenen Asts von υ_k an: gilt $\upsilon_k(w) \neq \emptyset$ und $\upsilon_k(w0) = \emptyset$ und enthält der entsprechende Ast von υ_k keinen Widerspruch, setze für jedes nichtleere Binärwort $v \in \{0,1\}^+$

$$\upsilon_{k+1}(wv) := \sigma_k(v)$$

     - 1.1.2. Markiere neu entstandene abgeschlossene Äste.

Bemerkungen.

- Bei unerfüllbarem Γ terminiert der Algorithmus nach endlich vielen Schritten und liefert einen Beweis der Unerfüllbarkeit einer endlichen Teilmenge von Γ. Daraus folgt der Kompaktheitssatz für abzählbar unendliche Formelmengen Γ.
- Terminiert der Algorithmus nicht, so entsteht eine geordnete Kette von Tableaus, deren komponentenweise Vereinigung ein vollständiges Tableau für Γ ist.
- Man kann die zugrundeliegende Operation des obigen Algorithms als „Komposition“ von Tableaus auffassen, mit dem konstant leeren Tableau als neutralem Element; damit starten wir auch. Diese Komposition ist sicherlich nicht kommutativ, ob sie wirklich assoziativ ist, bleibt zu zeigen. Dass widersprüchlide Äste nicht weiter berücksichtigt werden, gedacht zur Steigerung der Effizienz, könnte evtl. Schwierigkeiten bereiten.

Normalformen

Oft lassen sich logische Probleme schneller lösen, wenn die Eingaben eine bestimmte einfache Gestalt haben; man spricht dann von Normalformen.

Dabei ist darauf zu achten, dass die Transformation von A nach $T(A)$ nicht zu teuer ist, hinsichtlich Zeit und Platz, sonst lohnt sich der Aufwand nicht. Prinzipiell unterscheidet man

- logisch äquivalente Transformationen mit $A \models\!\!\!\models T(A)$ von
- erfüllbarkeitsäquivalenten mit A erfüllbar gdw. $T(A)$ erfüllbar.

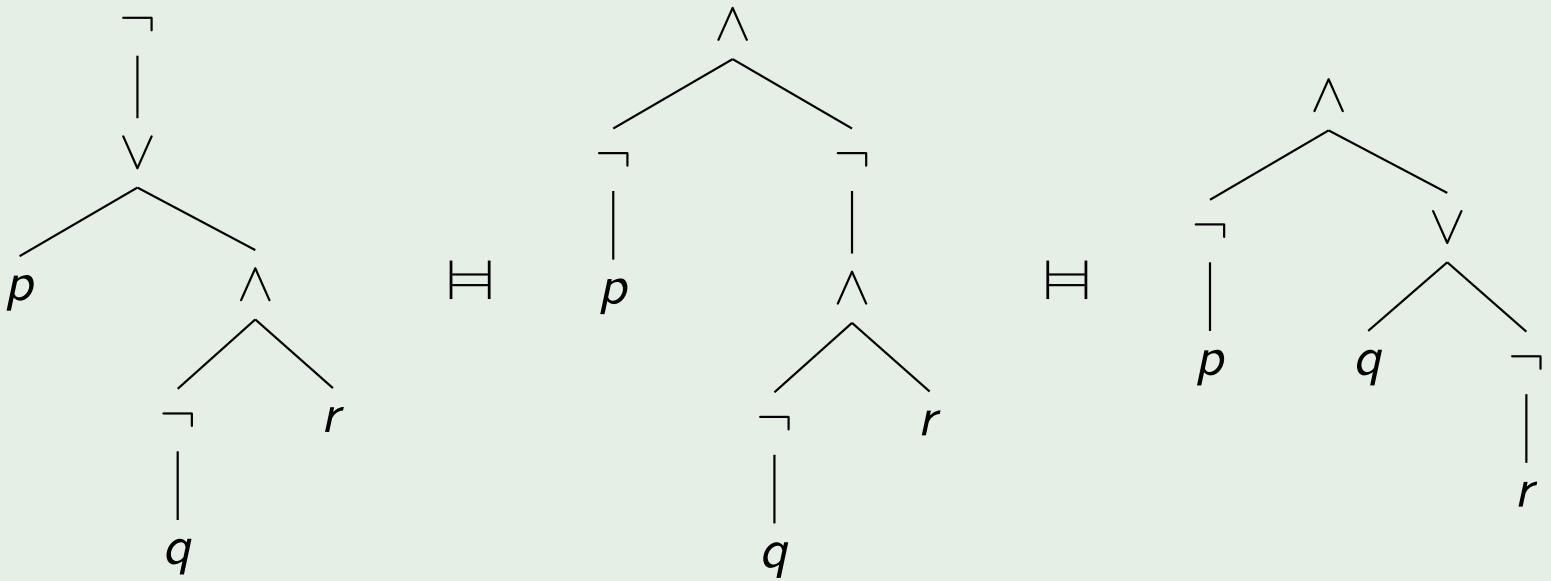
Wir werden uns im Folgenden auf die Junktorenmenge $\mathcal{J}_1 = \{\neg, \wedge, \vee\}$ beschränken. Der Begriff „Normalform“ ist insofern irreführend, als es keine universell beste/kleinste/einfachste Darstellung einer jeden Formel über $\mathcal{J}_1[\mathcal{A}]$ gibt. Unsere Normalformen sind immer auf die (algorithmische) Lösung eines bestimmten Problems zugeschnitten, vorzugsweise auf Anwendungen, wo ohnehin nur Eingaben in der passenden Form entstehen, oder diese leicht in die passenden From gebracht werden können.

Beispiel

Folgende Formeln lassen sich durch Anwendung der de Morgan'schen Regeln ineinander umformen; andere Rechenregeln sind nicht anwendbar:

$$\neg(A \vee (\neg B \wedge C)) \models\!\!\!\models \neg A \wedge \neg(\neg B \wedge C) \models\!\!\!\models \neg A \wedge (B \vee \neg C)$$

Die Syntaxbäume der äußeren Formeln haben 7 Knoten und 6 Kanten, unterscheiden sich aber in der Tiefe:



Die rechte Formel gehört denn auch zu KNF $\subseteq$ NNF , s.u.

NNF

Definition

NNF Die Teilmenge $\mathrm{NNF} \subseteq \mathcal{F}[\mathcal{A}]$ der Formeln in Negationsnormalform ist induktiv definiert durch

- $\mathcal{A} \cup \neg\mathcal{A} \subseteq \mathrm{NNF}$, d.h., alle Literale gehören zu NNF;
- NNF is unter Konjunktion ($\wedge$) und Disjunktion ($\vee$) abgeschlossen.

Für $A \in \mathrm{NNF}$ sei $\|A\|$ die Anzahl der Positionen, wo Literale auftreten.

Intuitiv sind alle Negationen so weit wie möglich „nach innen“ gezogen.

Das nächste Ergebnis ist eine Hausaufgabe:

Lemma

Zu jeder Formel $A \in \mathcal{F}[\mathcal{A}]$ existiert eine äquivalente Formel $B \in \mathrm{NNF}$, so dass die Länge $|B|$ in $\mathcal{Q}(|A|)$ liegt, d.h., bis auf eine Konstante linear von $|A|$ abhängt. □

KNF und DNF

Definition

- Eine Disjunktion von Literalen heißt Klausel. Man unterscheidet
  - positive/negative Klauseln, in denen alle Literale positiv/negativ sind;
  - Horn-Klauseln mit maximal einem positiven Literal;
  - k-Klauseln, wenn maximal k Literale auftreten; im Fall $k = 1$ spricht man auch von Unit-Klauseln.
- Eine Konjunktion von Klauseln heißt konjunktive Normalform (KNF), speziell k-KNF im Fall von k-Klauseln. Die entsprechenden Teilmengen von $\mathcal{F}_1[\mathcal{A}]$ bezeichnen wir ebenso, also k-KNF $\subseteq$ KNF $\subseteq$ NNF.

Definition

Vertauscht man in der obigen Definition die Rollen von Konjunktion ($\wedge$) und Disjunktion($\vee$), so erhält man die Begriffe der co-Klausel und der disjunktiven Normalform (DNF). Es gilt k-DNF $\subseteq$ DNF $\subseteq$ NNF.

Beispiel (alternative Mengendarstellung, nur für KNF!)

Die 2-KNF $A = (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee q)$ mit $\|A\| = 6$ hat folgende alternative Darstellung als Menge von Mengen von Literalen:

$$\{\{p, q\}, \{\{p, \neg q\}, \{\neg p, q\}\}$$

Lemma

Zu jeder Formel $A \in \mathcal{F}[\mathcal{A}]$ existiert eine äquivalente Formel $B \in KNF$, so dass $\|B\|$ in $\mathcal{Q}\left(2^{\|A\|}\right)$ liegt. □

Die obige Schranke ist strikt: es gibt eine Folge von Formeln A_n, $n \in \mathbb{N}$, mit $\|A_n\| = 2n$, so dass jede logisch äquivalente Formel B_n in KNF mindestens 2^n Positionen mit Literalen hat (HA). Die Länge der vollständig geklammerten Formeln eignet sich weniger für derartige Betrachtungen.

Duale Formeln und einfache Zusammenhänge

Definition

Die duale Formel zu $A \in \mathcal{F}_1[\mathcal{A}]$ ist gegeben durch

$$d(p) := p \text{ für } p \in \mathcal{A} \qquad d(B \wedge C) = d(B) \vee d(C)$$
$$d(\neg A) = \neg d(A) \qquad d(B \vee C) = d(B) \wedge d(C)$$

Lemma

- $A \in KNF$ *impliziert* $NNF(\neg A) \in DNF$
- $A \in KNF$ *genau dann wenn* $d(A) \in DNF$. □

Lemma

- $(1 - \varphi)(d(A)) = 1 - \varphi(A)$ *für jede Belegung* φ.
- A *ist eine Tautologie gdw.* $d(A)$ *ist widersprüchlich.*
- A *ist erfüllbar gdw.* $d(A)$ *ist keine Tautologie.* □

Davis-Putnam-Verfahren (für NNF)

Die Erfüllbarkeit einer Formel läßt sich statt mittels einer Wahrheitstabelle gezielter überprüfen, indem man bottom-up $\top$ oder $\bot$ für einzelne Variablen substituiert (Homomorphismus!, siehe Folie 16), was bei NNF-Formeln aufgrund der Rechenregeln für $\top$ und $\bot$ leicht zu vereinfachen ist und einen binären Formel-Baum liefert mit Blättern aus $\{\top, \bot\}$ liefert.

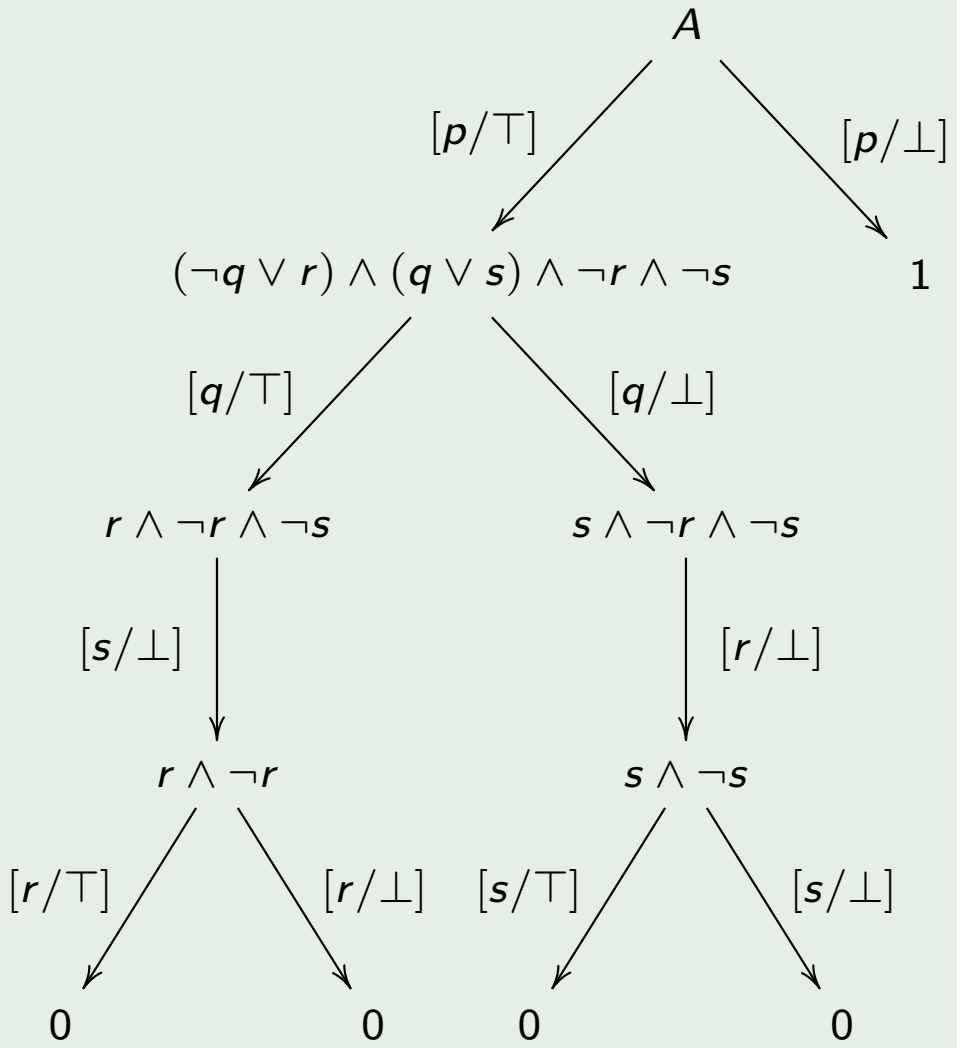
Lemma

$A \in NNF$ ist genau dann erfüllbar, wenn eine der Formeln $A[p/\top]$ und $A[p/\bot]$ äquivalent zu einer erfüllbaren Formel ist. □

Algorithmen, die diese Idee umsetzen und mit Heuristiken weiter verfeinern, sind als Davis[10]-Putnam[11]-Verfahren bekannt. Das ursprüngliche Verfahren wurde 1960 veröffentlicht, und noch heute kommen seine Varianten in den schnellsten SAT-Solvern zur Anwendung.

[10] Martin Davis (*1928)
[11] Hilary Whitehall Putnam (1926-2016)

Beispiel ($\neg p \vee ((\neg q \vee r) \wedge (q \vee s) \wedge \neg r \wedge \neg s \wedge (p \vee q)) = A$)



Damit erfüllt jede Belegung mit $\varphi(p) = 1$ die Formel A.

Regel-baserte Definition von Davis-Putnam

(0) keine Verzweigungen:

- Unit-Regel: hat A die Form $p \wedge B$ oder $\neg p \wedge B$ für ein Atom p, oder
- Pure-Literal Regel: tritt $p \in V$ in A nur positiv oder nur negativ auf,

wende nur $[p/\top]$ bzw. $[p/\bot]$ an; dann ist A erfüllbarkeitsäquivalent zum Substitut (im ersten Fall zu B).

(1) Splitting-Regel: sonst wende beide Substitutionen an (siehe Lemma).

Im Fall von KNF-Formeln greifen eine weitere Vereinfachung:

Lemma

- *Sind $K \subseteq L$ Klauseln („K subsumiert L“), so gilt $K \models\!\models K \wedge L$.*
- *Enthält die Klausel K komplementäre Literale, so gilt $K \models\!\models \top$.* □

Das rechtfertigt das Entfernen von subsumierten und tautologischen Klauseln aus einer KNF.

Auswahlkriterien für die Splitting-Regel

Bei der Splitting Regel ist der „Preis“ für den Prozess der Auswahl des Atoms abzuwägen gegen die zu erwartende Vereinfachung beim restlichen Verfahren. Mögliche Auswahlkriterien sind etwa

- das erste vorkommende Atom (keine Auswahlkosten);
- ein am häufigsten vorkommendes Atom;
- ein Atom p mit $\sum_{p \in K_i} |K_i|$ minimal;
- ein Atom p, das in den „kurzen“ Klauseln am häufigsten vorkommt; (braucht eine explizite Schranke, ab wann eine Klausel als „kurz“ gilt);
- ein Atom, bei dem die Differenz zwischen positiven und negativen Auftreten in den „kurzen“ Klauseln maximal ist.

Konkrete Implementierungen können weitere Heuristiken verwenden.

Resolventen-Methode (für KNF, in Mengenschreibweise)

Satz (Resolutionslemma)

Sind K *und* K' *Klauseln und ist* X *ein Literal mit* $X \in K$ *und* $\neg X \in K'$, *so erfüllt die sog. Resolvente* $L := (K - X) \cup (K' - \neg X)$,

$$K \wedge K' \models L \quad \textit{und damit} \quad K \wedge K' \rightleftharpoons K \wedge K' \wedge L \qquad \square$$

Daraus gewinnt man einen Resolutions- oder R-Kalkül wie folgt:

Definition

Unter einer R-Herleitung einer Klausel K aus $A \in \mathrm{KNF}$, geschrieben $A \vdash_{\mathrm{res}} K$, versteht man eine Klausel-Folge K_i, $i < n$, mit

- $K_{n-1} = K$;
- für $i < n$ gilt
  - entweder $K_i \in A$,
  - oder K_i ist Resolvente von K_j und K_k mit $j, k < i$.

Satz

Der R-Kalkül ist korrekt aber nicht vollständig, d.h.,

$$A \vdash_{res} K \quad \textit{impliziert} \quad A \models K$$

aber nicht notwendig umgekehrt.

Beweis.

Die Korrektheit folgt aus dem Resolutionslemma, während $p \wedge (p \vee q) \models p$ zeigt, dass der R-Kalkül nicht vollständig ist. $\square$

Satz (Widerlegungsvollständig- und Korrektheit, Robinson)

$A \in KNF$ *ist genau dann unerfüllbar, wenn* $A \vdash_{res} \emptyset$ *.*

Beweis.

Tritt $\emptyset$ als Resolvente auf, gilt nach Resolutionslemma $A \models\!\!\models A \wedge \bot \models\!\!\models \bot$.

Beweis, Fortsetzung.

Sei A unerfüllbar. Betrachte die Anzahl k verschiedener Literale in A.

$k = 0$: Dann gilt $A = \emptyset$.

Annahme: Die Behauptung stimmt für alle $i < k$.

$k > 0$: OBdA enthalte A keine tautologischen oder subsumierten Klauseln. In A tritt ein Atom p positiv und negativ auf, sonst wäre A erfüllbar.

A_+ enthalte alle A-Klauseln, in denen p auftritt;

A_- enthalte alle A-Klauseln, in dene $\neg p$ auftritt;

A_* enthalte alle A-Klauseln, in denen weder p noch $\neg p$ auftritt.

Wegen $A = A_+ \cup A_- \cup A_*$ folgt aus der Unerfüllbarkeit einer oder der Vereinigung zweier dieser Klauselmengen nach Annahme die Behauptung.

Andernfalls sind $A_+ \cup A_*$ und $A_- \cup A_*$ erfüllbar, aber nicht von derselben Belegung.

Behauptung: $A_+ \cup A_* \vdash_{\text{res}} \{p\}$ und $A_- \cup A_* \vdash_{\text{res}} \{\neg p\}$

Beweis, Fortsetzung.

Betrachte $\tilde{A}_+ := \{ K - \{p\} : K \in A_+ \}$.

Anname: $\tilde{A}_+ \cup A_*$ wird von φ erfüllt. Dann gilt oBdA $\varphi(p) = 0$ und folglich werden $A_+ \cup A_*$ wie auch $A_- \cup A_*$ von φ erfüllt, Widerspruch.

Also gilt $\tilde{A}_+ \cup A_* \vdash_{\mathsf{res}} \emptyset$, etwa mittels der R-Herleitung J_r, $r < t$ minimaler Länge. Da A_* nach Voraussetzung erfüllbar ist, garantiert die Minimalität, dass immer wenn J_s Resolvente von Klauseln J_p und J_q mit $p, q < r$ sind, mindestens eine der Klauseln zu $\tilde{A}_+$ gehört. Dann liefert

$$J'_r := \begin{cases} J_r \cup \{p\} & \text{falls } J_r \in A_+ \\ J_r & \text{sonst} \end{cases}$$

eine R-Herleitung von $\{p\}$ aus $A_+ \cup A_*$. Analog gilt $A_- \cup A_* \vdash_{\mathsf{res}} \{\neg p\}$. Beides zusammen impliziert $A \vdash_{\mathsf{res}} \emptyset$. □

Resolutions-Heutistiken

Definition

Für $A \in \mathrm{KNF}$ bezeichnet $\mathbf{Res}(A)$ die Menge aller Klauseln, die in endlich vielen Schritten als Resolventen aus den Klauseln von A konstruierbar sind.

Ein naiver Algorithmus basiert auf der Tatsache, dass $A \in \mathrm{KNF}$ genau dann erfüllbar ist, wenn $\emptyset \in \mathbf{Res}(A)$ gilt. Dies wird nicht empfohlen.

Stattdessen kann man sich auf starkte Herleitungen beschränken, in denen

- keine Klausel mehrfach auftritt;
- keine tautologischen Klauseln auftreten;
- keine Klauseln von Vorgängern subsumiert werden.

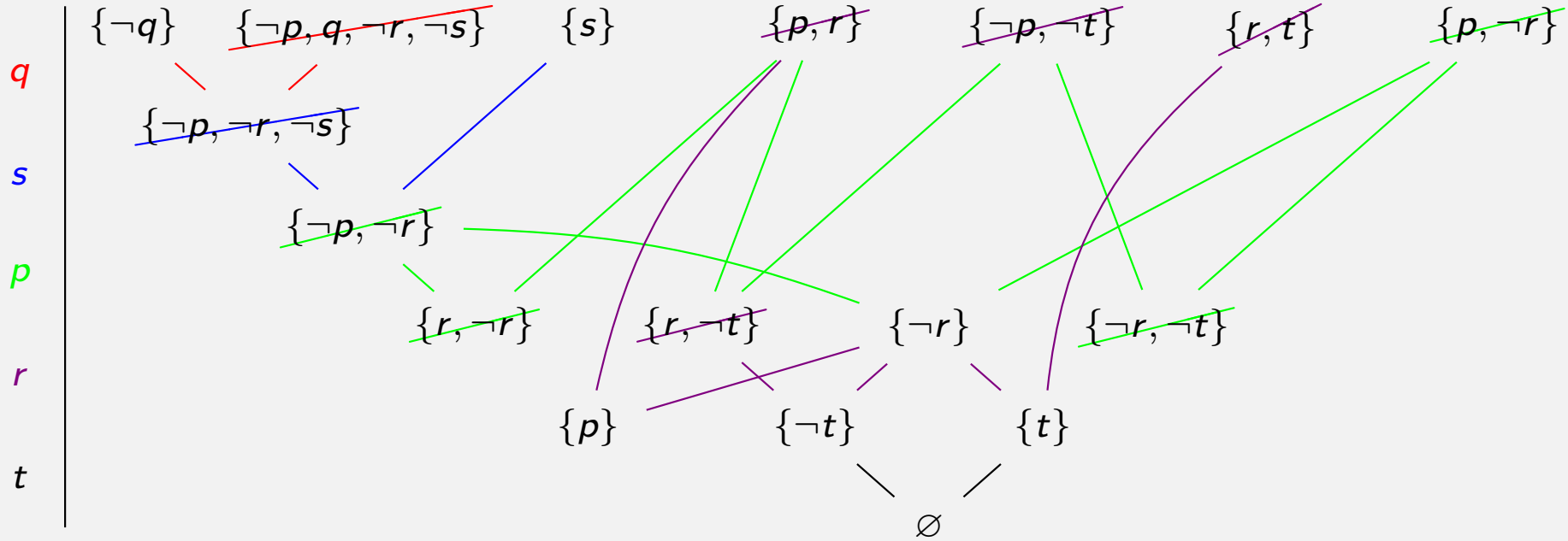
Dies erlaubt es, aus $\mathbf{Res}(A)$ bestimmte Klauseln zu enfernen und mit einer potentiell kleineren Menge $\mathbf{Res}'(A)$ zu arbeiten.

Zur Handrechnung ziehen wir ein systematisches graphisches Verfahren vor:

Bevorzugtes Verfahren zur Handrechnung mit Beispiel

$A = \{\{\neg q\}, \{\neg p, q, \neg r, \neg s\}, \{s\}, \{p, r\}, \{\neg p, \neg t\}, \{r, t\}, \{p, \neg r\}\}$

- Ordne die auftretenden Atome (beliebig) linear an;
- konstruiere schichtweise alle Resolventen bzgl. des jeweils aktuellen Atoms; streiche dabei so früh wie möglich entstehende tautologische oder subsumierte Formeln;



R-Herleitung: $\{p, r\}, \{\neg p, \neg t\}, \{r, t\}, \{r, \neg t\}, \{\neg r\}, \{t\}, \{\neg t\}, \emptyset$.

Zur Übung möge man eine andere Reihenfolge der Atome ausprobieren!

Bemerkungen

- Das Berechnen des Resolutionsabschlusses $\mathbf{Res}(A)$ (außer tautologischen Klauseln) ist unter dem Namen Stufenstrategie bekannt. Sofern $\emptyset$ nicht auftritt kann man sämtliche erfüllenden Belegungen bestimmen. (Für Handrechnung zu fehleranfällig.)
- Bei der sog. Stützmengenrestriktion werden Unit-Klauseln bevorzugt zur Resolventenbildung herangezogen.
- Bei P- bzw. N-Resolution sollte eine der beteiligten Klauseln nur positive (negative) Literale enthalten.
- Zumindest für Formeln in 2-KNF unf für Horn-Formeln (mit höchstens einem positiven Literal pro Klausel) ist die Resolution effizient. I.A. ist das nicht der Fall:

Resolution ist i.A. nicht effizient

Satz

Es gibt eine Folge $\emptyset \neq A_k \in KNF$, $k \in \mathbb{N}$, *mit folgenden Eigenschaften:*

- *in* A_k *kommen höchstens die Atome* p_i, $i < 2k+1$ *vor;*
- A_k *hat* $k+1$ *Klauseln;*
- *keine der* $2^{k+1}-1$ *Klauseln in* $\mathbf{Res}(A_k)$ *subsumiert eine andere.*

Beweis.

$k = 0$: $A_0 = p_0$ hat $2^0 - 1 = 0$ binäre Resolventen.

Annahme: $A_k = \bigwedge_{i<k+1} K_{k,i}$ habe die gewünschten Eigenschaften.

$k+1$: $A_{k+1} := \mathrm{KNF}(A_k \vee q_{2k}) \wedge (\neg q_{2k} \vee q_{2k+1})$ hat zwei Atome und eine Klausel mehr als A_k, und $\mathbf{Res}(A_{k+1})$ hat alle um p_{2k} bzw. p_{2k-1} vergrößerten Resolventen von A_k, sowie $\{\neg p_{2k}, p_{2k-1}\}$. Dabei entstehen keine neuen Mengeninklusionen. □

Teil 2
Prädikatenlogik

(1. Stufe mit Gleichheit)

Kapitel 6
Motivation und Überblick

Defizite der Aussagenlogik

- Die Aussagenlogik ist universell anwendbar, wo potentiell wahre oder falsche Aussagen formuliert und miteinander kombiniert werden können, sei es die Herstellung von Würstchen oder die Theorie der Quantengraviation. Ihre recht einfache mathematische Struktur ist Konsequenz dieser beschränkten Ausdrucksfähigkeit.
- So ist die AL nicht in der Lage, Aussagen über die Elemente einer spezifischen (nichtleeren) Datenbereiches zu formulieren, z.B. die natürlichen Zahlen, gerichtete Graphen oder Datenbanken.
- Dazu bedarf es der Prädikatenlogik (der ersten Stufe), die sich an die Gegebenheiten der Datenbereiche von Interesse anpassen läßt und dann viel ausdrucksstärker ist als die Aussagenlogik.

Semantisches Ziel

Datenbereiche in Anwendungen sind üblicherweise Mengen D mit einer „inneren Struktur“, die sich in gewissen Funktionen $D^n \xrightarrow{f} D$ und gewissen Prädikaten $D^n \xrightarrow{R} \mathbb{B}$, oder äquivlalent, Teilmengen $R \subseteq D^n$ manifestiert.

Die Anwendungen bedienen sich dieser Struktur, z.B. bei

- Lösung von Anfragen auf Datenmengen in der KI oder in Informationssystemen;
- Formulierung von Integritätsbedingungen auf Daten: Schleifeninvarianten eines Programms, Constraints auf XML-Dateien oder Datenbankeinträgen;
- Lösung von Constraint-Systemen beim Testen oder Planen.
- Logischem Programmieren.

Syntax, Übersicht

Frege[12] definierte 1879 die Syntax der PL in seiner „Begriffsschrift – Eine der arithmetischen nachgebildete Formelsprache des reinen Denkens“.

In moderner Terminologie:

- Man fasst formale Funktions- und Relationssymbole der gewünschten Zahl und Stelligkeit in einer Signatur $\mathcal{S} = \langle \mathbf{Fun}, \mathbf{Pred} \rangle$ zusammen;
- über einer (abzählbaren) Menge $\mathcal{V}$ von Variablen baut man in einem 1. Schritt Terme in den Funktionssymbolen auf und erhält einen abstrakten Datenbereich $\mathbf{Term}(\mathbf{Fun}, \mathcal{V})$ (vergl. Folie 12, Rekursionssatz!);
- 2. Schritt: Prädikate mit Termen als Eingaben sowie formale Gleichungen zwischen Termen bilden nun die atomare Formeln $\mathcal{A}(\mathcal{S})$;
- Die bekannten Junktoren der Aussagenlogik und zwei unäre Junktoren: $\forall x$ („für alle x“) und $\exists x$ („es gibt ein x“) für jede Variable x, liefern die Menge $\mathbf{FO}(\mathcal{S})$ aller Formeln; $\forall$ und $\exists$ heißen Quantoren.

[12] Friedrich Ludwig Gottlob Frege (1848–1925)

Semantik, Übersicht

Die Semantik wurde erst 1934 von Tarski[13] entwickelt.

In moderner Terminologie:

- Eine $\mathcal{S}$-Struktur $\mathcal{M} = \langle D, I \rangle$ interpretiert $\mathcal{S}$ in einer Trägermenge;
- Jede Belegung $\mathcal{V} \xrightarrow{\sigma} D$ der Variablen liefert einen eindeutigen **Fun**-Homomorphismus $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \xrightarrow{\hat{\sigma}} \langle D, I_{\mathbf{Fun}} \rangle$;
- Alle atomaren Formeln in den Symbolen von **Pred** und der formalen Gleichheit $\doteq$ erhalten aufgrund von $\hat{\sigma}$ und $I_{\mathbf{Pred}}$ Wahrheitswerte zugewiesen; dies entspricht den Belegungen $\mathcal{A} \xrightarrow{\varphi} \mathbb{B}$ in der AL.
- Diese Belegung der atomaren Formeln läßt sich wieder eindeutig zu einer Bewertung aller Formeln $F \in \mathbf{FO}(\mathcal{S})$ fortsetzen, in Analogie zu $\mathcal{F}[\mathcal{A}] \xrightarrow{\hat{\varphi}} \mathbb{B}$.
- Mit einem Trick lassen sich die Semantiken für Terme und Formeln in eine ähnliche Form bringen.

[13] Alfred Tarski bzw. ursprünglich Alfred Tajtelbaum, 1901 – 1983)

Beschreibung mathematischer Beziehungen

Beispiel

Syntax: Konstanten 1, 2, 3; 2-stellige Funktionssymbole $+$, $/$; 2-stelliges Prädikat $<$:

$$\text{Signatur} \quad \mathcal{S} = \langle \{1_{/0}, 2_{/0}, 3_{/0}, +_{/2}, /_{/2}\}, \{<_{/2}\} \rangle$$

$$\text{Terme} \quad 1 \quad , \quad 1 + 2/3 \quad , \quad x + 3/2$$

Logik: Junktoren $\rightarrow$, $\wedge$, Quantoren $\forall$, $\exists$;

$$\text{Formeln} \quad x < 3 \quad , \quad \forall x \, \forall y \; (x < y \rightarrow \exists z \, (x < z \wedge z < y))$$

Semantik: Datenbereich $D = \mathbb{Q}$, Konstante 1 bis Prädikat $<$ mit der üblichen Bedeutung.

Achtung: Andere Interpretationen der formalen Symbole in $\mathcal{S}$ sind möglich und dürfen nicht ignoriert werden!

Beschreibung von Beziehungen zwischen Daten

Beispiel

Syntax: Funktion *WeiteDerReise*(-), Prädikate *istHund*(-), *istFisch*(-), $<_{/2}$
Logik: Junktoren $\rightarrow$, $\wedge$, Quantoren $\forall$;
typische Formel:

$$\forall x \forall y (\mathit{istHund}(x) \wedge \mathit{istFisch}(y) \rightarrow \mathit{WeiteDerReise}(x) < \mathit{WeiteDerReise}(y))$$

Semantik: Datenbereich $D = \{\text{Lassie}, \text{Nemo}\} \cup \mathbb{N} \cup \{\perp\!\!\!\perp\}$

Die Standard-Interpretation der Funktion *WeiteDerReise*(-) liefert die Weite er Reise, die das Tier im Argument zurückgelegt hat. oder $\perp\!\!\!\perp$ sonst.

istHund und *istFisch* möge die charakteristische Funktion von $\{\text{Lassie}\}$ bzw. $\{\text{Nemo}\}$ sein.

Kapitel 7
Syntax der Prädikatenlogik

Syntax der Prädikatenlogik

Gegeben seien zwei entscheidbare aber nicht notwendig endliche Mengen **Fun** und **Pred**, die zum Alphabet der Aussagenlogik disjunkt sind, und eine Signatur

$$\mathcal{S} := \mathbf{Fun} + \mathbf{Pred} \xrightarrow{\mathbf{ar}} \mathbb{N}$$

Wir wollen die Elemente aus **Fun** als Funktionensymbole interpretieren, und die Elemente aus **Pred** as Prädikatssymbole.

Üblicherweise verwenden wir Kleinbuchstagben f, g, $h \ldots$ für erstere, und Großbuchstaben R, S, $T \ldots$ für letztere.

$f_{/k}$ und $R_{/k}$ ist Kurzschreibweise für $\mathbf{ar}(f) = k$ bzw. $\mathbf{ar}(R) = k$.

0-stellige Funktionssymbole heißen auch Konstanten, und 0-stellige Prädikatssymbole Propositionen.

Weiter sei $\mathcal{V}$ eine (abzählbare entscheidbare) Menge von Variablen.

Aufbau der Formeln in drei Schritten

- Zuerst bilden wir, wie auf Folie 12, die Termalgebra $\mathbf{Term}(\mathbf{Fun}, \mathcal{V})$, allerdings nur bzgl. der Funktionssymbole:

$$t ::= v \mid f(t_0, \ldots, t_{\mathbf{ar}(f)-1}) \quad \text{mit} \quad v \in \mathcal{V} \quad \text{und} \quad f \in \mathbf{Fun}$$

- Danach bilden wir die Menge $\mathbf{Atm} = \mathbf{Atm}(\mathbf{Pred}, \mathbf{Term}(\mathbf{Fun}, \mathcal{V}))$ der atomaren Formeln (mit Gleichheit):

$$A ::= t_0 \doteq t_1 \mid R(t_0, \ldots, t_{\mathbf{ar}(f)-1}) \quad \text{mit} \quad R \in \mathbf{Pred}$$

- Und schließlich bilden wir mit Hilfe der um $\forall x_{/1}$ und $\exists x_{/1}$, $x \in \mathcal{V}$, erweiterten Junktormenge $\mathcal{J}$ die Termalgebra $\mathbf{FO}(\mathcal{S})$ der prädikatenlogischen Formeln erster Stufe (first order formulae):

$$F ::= A \mid \top \mid \bot \mid \neg F \mid (F_0 \star F_1) \mid (\forall x\, F) \mid (\exists x\, F)$$

mit $A \in \mathbf{Atm}$, $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ und $x \in \mathcal{V}$.

Gebundene und freie Variablen

Als einstellige Junktoren binden $\forall x$ und $\exists x$ stärker als alle 2-stelligen.

Definition

Die Menge $\mathbf{V}(t)$ der in einem Term t auftretenden Variablen ist

$$\mathbf{V}(x) = \{x\} \quad \text{und} \quad \mathbf{V}(f(t_0, \ldots, t_{\mathbf{ar}(t)-1})) = \bigcup \{\, V(t_i) \,:\, i < \mathbf{ar}(f) \,\}$$

Analog sind die in einer (atomaren) Formel auftretenden Variablen definiert.

In $(\mathcal{Q}x\, F)$ ist F der Geltungsbereich für $\mathcal{Q}x$; jedes Auftreten von x in einem solchen Geltungsbereich heißt gebunden, außerhalb jedes solchen Geltungsbereichs frei. Die Menge der gebunden/frei auftretenden Variablen in $H \in \mathbf{FO}(\mathcal{S})$ wird mit $\mathbf{GV}(H)$ bzw. $\mathbf{GV}(H)$ bezeichnet; sie brauchen nicht disjunkt zu sein!

Formeln ohne frei vorkommende Variablen heißen abgeschlossen.

Anmerkungen

Der Begriff der Entscheidbarkeit einer Menge wird erst in TheoInf2 offiziell eingeführt. Informell soll er hier bedeuten, dass wir ihre Elemente effizient, d.h., mit geringem Rechenaufwand oder sogar unmittelbar erkennen können.

Lemma

- *Die Entscheidbarkeit der Signatur $\mathcal{S}$ und der Variablenmenge $\mathcal{V}$ vererbt sich auf die Mengen der Terme und der (atomaren) Formeln.*
- *Zusammenesetzte Terme und Formeln lassen sich eindeutig zerlegen.*
- *Gebundene und freie Vorkommen von Variablen lassen sich effizient bestimmen.*

Kapitel 8
Semantik der Prädikatenlogik

$\mathcal{S}$-Strukturen

Das Ziel ist die Beschreibung von Beziehungen zwischen Elementen eines konkreten strukturierten Datenbereichs D.

Dafür war eine passende Signatur $\mathcal{S} = \mathbf{Fun} + \mathbf{Pred}$ gewählt worden, evtl. mit suggestiven Namen für die Funktionen- bzw. Prädikatensymbole.

Bei der Definition einer Semantik für die Formeln in $\mathbf{FO}(\mathcal{S})$ ist aber darauf zu achten, dass D evtl. nur einer von vielen möglichen Datenbereichen ist, der zur gewählten Signatur passt.

Definition

Unter einer $\mathcal{S}$-Struktur $\mathcal{M} = \langle D, I \rangle$ versteht man eine Menge D, den Datenbereich zusammen mit einer Interpretation der Symbole in $\mathcal{S}$

$$D^{\mathbf{ar}(f)} \xrightarrow{I(f)} D \text{ für } f \in \mathbf{Fun} \quad \text{und} \quad D^{\mathbf{ar}(R)} \xrightarrow{I(R)} \mathbb{B} \text{ für } R \in \mathbf{Pred}$$

Oft schreibt man $f^{\mathcal{M}}$ und $R^{\mathcal{M}}$ statt $I(f)$ bzw. $I(R)$.

Belegungen, Semantik der Terme

In der AL konnte die Menge $\mathcal{A}$ der atomaren Formeln direkt mit Wahrheitswerten belegt werden. In der PL gelingt das nur indirekt. Dennoch wollen wir versuchen möglichst viel von der AL zu übernehmen.

Definition

Eine Belegung der Variablen in einer $\mathcal{S}$-Struktur $\mathcal{M}\langle D, I\rangle$ ist eine Abbildung $\mathcal{V} \xrightarrow{\sigma} D$.

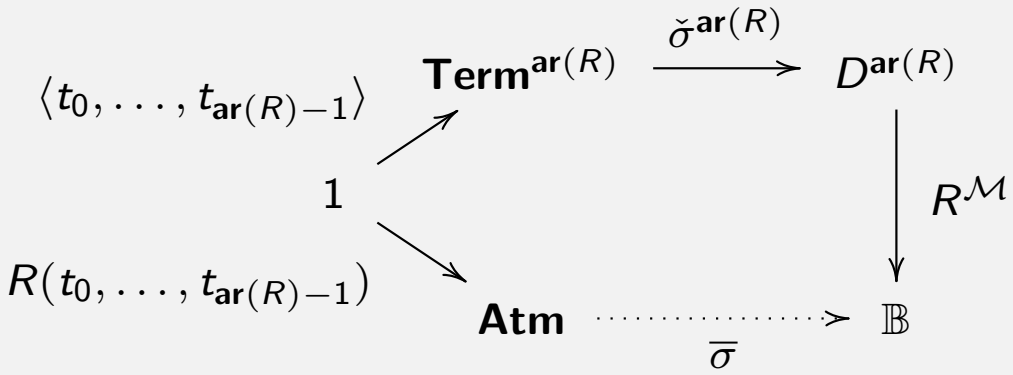
Aufgrund des Rekursionssatzes (Folie 12) lässt sich solch eine Belegung σ eindeutig zu einem $\mathbf{Fun}$-Homomorphismus $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \xrightarrow{\check{\sigma}} \langle D, I_{\mathbf{Fun}}\rangle$ fortsetzen, der Semantik der Terme bzgl. $\sigma \in D^{\mathcal{V}}$.

Daraus gewinnen wir auf kanonische Weise die Semantik der atomaren Formeln bzgl. σ als Abbildung $\mathbf{Atm}(\mathbf{Pred}, \mathbf{Term}(\mathbf{Fun}, \mathcal{V})) \xrightarrow{\overline{\sigma}} \mathbb{B}$, die auf verschiedene Weise beschrieben werden kann:

Semantik atomarer Formeln

Achtung: die formale Gleichheit $\doteq_{/2}$ gehört hier nicht zu **Pred**, sondern gilt als logisches Symbol, das immer als tatsächliche Gleichheit bzw. als deren charakteristische Funktion zu interpretieren ist.

$R \in \mathbf{Pred} + \{\doteq\}$ und $t_i \in \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$, $i < \mathbf{ar}(R)$ ergibt in Diagramm-Form



oder mit Teilmengen $R^{\mathcal{M}}$ anstelle von charakteristischen Funktionen:

$$\overline{\sigma}(t_0 \doteq t_1) = 1 \text{ gdw } \check{\sigma}(t_0) = \check{\sigma}(t_1)$$

$$\overline{\sigma}(R(t_0, \ldots, t_{\mathbf{ar}(R)-1})) = 1 \text{ gdw } \langle \check{\sigma}(t_0), \ldots, \check{\sigma}(t_{\mathbf{ar}(R)-1}) \rangle \in R^{\mathcal{M}} \subseteq D^{\mathbf{ar}(R)}$$

Semantik von Formeln

Schließlich können wir den Rekursionssatz ein weiteres Mal anwenden und $\mathbf{Atm}(\mathbf{Pred}, \mathbf{Term}(\mathbf{Fun}, \mathcal{V})) \xrightarrow{\overline{\sigma}} \mathbb{B}$ eindeutig zu einem Homomorphismus $\mathbf{FO}(\mathcal{S}) \xrightarrow{\hat{\sigma}} \mathbb{B}$ bzgl. der Signatur $\mathcal{J} + (\{\forall, \exists\} \times \mathcal{V})_{/1}$ fortsetzen, indem wir die Junktoren in $\mathcal{J}$ ebenso wie auf Folie 19 behandeln. Weiter gilt:

Definition

Jedes $\sigma \in D^{\mathcal{V}}$ hat Modifikationen $\sigma\{x/d\}$ [a], $\langle x, d\rangle \in \mathcal{V} \times D$,

$$\sigma\{x/d\}(y) := \begin{cases} d & \text{falls } y = x \\ \sigma(y) & \text{sonst} \end{cases}$$

die es erlauben, die Semantik quantifizierter Formeln zu formulieren:

$$\hat{\sigma}(\forall x\, A) := \inf\{\, \widehat{\sigma\{x/d\}}(A) \,:\, d \in D \,\}$$

$$\hat{\sigma}(\exists x\, A) := \sup\{\, \widehat{\sigma\{x/d\}}(A) \,:\, d \in D \,\}$$

[a] Beachte die Reihenfolge! Der Operator steht rechts.

Alternative Sicht auf die Semantik der Terme

Die Semantik der Terme, aufgefasst als durch σ parametrisierte Familie von Funktionen

$$D^{\mathcal{V}} \longrightarrow \mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \longrightarrow D \quad , \quad \sigma \longmapsto \check{\sigma}$$

lässt sich in eine (Auswertungs-)Funktion mit zwei Argumenten umwandeln

$$\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \times D^{\mathcal{V}} \xrightarrow{\mathcal{M}[\![-]\!](-)} D, \quad , \quad \langle t, \sigma \rangle \longmapsto \check{\sigma}(t)$$

ein Verfahren, das als uncurrying[14] bekannt ist. Aufgrund der Symmetrie des cartesischen Produkts erhalten wir mittels currying eine durch Terme parametrisierte Familie

$$\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \longrightarrow D^{\mathcal{V}} \longrightarrow D \ , \ t \longmapsto \mathcal{M}[\![t]\!] \ , \ \sigma \longmapsto \mathcal{M}[\![t]\!](\sigma) := \check{\sigma}(t)$$

die ebenfalls Semantik der Terme genannt wird.

[14] nach Haskell Brooks Curry (1900-1982)

Alternative Sicht auf die Semantik der Formeln

Die durch $\sigma \in D^{\mathcal{V}}$ parametrisierte Familie von Abbildungen

$$D^{\mathcal{V}} \longrightarrow \mathbf{FO}(\mathcal{S}) \longrightarrow \mathbb{B} \quad , \quad \sigma \longmapsto \hat{\sigma}$$

hat nach einem analogen uncurry-curry-Trick die Form

$$\mathbf{FO}(\mathcal{S}) \longrightarrow D^{\mathcal{V}} \longrightarrow \mathbb{B} \quad , \quad A \longmapsto \mathcal{M}[\![A]\!] \quad , \quad \sigma \longmapsto \mathcal{M}[\![A]\!](\sigma) = \hat{\sigma}(A)$$

Diese Variante der Semantik der Formeln hat eine zur obigen Semantik der Terme ähnliche Form. Ob diese Sichtweise der Semantik tiefere Einsichten beschert, bleibt abzuwarten. Der notationelle Aufwand erscheint zunächst disproportional hoch, aber man muß diese Notation (auch) beherrschen.
Vorteil: bei geschlossenen Formeln kann man das Argument σ weglassen.

Die Semantik-Klammern $[\![\cdot]\!]$ gehen wohl auf die denotationellen Semantik (Scott, Strachey 1971) zurück, und haben seither in vielen Bereichen der formalen Semantik, wie auch der formalen Linguistik Verbreitung gefunden.

Semantik und freie Variable

In der AL konnte die Bewertung $\hat{\varphi}(B)$ einer Formel B nur von den Werten $\varphi(p)$ derjenigen Atome abhängen, die in B vorkamen.

Entsprechend kann in der PL die Semantik $\mathcal{M}[\![A]\!](\sigma) = \hat{\sigma}(A)$ nur von den Werten der in A auftretenden atomaren Formeln abhängen, und somit nur von den σ-Werten der darin vorkommenden Variablen.

Gebundene Auftreten von Variablen nehmen dabei keinen Einfluss; daher können gebundene Variablen auch umbenannt werden, siehe Folie 127:

Lemma (Koinzidenzlemma)

Ist A eine prädikatenlogische Formel über der Signatur $\mathcal{S}$ und $\mathcal{M} = \langle D, I \rangle$ eine $\mathcal{S}$-Struktur, so gilt für alle Belegungen $\sigma, \tau \in D^{\mathcal{V}}$ mit $\sigma(x) = \tau(x)$ für alle $x \in \mathbf{FV}(A)$:

$$\mathcal{M}[\![A]\!](\sigma) = \mathcal{M}[\![A]\!](\tau) \qquad \textit{bzw.} \qquad \hat{\sigma}(A) = \hat{\tau}(A) \qquad \square$$

Erfüllbar- und Allgemeingültigkeit, logische Folgerung $\models$

Definition (vergl. Folie 22)

- Die durch $\mathcal{M}[\![A]\!](\sigma) = 1$ (A gilt in $\mathcal{M}$ unter σ) spezifizierte Relation zwischen Tripeln $\langle D, I, \sigma \in D^{\mathcal{V}} \rangle$ und Formeln A induziert einen ▸ Hüllenoperator $(\ )^{\models}$ auf $P(\mathbf{FO}(\mathcal{S}))$. Schreib- bzw. Sprechweise: $\Gamma \models A$ für $A \in \Gamma^{\models}$; A folgt logisch aus der Menge Γ der Prämissen.
- Ist A geschlossen, so ist die Belegung der Variablen irrelevant; statt zu sagen „ A gilt in $\mathcal{M}$ für jedes σ “, nennt man $\mathcal{M}$ ein Modell für A.
- $A \in \mathbf{FO}(\mathcal{S})$ ($\Gamma \subseteq \mathbf{FO}(\mathcal{S})$) heißt erfüllbar, wenn es eine $\mathcal{S}$-Struktur $\mathcal{M} = \langle D, I \rangle$ und eine Belegung $\sigma \in D^{\mathcal{V}}$ gibt mit so dass A (jedes $A \in \Gamma$) in $\mathcal{M}$ unter σ gilt.
- A heißt allgemeingültig oder Tautologie, geschrieben $\models A$, falls A in jeder $\mathcal{S}$-Struktur $\mathcal{M}$ unter allen Belegungen σ gilt.

Die Tripel $\langle D, I, \sigma \in D^{\mathcal{V}} \rangle$ entsprechen den Belegungen $\varphi \in \mathbb{B}^{\mathcal{A}}$ der AL.

Irritierender Gebrauch des Symbols $\models$

Der Sachverhalt A gilt in $\mathcal{M}$ unter σ, also $\mathcal{M}[\![A]\!](\sigma) = 1$, oder einfacher $\hat{\sigma}(A) = 1$ wird häufig durch

$$\mathcal{M}, \sigma \models A \quad \text{bzw.} \quad \mathcal{M} \models A \text{ falls } A \text{ abgeschlossen}$$

ausgedrückt, was á priori nicht zum obigen Gebrauch von „ $\models$ “ passt. Gemeint ist tatsächlich

$$\{ B \in \mathbf{FO}(\mathcal{S}) : B \text{ gilt in } \mathcal{M} \text{ unter } \sigma \} \models A$$

und da es sich bei der linken Seite um eine Fixpunkt der Polarität handelt, gilt natürlich

$$\{ B \in \mathbf{FO}(\mathcal{S}) : B \text{ gilt in } \mathcal{M} \text{ unter } \sigma \} \ni A$$

Die kanonische Ordnung und Äquivalenz auf $\mathbf{FO}(\mathcal{S})$

Lemma (vergl. Folie 32)

Eine kanonische Quasi-Ordnung $B \sqsubseteq A$ *auf* $\mathbf{FO}(\mathcal{S})$ *wird durch*

$$\begin{aligned} \{B\} \models A \quad & \textit{gdw.} \quad \mathcal{M}[\![B]\!](\sigma) = 1 \quad \textit{impliziert} \quad \mathcal{M}[\![A]\!](\sigma) = 1 \quad (*) \\ & \textit{gdw.} \quad \mathcal{M}[\![B]\!](\sigma) \leq \mathcal{M}[\![A]\!](\sigma) \quad (*) \\ & \textit{gdw.} \quad \mathcal{M}[\![B \to A]\!](\sigma) = 1 \quad (*) \end{aligned}$$

$(*)$ *für alle* $\mathcal{S}$*-Strukturen* $\mathcal{M} = \langle D, I \rangle$ *und alle Belegungen* $\sigma \in D^{\mathcal{V}}$

definiert. Wir betrachten sie wieder als Externalisierung des Junktors $\to$. □

Definition

$\models\!\!\!\models$ sei die von $\sqsubseteq$ induzierte ÄR, die Externalisierung des Junktors $\leftrightarrow$.

Die kanonische Quasi-Ordnung auf $\mathbf{FO}(\mathcal{S})$ mit $\models$ zu bezeichnen kann zu noch mehr Missverständnisse führen, daher verwenden wir $\sqsubseteq$.

Rechenregeln für Quantoren

Neben den Rechenregeln auf Folien 34 und 35 gelten weitere Regeln für die mittels Quantoren gebildeten neuen unären Junktoren $\forall x$ und $\exists x$:

Lemma (weitere logische Äquivalenzenv in $\mathbf{FO}(\mathcal{S})$)

$$\neg\forall x\, A \models\!\!\models \exists x\, \neg A \qquad \neg\exists x\, A \models\!\!\models \forall x\, \neg A \tag{1}$$

$$\forall x\, A \wedge \forall x\, B \models\!\!\models \forall x\, (A \wedge B) \qquad \exists x\, A \vee \exists x\, B \models\!\!\models \exists x\, (A \vee B) \tag{2}$$

$$\forall x\, \forall y\, A \models\!\!\models \forall y\, \forall x\, A \qquad \exists x\, \exists y\, A \models\!\!\models \exists y\, \exists x\, A \tag{3}$$

Sofern $x \notin \mathbf{FV}(A)$ *gilt weiterhin*

$$A \star \mathcal{Q}x\, B \models\!\!\models \mathcal{Q}x\, (A \star B) \quad \textit{für } \mathcal{Q} \textit{ Quantor und } \star \in \{\wedge, \vee, \rightarrow\} \tag{4}$$

$$\mathcal{Q}x\, B \rightarrow A \models\!\!\models \bar{\mathcal{Q}}x\, (B \rightarrow A) \quad \textit{für } \mathcal{Q} \textit{ und } \bar{\mathcal{Q}} \textit{ komplementär} \tag{5}$$

Aber i.A.

$$\forall x\, A \vee \forall x\, B \not\models\!\!\models \forall x\, (A \vee B) \qquad \exists x\, A \wedge \exists x\, B \not\models\!\!\models \exists x\, (A \wedge B) \qquad \forall x\, \exists y\, A \not\models\!\!\models \exists y\, \forall x\, A$$

Substitutionen via Rekursionssatz und Modifikationen

Folie 117 zeigte, wie jedes $\langle x, d\rangle \in \mathcal{V} \times D$ Belegungen $\sigma \in D^{\mathcal{V}}$ in neue Belegungen $\sigma\{x/d\} \in D^{\mathcal{V}}$ transformiert. Betrachte $D = \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$:

Definition

Ein **Fun**-Endomorphismus

$$\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \xrightarrow{\check{\vartheta}} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$$

der die Anwendung einer endlichen Komposition ϑ von Modifikationen

$$\mathbf{Term}(\mathbf{Fun}, \mathcal{V})^{\mathcal{V}} \xrightarrow{\{x,\, t\}} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})^{\mathcal{V}}$$

auf die kanonische Belegung $\mathcal{V} \xrightarrow{\iota} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$ eindeutig fortsetzt, heißt Substitution, wie auch die eindeutigen Fortsetzungen

$$\mathbf{Atm} \xrightarrow{\overline{\vartheta}} \mathbf{Atm} \quad \text{und} \quad \mathbf{FO}(\mathcal{S}) \xrightarrow{\hat{\vartheta}} \mathbf{FO}(\mathcal{S})$$

Anwendung von Substitutionen

Die verdrehte Schreibweise für Modifikationen überträgt sich auf Substitutionen; man braucht $\check{\vartheta}$, $\overline{\vartheta}$ und $\hat{\vartheta}$ nicht länger zu unterscheiden:

Bei der Anwendung auf quantifizierte Formeln dürfen keine neuen Bindungen erzeugt werden. Ggf. sind gebundene Variable umzubenennen:

Definition (Vereinheitlichte Substitutionen)

$$
\begin{aligned}
x\vartheta &:= \check{\vartheta}(x) \\
f(t_0, \ldots, t_{\mathbf{ar}(f)-1})\vartheta &:= f(t_0\vartheta, \ldots, t_{\mathbf{ar}(f)-1}\vartheta) \\
(t_0 \doteq t_1)\vartheta &:= t_0\vartheta \doteq t_1\vartheta \\
R(t_0, \ldots, t_{\mathbf{ar}(R)-1})\vartheta &:= R(t_0\vartheta, \ldots, t_{\mathbf{ar}(R)-1}\vartheta) \\
(\neg A)\vartheta &:= \neg(A\vartheta) \\
(A \star B)\vartheta &:= A\vartheta \star B\vartheta \\
(\mathcal{Q}x\, A)\,\vartheta &:= \mathcal{Q}y\,(A\{x/y\}\vartheta)\ ,\ y \notin \mathbf{V}(A)\ ,\ y\vartheta = y
\end{aligned}
$$

($\{x/y\}\vartheta$ ist natürlich die Komposition von Modifikationen, die erst $\{x/y\}$ und dann ϑ anwendet.)

Substitutionslemma und gebundene Umbenennung

Der Zusammenhang zwischen Substitutionen (in Termen und (atomaren) Formeln) und der Modifikation von Belegungen nimmt nun folgende eindrucksvolle Form an, was sich mittels Induktion über den Aufbau von Termen bzw. Formeln zeigen lässt (gute Übung, um die Notation zu beherrschen!):

Lemma (Substitutionslemma)

$$\mathcal{M}[\![A\{x/t\}]\!](\sigma) = \mathcal{M}[\![A]\!]\,(\sigma\{x/\mathcal{M}[\![t]\!](\sigma)\}) \qquad \hat{\sigma}(A\{x/t\}) = \sigma\{\widehat{x/\check{\sigma}(t)}\}(A)$$

Korollar.

1. Ist $A \in \mathbf{FO}(\mathcal{S}^{\rceil})$ allgemeingültig, dann auch $A\{x/t\}$.
2. Die Formel $\forall x\ A \to A\{x/t\}$ ist allgemeingültig.

Lemma (Gebundene Umbenennung erhält Äquivalenz)

$\mathcal{Q}x\,A \rightleftharpoons \mathcal{Q}y\,A\{x/y\}$ *sofern* $y \notin \mathbf{FV}(A)$. □

bereinigte Formeln

Die Syntax der Prädikatenlogik enthält manche Fallstricke, die man explizit umgehen muß.

Definition

$A \in \mathbf{FO}(\mathcal{S})$ heißt bereinigt, sofern

- keine Variable frei und gebunden auftritt, $\mathbf{FV}(A) \cap \mathbf{GV}(A) = \emptyset$;
- jede Variable höchstens einmal gebunden wird.

Durch iterierte gebundene Umbenennung lässt sich jede Formel bereinigen:

Lemma

Zu jeder Formel $A \in \mathbf{FO}(\mathcal{S})$ *existiert eine bereinigte Formel* $B \in \mathbf{FO}(\mathcal{S})$ *mit* $A \rightleftharpoons B$. □

Folie 124(2) zeigt aber, dass man sich nicht allein auf bereinigte Formeln beschränken kann.

Normalformen

Die Motivation (Folie 82), Formeln der AL in bestimmte einfache Formen zu überführen, greift auch in der PL. Ziel sind einfachere Beweise und effizientere Algorithmen.

Wir werden PL-Formeln in zwei Normalformen transformieren:

- ▷ Pränex-Normalform: alle Quantoren außen; logisch äquivalent;
- ▷ Skolem-Normalform: PNF ohne $\exists$; erfüllbarkeitsäquivalent.

Lemma (Universeller und existenzieller Abschluss)

Für $A \in \mathbf{FO}(\mathcal{S})$ *mit* $\mathbf{FV}(A) \subseteq \{x_i : i < n\}$ *gilt:*

$$A \text{ ist allgemeingültig} \quad \text{gdw.} \quad \forall x_0 \ldots \forall x_{n-1}\, A \text{ ist allgemeingültig}$$
$$A \text{ ist erfüllbar} \quad \text{gdw.} \quad \exists x_0 \ldots \exists x_{n-1}\, A \text{ ist erfüllbar}$$

Die Formeln auf der rechte Seite heißen universeller bzw. existentieller Abschluss von A.

Pränex-Normalform

Definition

Eine Formel der Form

$$A = \mathcal{Q}_0 y_0 \, \mathcal{Q}_1 y_1 \ldots \mathcal{Q}_{n-1} y_{n-1} B$$

mit $\mathcal{Q}_i \in \{\forall, \exists\}$, $i < n$, liegt in Pränex-Normalform oder kurz PNF vor, sofern B keine Quantoren enthält.

Im bereinigten Fall sprechen wir von einer bereinigten PNF, oder kurz BPF.

Satz

Jede Formel $A \in \mathbf{FO}(\mathcal{S})$ besitzt eine äquivalente Formel B in BPF.

Beweis.

Verwende die logischen Äquivalenzen von Folie 124, HA □

Pränex- und Skolem[15] Normalform

Definition

Ist B quantorenfrei, so nennt man eine Formel $A \in \mathbf{FO}(\mathcal{S})$ der Form

$$\mathcal{Q}_0 y_0 \, \mathcal{Q}_1 y_1 \ldots \mathcal{Q}_{n-1} y_{n-1} B$$

mit $\mathcal{Q}_i \in \{\forall, \exists\}$, $i < n$, eine

- Pränex-Normalform oder kurz PNF; im bereinigten Fall spricht man von einer bPNF (BPF in früheren Folien);
- Skolem-Normalform oder kurz SNF, falls es sich um eine bPNF ohne Existenzquantoren handelt, d.h., $\mathcal{Q}_i = \forall$ für $i < n$

Mit den logischen Äquivalenzen auf Folie 124 sieht man leicht (HA):

Satz

Jede Formel $A \in \mathbf{FO}(\mathcal{S})$ besitzt eine äquivalente Formel B in bPNF. □

[15] Thoralf Albert Skolem (1887–1963)

Vorüberlegung zur Skolemisierung

Ziel: Die Existenzquantoren aus einer zu $A \in \mathbf{FO}(\mathcal{S})$ äquivalenten bPNF

$$B = \mathcal{Q}_0 y_0 \, \mathcal{Q}_1 y_1 \ldots \mathcal{Q}_{n-1} y_{n-1} C$$

so entfernen, dass zumindest eine erfüllbarkeitsäquivalente Formel entsteht; am zweckmäßigsten (aber nicht zwingend) von außen nach innen.

Der erste Existenzquantor möge in Position k von links auftreten:

$$B = \forall y_0 \ldots \forall y_{k-1} \exists y_k \mathcal{Q}_{k+1} y_{k+1} \ldots \mathcal{Q}_{n-1} y_{n-1} C$$

Die Variable y_k (bzw. ihr Wert in einem Datenbereich D), deren Existenz verlangt wird, kann von den k zuvor universell quantifizierten Variablen y_i, $i < k$, abhängen, bzw. von den zugeordneten Elementen aus D^k.

Trick: formal einen funktionalen Zusammenhang zwischen den y_i, $i < k$, und y_k schaffen mittels eines frischen Funktionssymbols $f_{/k} \notin \mathbf{Fun}$: statt B betrachten wir nun in $\mathbf{FO}(\mathcal{S} + \{f_{/k}\})$ die erfüllungsäquivalente Formel

$$\forall y_0 \ldots \forall y_{k-1} \mathcal{Q}_{k+1} y_{k+1} \ldots \mathcal{Q}_{n-1} y_{n-1} C\{y_k / f(y_0, \ldots, y_{n-k})\}$$

Anmerkungen

- Sobald wir uns auf Erfüllbarkeitsäquivalenz anstelle von Äquivalenz konzentrieren, gewinnen wir den Spielraum, die Signatur zu unserem Vorteil zu verändern. Insbesondere hat jede Formel A eine minimale endliche Signatur Σ_A, in der sie formuliert werden kann.
- Weder die Reihenfolge noch die Anzahl der Quantoren in einer (b)PNF B von $A \in \mathbf{FO}(\mathcal{S})$ sind eindeutig bestimmt:
  - Statt Rechenregel (2) auf Folie 124 anzuwenden, liefert Bereinigen und zweimalige Anwendung von (4) eine äquivalente Formel mit zwei Quantoren; hier ist die Anwendung von (2) vorzuziehen.
  - Falls in (4) die Formel B die Form $\mathcal{Q}'y\,C$ hat, dann können $\mathcal{Q}x$ und $\mathcal{Q}'y$ durch zweimalige Anwendung von (4) in beliebiger Reihenfolge nach außen gezogen werden, selbst wenn es sich um verschiedene Quantoren handelt.
- Folglich ist nicht einmal die Signatur für Skolemisierungen von $A \in \mathbf{FO}(\mathcal{S})$ eindeutig bestimmt. Hat man die Wahl, sind Skolemsymbole möglichst geringer Stelligkeit vorzuziehen.

Skolemisierung

Algorithmus

Gegeben $A \in \mathbf{FO}(\mathcal{S})$.

- Bestimme eine zu A äquivalente bPNF B; dabei
  - bevorzuge Regel (2) auf Folie 124 gegenüber Bereinigung und Regel (4);
  - bei Anwendung von Regel (4) auf zwei Formeln mit verschiedenen ersten Quantoren, ziehe Existenz-Quantoren vor Allquantoren nach außen, um die Stelligkeit der später benötigten Skolem-Symbole zu minimieren.
- Eliminiere die Existenz-Quantoren der resultierenden bPNF (etwa von links nach rechts) mit Hilfe passender Skolem-Symbole, die zur Signatur hinzuzufügen sind.

Satz (HA)

Jede bPNF-Formel $B \in \mathbf{FO}(\mathcal{S})$ *ist zu ihrer Skolemisierung in* $\mathbf{FO}(\mathcal{S} + \mathbf{Sko})$ *erfüllbarkeitsäquivalent.* □

Das Allgemeingültigkeitsproblem $\mathrm{AGP}(\mathrm{PL})$

Gegeben:	$A \in \mathbf{FO}(\mathcal{S})$
Frage:	ist A allgemeingültig?
oder äquivalent:	ist $\neg A$ unerfüllbar?

Es wird sich zeigen, dass tatsächlich ein Algorithmus existiert, der in endlich vielen Schritten terminiert, wenn $\neg A$ unerfüllbar ist, aber andernfalls nicht notwendig terminiert. In der Tat existiert kein Algorithmus, der in jedem Fall terminiert. Daher ist $\mathrm{AGP}(\mathrm{PL})$, genau wie das Unerfüllbarkeitsproblem für Formelmengen der AL, nur semi-entscheidbar.

Das offensichtliche Problem bei der Suche nach einem Algorithmus ist die Vielzahl der möglichen $\mathcal{S}$-Strukturen $\mathcal{M} = \langle D, I \rangle$:

- die Mächtigkeit des Datenberichs D ist unbeschränkt;
- wir haben keine Information über I.

Vorarbeiten zur Herbrand[16] Theorie: Konstanten

Zum Glück kann man sich auf einen kanonischen Datenbereich beschränken

- wenn die Signatur **Fun** mindestens eine Konstante enthält,
- und A das Symbol $\doteq$ nicht enthält, geschrieben $A \in \mathbf{FO}^{\neq}(\mathcal{S})$.

Beide Bedingungen lassen sich immer erzwingen:

Da die Datenbereiche unserer $\mathcal{S}$-Strukturen nicht leer sein müssen, können wir einer Signatur $\mathcal{S} = \mathbf{Fun} + \mathbf{Pre}$ ohne Konstanten in **Fun** problemlos eine Konstante c hinzufügen. Einerseits gilt

$$\mathbf{FO}(\mathcal{S}) \subseteq \mathbf{FO}(\mathcal{S} + \{c_{/0}\})$$

Andererseits hat jede Formel in $B \in \mathbf{FO}(\mathcal{S} + \{c_{/0}\})$, die c enthält, eine erfüllbarkeitsäquivalente Formel in $\mathbf{FO}(\mathcal{S})$: OBdA möge B in (b)PNF vorliegen. Für jedes $x \in \mathcal{V} - \mathbf{FV}(B)$ hat die gewünschte Eigenschaft dann

$$\exists x\, B\{x/c\}^{-1} \in \mathbf{FO}(\mathcal{S})$$

[16] Jacques Herbrand (1908–1931)

Vorarbeiten zur Herband Theorie: Eliminierung von $=$

Ebenso können wir **Pred** um ein binäres Predikat $\mathbb{E}$ erweitern, so dass jede Formel $A \in \mathbf{FO}(\mathcal{S})$, in der $\doteq$ vorkommt, erfüllungsäquivalent zu einer Formel $B \in \mathbf{FO}^{\neq}(\mathcal{S} + \{\mathbb{E}\})$ ist.

OBdA möge A in bPNF vorliegen, und Σ_A sei die Minimalsignatur für A. A' entstehe, indem jedes Auftreten von $\doteq$ in A durch $\mathbb{E}$ ersetzt wird, unter Mißbrauch der Notation $A' := A\{\doteq / \mathbb{E}\}$.

Jedes Modell $\mathcal{M}$ für A wird zu einem Modell von A', wenn man $\mathbb{E}^{\mathcal{M}}$ als Gleichheit interpretiert. Aber es kann A'-Modelle geben, in denen das nicht der Fall ist. Die liefern keine Information über die Existenz von A-Modellen.

Bilde die die Konjunktion $A^{\neq}$ von A' mit endlich vielen Formeln, die jede Interpretation von $\mathbb{E}$ zu einer Kongruenzrelation machen bzgl. der Minimal-Sigmatur für A'. Dann kann jedes Model für $A^{\neq}$ nach dieser Relation faktorisiert werden, was ein Modell für A ergibt (HA).

Der Satz von Herbrand

OBdA möge nun **Fun** eine Konstante enthalten und $A \in \mathbf{FO}^{\neq}(\mathcal{S})$ gelten.

Definition

- Die Unter-**Fun**-Algebra von $\mathbf{Term}(\mathbf{Fun}, \mathcal{V})$ bezeichnen wir mit $D_{\mathcal{H}}$.
- Jede $\mathcal{S}$-Struktur der Form $\mathcal{H} = \langle D_{\mathcal{H}}, I \rangle$ heißt Herbrand-Struktur.
- Falls $\mathcal{H} \models A$ nennen wir $\mathcal{H}$ ein Herbrand-Modell von A.

Die Interpretation von **Pred** in einer Herbrand-Struktur ist frei wählbar.

Im mathematischen Sinn ist $D_{\mathcal{H}}$ die freie **Fun**-Algebra über $\emptyset$; sie ist genau dann nicht leer, wenn mindestens eine Konstante in **Fun** existiert.

Satz (Herbrand)

Für jede Menge $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$ geschlossener Formeln in SNF gilt:

Γ *ist erfüllbar gdw.* Γ *hat ein Herbrand-Modell*

Beweis.

Wenn Γ ein Herbrand-Modell hat, ist Γ natürlich erfüllbar.

Ist $\mathcal{M} = \langle D, I \rangle$ ein Modell für Γ, so ist $\langle D, I_{\mathbf{Fun}} \rangle$ eine **Fun**-Algebra. Die leere Abbildung $\emptyset \xrightarrow{z} D$ lässt sich aufgrund des Rekursionssatztes eindeutig zu einem **Fun**-Homomorphismus $D_{\mathcal{H}} \xrightarrow{\bar{z}} D$ fortsetzen.

Die $\bar{z}$-Urbilder der Prädikate $R^{\mathcal{M}}$, $R \in \mathbf{Pred}$, machen $D_{\mathcal{H}}$ zu einer $\mathcal{S}$-Struktur $\mathcal{M}_{\mathcal{H}}$ und $\bar{z}$ zu einem starken **Pred**-Homomorpismus, d.h.,

$$R^{\mathcal{M}_{\mathcal{H}}}(u_0, \ldots, u_{\mathbf{ar}(R)-1}) = R^{\mathcal{M}}(\bar{z}(u_0), \ldots, \bar{z}(u_{\mathbf{ar}(R)-1}))$$

für alle $u \in D_{\mathcal{H}}^{\mathbf{ar}(R)-1}$.

Achtung: Dieselbe Konstruktion angewendet auf die Gleichheit über D liefert nicht notwendig die Gleichheit über $D_{\mathcal{H}}$, sondern i.A. nur eine Äquivalenzrelation. Aus diesem Grund durfte in Γ kein $\doteq$ vorkommen.

Beweis, Forsetzung.

Als geschlossene Formel hat $A \in \Gamma$ eine von Belegungen unabhängige Semantik. Wähle eine Belegung $\sigma \in D^{\mathcal{V}}$ und setze $\tau := \sigma \circ \bar{z} \in (D_{\mathcal{H}})^{\mathcal{V}}$. Die Quantifikation in A erstrecke sich über die Variablen $x = \langle x_i : i < n \rangle$. Aufgrund des Substitutionslemmas gilt nun für jedes $u \in (D_{\mathcal{H}})^n$:

$$\begin{aligned}\mathcal{M}_{\mathcal{H}}[\![A\{x/u\}]\!](\tau) &= \mathcal{M}[\![A\{x/\bar{z}(u)\}]\!](\sigma) \\ &= \mathcal{M}[\![A]\!](\sigma\{x/\mathcal{M}[\![\bar{z}(u)]\!](\sigma)\} = 1\end{aligned}$$

bzw. in weniger bombastischer Notation

$$\hat{\tau}(A\{x/u\}) = \hat{\sigma}(A\{x/\bar{z}(u)\}) = \sigma\{\widehat{x/\check{\sigma}(\bar{z}(u))}\}(A) = 1$$

woraus wir für alle $\rho \in D_{\mathcal{H}}^{\mathcal{V}}$ und alle $\sigma \in D^{\mathcal{V}}$ schließen

$$\mathcal{M}_{\mathcal{H}}[\![A]\!] = \mathcal{M}_{\mathcal{H}}[\![A]\!](\rho) = \mathcal{M}_{\mathcal{H}}[\![A]\!](\sigma \circ \bar{z}) = \mathcal{M}[\![A]\!](\sigma) = \mathcal{M}[\![A]\!] = 1$$

Damit ist $\mathcal{M}_{\mathcal{H}}$ ein Herbrand-Modell für A, also auch für Γ. □

Satz von Löwenheim[17]-Skolem

Satz (Löwenheim 1915; Skolem 1922)

Jede erfüllbare Menge Γ von Formeln hat ein abzählbares Modell.

Beweis.

Γ ist genau dann erfüllbar, wenn das für die Menge Γ' der existenziellen Abschlüsse gilt. Nun betrachten wir die Menger Γ'' derer Skolemisierungen; diese ist ebenfalls erfüllbarkeitsäquivalent zu Γ.

Nun kann in Γ, und damit in Γ'', das Symbol $\doteq$ vorkommen. Insofern braucht $\mathcal{M}_{\mathcal{H}}$ aus dem obigen Beweis kein Modell von Γ'' zu sein. Aber wir können diese Struktur nach dem $\bar{z}$-Urbild der Gleichheit auf D (und somit einer Kongruenzrelation auf $D_{\mathcal{H}}$) faktorisieren und erhalten so ein Modell für Γ'' und folglich auch für Γ. Aus der Abzählbarkeit von $D_{\mathcal{H}}$ folgt auch die der Quotientenmenge (warum?). □

[17] Leopold Löwenheim (1878–1957)

Herbrand Expansion

Definition

Ist die Formel $A = \forall x_0 \forall x_1 \ldots \forall x_{n-1} B \in \mathbf{FO}^{\neq}(\mathcal{S})$ mit quantorenfreiem B abgeschlossen und in Skolem-Normalform, so ist ihre Herbrand-Expansion

$$E(A) := \{ B\{x/t\} \,:\, t \in (D_{\mathcal{H}})^n \}$$

Anschaulich entsteht $E(A)$, indem die Variablen x_i, durch beliebige Terme $t_i \in D_{\mathcal{H}}$, $i < n$, substituiert werden. Analog: $E(\Gamma)$ für Formelmengen.

Bemerkung.

Die Formeln in $E(\Gamma)$ enthalten keine Variablen und können somit wie in der AL behandelt werden, mit der Tableau-Methode, oder mittles Resolution, falls jedes $B \in$ KNF. Das Belegen der atomaren Formeln in $D_{\mathcal{H}}$ mit Wahrheitswerten aus $\mathbb{B} = \{0, 1\}$ entspricht dann der Spezifikation einer $\mathcal{S}$-Struktur auf $D_{\mathcal{H}}$.

Lemma

Belegungen $\mathbf{ATM}\,(\mathbf{Pred}, D_{\mathcal{H}}) \xrightarrow{\varphi} \mathbb{B}$ *stehen in bijektiver Beziehung zu Interpretationen der Symbole* $R \in \mathbf{Pred}$ *als Funktionen* $D_{\mathcal{H}}^{\mathbf{ar}(R)} \xrightarrow{I_{\mathbf{Pred}}(R)} \mathbb{B}$.

Beweis.

$\mathbf{ATM}\,(\mathbf{Pred}, D_{\mathcal{H}})$ ist die disjunkte Vereinigung der Mengen

$$\{\, R(t_0, \ldots, t_{\mathbf{ar}(R)-1}) \,:\, t \in D_{\mathcal{H}}^{\mathbf{ar}(R)} \,\} \;,\; R \in \mathbf{Pred}$$

mit $\{\, t_0 \doteq t_1 \,:\, t \in D_{\mathcal{H}}^2 \,\}$. Die Einschränkung von φ auf diese Mengen liefert die gewünschte Familie $I_{\mathbf{Pred}}$ von Interpretation via

$$I_{\mathbf{Pred}}(R)(t_0, \ldots, t_{\mathbf{ar}(r)-1}) := \varphi(R(t_0, \ldots, t_{\mathbf{ar}(r)-1}))$$

Umgekehrt lässt sich aus einer Familie von Interpretation eine Belegung zusammenstückeln. □

Satz von Gödel[18]-Herbrand-Skolem

Satz

Für eine Menge $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$ *geschlossener Formeln in SNF gilt*

Γ *ist erfüllbar gdw.* $E(\Gamma)$ *ist aussagenlogisch erfüllbar*

Beweis.

Es genügt nachzuweisen, dass aus der Erfüllbarkeit von $E(\Gamma)$ die Existenz eines Herbrand-Modells folgt.

Aus einer Belegung φ der atomaren Formeln über $D_{\mathcal{H}}$ erhalten wir nach obigem Lemma eine Interpretation der Prädikatssymbole in $D_{\mathcal{H}}$, und somit eine Herbrand- Struktur $\mathcal{M}_{\mathcal{H}} = \langle D_{\mathcal{H}}, I \rangle$.

Für $A \in \Gamma$ der Form $\forall x_0 \ldots \forall x_{n-1} B$ mit B quantorenfrei, gilt wegen der Geschlossenheit von A unabhängig von jedweder Belegung $\sigma \in D_{\mathcal{H}}^{\mathcal{V}}$:

[18] Kurt Gödel (1906–1978)

Beweis, Fortsetzung.

$$
\begin{aligned}
& \hat{\varphi}(C) = 1 \text{ für alle } C \in E(A) \\
\text{gdw} \quad & \mathcal{M}_{\mathcal{H}}[\![C]\!](\sigma) = 1 \text{ für alle } C \in E(A) \\
\text{gdw} \quad & \mathcal{M}_{\mathcal{H}}[\![B\{x/t\}]\!](\sigma) = 1 \text{ für alle } t \in (D_{\mathcal{H}})^n \\
\text{gdw} \quad & \mathcal{M}_{\mathcal{H}}[\![B]\!](\sigma\{x/\mathcal{M}_{\mathcal{H}}[\![t]\!](\sigma)\} = 1 \text{ für alle } t \in (D_{\mathcal{H}})^n \\
\text{gdw} \quad & \mathcal{M}_{\mathcal{H}}[\![A]\!](\sigma) = 1 \\
\text{gdw} \quad & \mathcal{M}_{\mathcal{H}}, \sigma \text{ ist ein Herbrand-Modell für } A \\
\text{gdw} \quad & \mathcal{M}_{\mathcal{H}} \text{ ist ein Herbrand-Modell für } A
\end{aligned}
$$

wobei im 3. Schritt das Substitutionslemma zum Tragen kommt. □

In Verbindung mit dem Kompaktheitssatz der Aussagenlogik ergibt sich

Corollar

Eine Menge $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$ geschlossener Formeln in SNF ist unerfüllbar, genau dann wenn eine endliche Teilmenge von $E(\Gamma)$ unerfüllbar ist.

Algorithmus von Gilmore (ineffizient)

Algorithmus

Eingabe: $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$ geschlossen und in SNF, A_i, $i \in \mathbb{N}$ Aufzählung von $E(\Gamma)$.

Algorithmus: Solange $G_n := \bigwedge_{i<n} A_i$ erfüllbar ist, bilde $G_{n+1} = G_n \wedge A_n$.

A ist genau dann unerfüllbar, wenn das Verfahren terminiert.

Der Algorithmus terminiert genau dann, wenn A unerfüllbar ist und liefert dann das korrekte Ergebnis. Daher ist das $\mathrm{AGP}(\mathrm{PL})$ semi-entscheidbar.

Achtung: für die Entscheidbarkeit von $\mathrm{AGP}(\mathrm{PL})$ bräuchte man die Semi-Entscheidbarkeit von $\not\models A$, was aber leider nicht zu $\models \neg A$ äquivalent ist; nur letzteres lässt sich mit dem Gilmore-Algorithmus semi-entscheiden.

Die Begriffe der „Entscheidbarkeit“ und der „Semi-Entscheidbarkeit“ werden offiziell in der VL „Theoretische Informatik 2“ behandelt.

Tableaus in der PL

Um die Tableau-Methode in die PL übertragen, ist die Klassifikation der Formeln aus $\mathbf{FO}^{\neq}(\mathcal{S})$ zu erweitern:

Definition

- „Literale“: atomare Formeln und ihre Negationen;
- α: $A \wedge B$, $\neg(A \vee B)$, $\neg(A \to B)$, $\neg\neg A$;
- β: $A \vee B$, $A \to B$, $\neg(A \wedge B)$;
- γ: $\forall x\, A$, $\neg\exists x\, A$;
- δ: $\exists x\, A$, $\neg\forall x\, A$.

Neue Regeln mit $t \in D_{\mathcal{H}}$ bzw. c frische Konstante für den Ast:

$$\frac{\forall x\, A}{A\{x/t\}} \quad , \quad \frac{\neg\exists x\, A}{\neg A\{x/t\}} \quad , \quad \frac{\exists x\, A}{A\{x/c\}} \quad , \quad \frac{\neg\forall x\, A}{\neg A\{x/c\}}$$

Details + Anwendungen: siehe alte Folien.

Resolution in der PL

Gehört die quantorenfreie Formel B der geschlossenen Skolem-Normalform A zu KNF, so auch alle Elemente der Herbrand-Expansion, und deren Konjunktionen. Nun lässt sich die Resolutionsmethode der AL anwenden.

Beispiel

$\mathcal{S} = \{a_{/0}, f_{/1}; R_{/1}\}$ und $A = \forall x\big(R(x) \wedge \neg R(f(x))\big)$ liefert

$$E(A) = \{R(a) \wedge \neg R(f(A)), R(f(a)) \wedge \neg R(f(f(a))), \dots\}$$

Die vier Unit-Klauseln der ersten beiden Elemente liefern bereits die leere Resolvente. Damit ist A nicht erfüllbar.

Idee zur Vermeidung nicht-zielführender Klauseln: $E(\Gamma)$ „verfeinern“, indem man nicht in ganz B sondern nur in „vielversprechende“ Klauseln von B substituiert $\Longrightarrow$ Unifikation (siehe alte Folien)

Der Kompaktheitssatz der PL

Satz

Eine Formelmenge $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$ ist genau dann erfüllbar, wenn sie endlich erfüllbar ist, d.h., wenn jede endliche Teilmenge $\Gamma_0 \subseteq \Gamma$ erfüllbar ist.

Beweis.

Die Notwendigkeit ist klar.

Für die Hinlänglichkeit beschränken wir uns zunächst auf den Fall geschlossener Formeln in Skolem-Normalform ohne $\doteq$. Offenbar ist Γ genau dann erfüllbar, wenn das für $E(\Gamma) := \bigcup\{ E(A) : A \in \Gamma \}$ gilt, was nach dem KPS(AL) zur endlichen Erfüllbarkeit von $E(\Gamma)$ äquivalent ist.

Ist Γ endlich erfüllbar, finden wir zu jeder endlichen Teilmenge $\Delta_0 \subseteq E(\Gamma)$ eine endliche und somit erfüllbare Teilmenge $\Gamma_0 \subseteq \Gamma$ mit $\Delta_0 \subseteq E(\Gamma_0)$. Damit ist Δ_0 erfüllbar, und damit ist $E(\Gamma)$ endlich erfüllbar. Also ist $E(\Gamma)$ nach dem KPS(AL) erfüllbar.

Beweis, Fortsetzung.

Nun betrachte eine beliebige Menge $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$.

(0) alle freien Variablen, die in Formeln in Γ auftreten, werden durch frische Konstanten ersetzt; es ist sicherzustellen, dass mindestens eine Konstante in der neuen Signatur auftritt.

(1) In der resultierenden Menge $\Gamma' \subseteq \mathbf{FO}(\mathcal{S} + \mathbf{Con})$ kann noch das Symbol $\doteq$ auftreten. Dies ersetzen wir durch ein binäres Prädikatssymbol $\mathbb{E}$, und wir erweitern Γ' um neue Formeln, die sicherstellen, dass $\mathbb{E}$ in jeder Struktur als Kongruenz interpretiert werden muß (vergl. HA).

(2) Die Elemente der resultierenden Menge $\Gamma'' \subseteq \mathbf{FO}^{\neq}(\mathcal{S} + \mathbf{Con} + \{\mathbb{E}\})$ werden in Skolem-Normalform überführt.

(3) Die resultierende Menge $\Gamma''' \subseteq \mathbf{FO}(\mathcal{S} + \mathbf{Con} + \{\mathbb{E}\} + \mathbf{Sko})$ kann nun wie oben behandelt werden. □

Schritt (0) kann als Skolemisierung der existentiellen Abschlüsse aufgefaßt werden.

Nichtstandard-Modelle

Betrachte die Signatur der Arithmetik: $\mathcal{S}_{\mathrm{Arith}} = \{0_{/0}, 1_{/0}, +_{/2}, \cdot_{/2}; <_{/2}\}$; die intendierte Struktur sind die natürlichen Zahlen $\mathbb{N}$ mit den kanonischen Operationen/Relationen.

Ziel: zeigen, dass es „seltsame“ $\mathcal{S}_{\mathrm{Arith}}$-Strukturen $\mathcal{M}^* = \langle D^*, I^* \rangle$ gibt, die dieselben geschlossenen Formeln erfüllen wie $\mathbb{N}$ mit der kanonischen Interpretation, aber nicht zu $\mathbb{N}$ isomorph sind.

Solche Modelle heißen Nichtstandard-Modelle.

Einsicht: Wichtige Eigenschaften z.B. der natürlichen Zahlen lassen sich nicht in **FO** erfassen.

Anwendungen:

- ▸ Nichtstandard Analysis (Robinson, 1966);
- Computer-Algebra;
- Verifikation hybrider Systeme (Zug-und Flugzeugcontroller)

Satz

Es gibt Nicht-Standard-Modelle der Arithmetik.

Beweis.

Setze $A_n = n \cdot 1 := 1 + \cdots + 1 < x$ mit freiem x und

$$\Gamma = \{ A \in \mathbf{FO}(\mathcal{S}_{\text{arith}}) : A \text{ geschlossen, und } \mathbb{N} \models A \} \cup \{ A_i : i \in \mathbb{N} \}$$

Offenbar ist jede endliche Teilmenge von Γ erfüllbar, nämlich im Standard-Modell $\mathbb{N}$: da nur endlich viele Formeln der Form A_i vorkommen, findet man einen hinreichend großen Wert für x.

Jedes Modell $\mathcal{M}^*$ von Γ muß

- alle geschlossenen in $\mathbb{N}$ gültigen $\mathcal{S}_{\text{arith}}$-Formeln erfüllen,
- ein bzgl. $I^*(<)$ größtes Element haben, was $\mathcal{M}^* \ncong \mathbb{N}$ impliziert

Daher lassen sich $\mathbb{N}$ und $\mathcal{M}^*$ nicht durch geschlossene $\mathcal{S}_{\text{arith}}$-Formeln unterscheiden. □

Skolems Paradox

Die übliche Mengenlehre (Anhang C) ist ein Modell für die dortigen Axiom-Schemata. Nach dem Satz von Löwenheim-Skolem muß es also auch ein abzählbares Modell $\mathcal{M}_{\mathrm{LS}}$ von ZFC geben.

Gemäß Anhang zur Abzählbarkeit ist im Standarmodell der Mengenlehre die Potenzmenge von $\mathbb{N}$ überabzählbar. In $\mathcal{M}_{\mathrm{LS}}$ muß es Objekte N und P geben, die die Rolle der „Menge der natürlichen Zahlen“ bzw. deren „Potenzmenge“ spielen. Weiterhin muß dann P „überabzählbar“ sein.

Warum ist das kein Widerspruch?

Die „Überabzählbarkeit“ von P in $\mathcal{M}_{\mathrm{LS}}$ bedeutet lediglich, dass kein Analogon zu einer „Abbildung“ von P nach N in $\mathcal{M}_{\mathrm{LS}}$ „injektiv“ ist. Dagegen ist die Abzählbarkeit von $\mathcal{M}_{\mathrm{LS}}$ eine Aussage im Standad-Modell der Mengenlehre und kann insofern gar nicht mit der „Überabzählbarkeit“ in $\mathcal{M}_{\mathrm{LS}}$ in Beziehung gesetzt werden. Ein Problem entsteht erst dann, wenn man beide Modlell unzulässig vermischt (Anführungszeichen weglässt).

Logische Folgerung in der PL (vergl. Folie 121f)

Lemma

(0) $\Gamma \models A$ *gdw.* $\Gamma \cup \{\neg A\}$ *nicht erfüllbar.*

(1) $\emptyset \models A$ *bzw.* $\models A$ *gdw.* A *allgemeingültig.*

(2) Γ *nicht erf'bar gdw.* $\Gamma \models A$ *für alle* $A \in \mathbf{FO}(\mathcal{S})$ *gdw.* $\mathbf{FO}(\mathcal{S}) \subseteq \Gamma^{\models}$.

(3) $A \sqsubseteq B$ *gdw.* $\models A \to B$ *gdw.* $\mathcal{M}[\![A]\!](\sigma) \leq \mathcal{M}[\![B]\!](\sigma)$ *, alle* $\mathcal{M}, \sigma$

(4) $A \rightleftharpoons B$ *gdw.* $\models A \leftrightarrow B$ *gdw.* $\mathcal{M}[\![A]\!](\sigma) = \mathcal{M}[\![B]\!](\sigma)$ *, alle* $\mathcal{M}, \sigma$

.

Wichtige Sätze zur logischen Folgerung

Betrachte $\Gamma \subseteq \mathbf{FO}(\mathcal{S}) \ni A, B$.

- $\Gamma \cup \{B\} \models A$ gdw. $\Gamma \models B \to A$ (Deduktionstheorem).
- $\Gamma \models B$ und $\Gamma \models B \to A$ impliziert $\Gamma \models A$ (Modus Ponens).
- $\Gamma \cup \{B\} \models \neg A$ gdw. $\Gamma \cup \{A\} \models \neg B$ (Kontraposition).
- Falls $x \notin \mathbf{FV}(G)$ für alle $G \in \Gamma$, dann
  $\Gamma \models A$ gdw. $\Gamma \models \forall x\, A$ (Generalizierung);
  – insbesondere $\{A\} \models \forall x\, A$, bzw. $\models A \to \forall x\, A$, sofern $x \notin \mathbf{FV}(A)$.
- Entsteht A' aus A durch erlaubte (beachte Quantoren!) Ersetzung einiger Vorkommen von x durch y , dann
  $\models \forall x \forall y \left(x \doteq y \to (A \leftrightarrow A')\right)$ (Variante der Kongruenz)

Beispiel

- $\{\forall x A\} \models A$ folgt mittels Deduktionstheorem aus der Allgemeingültigkeit von $\forall x\, A \to A\{x/t\}$ (Folie 127), mit $t = x$.
- Falls $y \in \mathbf{FV}(A)$ braucht $\{A\} \models \forall y\, A$ i.A. nicht zu gelten:

  Für $\mathcal{S} = \{R_{/1}\}$ und $A = R(y)$ betrachte $\mathcal{M} = \langle \{0,1\}, R^{\mathcal{M}} = \chi_{\{0\}} \rangle$. Die konstante 0-wertige Belegung $\sigma \in \{0,1\}^{\mathcal{V}}$ liefert $\mathcal{M}[\![A]\!](\sigma) = 1$ aber $\mathcal{M}[\![\forall y\, A]\!](\sigma) = 0$, da auch $\mathcal{M}[\![A]\!](\sigma\{x/1\}) = 0$ hierbei zu berücksichtigen ist.
- $\models \exists x\ (R(x) \to \forall x\, R(x))$: Die Formel wird in $\mathcal{M}$ als wahr interpretiert, wenn ein $d \in D$ mit $R^{\mathcal{M}}(d) = 0$ existiert, oder wenn $R^{\mathcal{M}}(d) = 1$ für alle $d \in D$ gilt; und eine dieser Alternativen muß eintreten.
- $\forall x(A \to B) \models \forall x\, A \to \forall x\, B$, nach DT, RR (2) auf Folie 124 und MP der Aussagenlogik.

Beispiel

- $\models \exists x \forall y\, A \rightarrow \forall y \exists x A$

  gdw. $\exists x \forall y\, A \models \forall y \exists x\, A$ Deduktionstheorem

  gdw. $\exists x \forall y\, A \models \exists x\, A$ Generalisierungtheorem

  gdw. $\neg\forall x \neg\forall y\, A \models \neg\forall x \neg A$ logische Äquivalenz

  gdw. $\forall x \neg A \models \forall x \neg\forall y\, A$ Kontraposition

  gdw. $\forall x \neg A \models \neg\forall y\, A$ Generalisierungstheorem

  gdw. $\{\forall x \neg A, \forall y\, A\}$ nicht erfüllbar Lemma (0)

  gdw. $\{\exists y \forall x \neg A, \exists x \forall y\, A\}$ nicht erfüllbar existentieller Abschluß

  gdw. $\{\neg\forall y \exists x\, A, \exists x \forall y\, A\}$ nicht erfüllbar logische Äquivalenz

  gdw. $\exists x \forall y\, A \wedge \neg\forall y \exists x\, A$ nicht erfüllbar

- $\forall x \forall y \left(x \doteq y \rightarrow (f(x,y) = g(x) \leftrightarrow f(y,y) = g(x))\right)$ gilt immer, wenn $\mathcal{S}$ Funktionssymbole $f_{/0}$ und $g_{/2}$ enthält.

Anhang A
Ordnungstheorie

Eigenschaften von Relationen

Definition

Eine Relation $R \subseteq X \times X$ heißt

- reflexiv, falls xRx für alle $x \in X$;
- transitiv, falls aus $xRyRz$ folgt xRy für alle $x, y, z \in X$;
- symmetrisch, falls aus xRy folgt yRx für alle $x, y \in X$;
- antisymmetrisch, falls aus xRy und yRx folgt $x = y$ für alle $x, y \in X$;
- linear, falls xRz oder yRx gilt für alle $x, y \in X$;
- Äquivalenzrelation, falls R reflexiv, transitiv und symmetrisch ist;
- Quasi-Ordnung, falls R reflexiv und transitiv ist;
- Halb-Ordnung, falls R reflexiv, transitiv und antisymmetrisch ist.

Weiter sei $R^{\mathrm{op}} := \{\langle b, a\rangle \in X \times X : \langle a, b\rangle \in R\}$, die zu R duale Relation.

Beispiele für Quasi-/Halb-Ordnungen

Beispiel

- Die Gleichheit $=$ ist sowohl eine Äquivalenzrelation als auch eine Halbordnung auf jeder Menge X;
- $\leq$ ist eine lineare Halb-Ordnung auf $\mathbb{B}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$;
- $\subseteq$ ist eine Halb-Ordnung auf der Potenzmenge $P(X)$ einer Menge X, i.A. nicht linear;
- die Teilbarkeitsrelation $\mid$ ist eine nicht lineare Halbordnung auf $\mathbb{N}$;
- Jede Abbildung $X \xrightarrow{f} Y$ induziert eine Äquivalenzrelation auf X vermöge $x \sim x'$ gdw. $f(x) = f(x')$;
- Jede Abbildung $X \xrightarrow{f} \langle Y, \leq \rangle$ in eine quasi-geordnete Menge induziert eine Quasi-Ordnung auf X vermöge $x \sqsubseteq x'$ gdw. $f(x) \leq f(x')$;

Ordnungstheoretische Grundbegriffe

Definition

Sei $\langle X, \sqsubseteq \rangle$ eine quasi-geordnete Menge, $Q \subseteq X$ und $x \in X$.

- Q heißt unterer Abschnitt, falls $x \sqsubseteq q \in Q$ immer $x \in Q$ impliziert;
- der von Q erzeugte untere Abschnitt ist

$$\downarrow Q := \{ x \in X : \text{es gibt ein } q \in Q \text{ mit } x \sqsubseteq q \}$$

- x heißt untere Schranke von Q, falls $x \sqsubseteq q$ für alle $q \in Q$;
- Der untere Abschnitt aller unteren Schranken von Q ist

$$Q^{\downarrow} := \{ x \in X : \text{für alle } q \in Q \text{ gilt } x \sqsubseteq q \}$$

Duale Begriffe: oberer Abschnitt, $\uparrow Q$, obere Schranke, $Q^{\uparrow}$.

Verbände

Definition

In einem $\sqcap$-Halbverband hat jede endliche Teilmenge eine größte untere Schranke, auch Infimum genannt.

Dualer Begriff: $\sqcup$-Halbverband

In einem Verband hat jede endliche Teilmenge eine größte untere und eine kleinste obere Schranke.

Beispiel

- Jede linear geordnete Menge ist ein Verband mit $\sqcap = \min$ und $\sqcup = \max$.
- Jede Potenzmenge ist ein Verband mit $\sqcap = \cap$ und $\sqcup = \cup$.
- $\mathbb{N}$ ist ein Verband bzgl. der Teilbarkeitsrelation mit $\sqcap =$ **ggT** und $\sqcup =$ **kgV**.

Polaritäten

Definition

Eine Abbildung $\langle X, \leq \rangle \xrightarrow{f} \langle Y, \sqsubseteq \rangle$ zwischen quasi-geordneten Mengen heißt monoton, bzw. antiton, falls für alle $a, b \in X$

$$a \leq b \quad \text{impliziert} \quad f(a) \sqsubseteq f(b) \quad \text{bzw.} \quad f(b) \sqsubseteq f(a)$$

Satz

Jedes $R \subseteq X \times Y$ induziert ein Paar antitoner Abbildungen (Polarität)

$$P(X) \underset{R^\circ}{\overset{^\circ R}{\leftrightarrows}} P(Y) \qquad \text{via} \qquad \begin{aligned} {}^\circ R(V) &:= \{\, x \in X \,:\, xRy \text{ für jedes } y \in V \,\} \\ R^\circ(U) &:= \{\, y \in Y \,:\, xRy \text{ für jedes } x \in U \,\} \end{aligned}$$

mit $U \subseteq {}^\circ R(V)$ gdw. $V \subseteq R^\circ(U)$ für alle $U \subseteq X$ und alle $V \subseteq Y$. □

Für eine Quasi-Ordnung $\sqsubseteq$ auf X gilt $\sqsubseteq^\circ = (\ )^\uparrow$ und ${}^\circ\sqsubseteq = (\ )^\downarrow$.

Hüllenoperatoren

Definition

Eine monotone Abbildung $\langle X, \leq \rangle \xrightarrow{H} \langle X, \leq \rangle$ auf einer quasi-geordneten Menge heißt Hüllenoperator, falls sie

- expansiv ist, d.h. $x \leq H(x)$ für alle $x \in X$;
- idempotent ist, d.h., $H(H(x)) \leq H(x)$ für alle $x \in X$.

Im halb-geordneten Fall gilt wegen der Monotonie $H(H(x)) = H(x)$.

Satz

Für jede Relation $R \subseteq X \times Y$ ist $g_R \circ f_R$ und $f_R \circ g_R$ ein Hüllenoperator auf $P(X)$ bzw. $P(Y)$.

Beweis für $f_R \circ g_R$.

Wegen $g_R(V) \subseteq g_R(V)$ gdw. $V \subseteq f_R(g_R(V))$ ist $f_R \circ g_R$ expansiv, wegen $g_R(V) \supseteq g_R(f_R(g_R(V)))$ also auch idempotent. □

Anhang B
Abzählbarkeit

Abzählbarkeit

$\mathbb{N}$ bezeichnet die unendliche Menge $\{0, 1, 2, \dots\}$ der natürlichen Zahlen.

Definition

Eine Menge B heißt abzählbar, wenn es eine injektive Abbildung $B \xrightarrow{f} \mathbb{N}$ gibt. Anderfalls heißt sie *überabzählbar*.

Insbesondere ist jede endliche Menge abzählbar. Um diese auszuschließen, spricht man von abzählbar unendlichen Mengen.

Satz.

Folgende Bedingungen für B sind äquivalent:

(a) B ist abzählbar.

(b) $B = \emptyset$ oder es gibt eine surjektive Abbildung $\mathbb{N} \xrightarrow{g} B$.

(c) Es gibt eine surjektive partielle Abbildung $\mathbb{N} \xrightarrow{h} B$. □

Solch ein g oder h heißt dann Aufzählung.

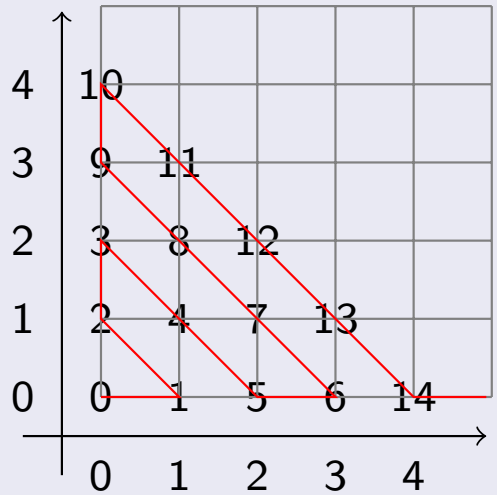
Satz

Teilmengen, endliche cartesische Produkte und abzählbare Vereinigungen abzählbarer Mengen sind wieder abzählbar. Dagegen sind Potenzmengen abzählbar unendlicher Mengen überabzählbar.

Beweis.

Teilmengen: Komponiere die injektive Inklusion $C \xrightarrow{\iota} B$ mit $B \xrightarrow{f} \mathbb{N}$.

Cartesisches Produkt: Es genügt, $\mathbb{N} \times \mathbb{N}$ als abzählbar nachzuweisen. Eine Injektion ist z.B. gegeben durch



Beweis (Fortsetzung).

Abzählbare Vereinigungen: Es genügt, die disjunkte Vereinigung von $\mathbb{N}$ Kopien von $\mathbb{N}$ als abzählbar nachzuweisen (warum?). Aber eine derartige Vereinigung ist isomorph zu $\mathbb{N} \times \mathbb{N}$.

Unendliche Potenzmengen: Es genügt zu zeigen, dass $P(\mathbb{N})$ überabzählbar ist. Wir verfahren indirekt: ist $P(\mathbb{N}) \xrightarrow{g} \mathbb{N}$ injektiv, so betrachten wir die Menge

$$K := \{\, g(B) \,:\, B \subseteq \mathbb{N} \wedge g(B) \notin B \,\} \subseteq \mathbb{N}$$

Wegen der Injektivität von g ist K das einzige g-Urbild von $g(K)$. Gilt $g(K) \in K$, muß das aufgrund von $g(K) \notin K$ der Fall sein. Umgekehrt kann $g(K) \notin K$ nur aufgrund von $g(K) \in K$ gelten, Widerspruch. (Dieses Argument funktioniert für jede unendliche Menge X und zeigt, dass keine injektive Abbildung von $P(X)$ nach X existiert.) □

Lemma

Ist X abzählbar, so auch die Menge aller endlichen Wörter (= Tupel) über X, d.h., die disjunte Vereinigung

$$X^* := \sum_{i \in \mathbb{N}} X^i = X^0 + X^1 + X^2 + \cdots$$

Beweis.

Es handelt sich um eine disjunkte Vereinigung endlicher cartesischer Produkte abzählbarer Mengen, und diese ist nach obigem Satz abzählbar. □

Corollar.

Die Menge $\mathcal{F}[\mathcal{A}]$ aller aussagenlogischen Formeln ist abzählbar.

Beweis.

Es handelt sich um eine Teilmenge von $(\mathcal{A} + \mathcal{J} + \{ \mathbb{C} , \mathbb{D} \})^*$. □

Lemma

Für jede abzählbare Signatur $\mathcal{S}$ ist die Menge $\mathbf{FO}(\mathcal{S})$ abzählbar.

Beweis.

Da $\mathcal{V}$ abzählbar ist, gilt das auch für $(\mathcal{S} + \mathcal{V})^*$ und somit für die Teilmenge $\mathbf{Term}(\mathbf{Fun}, \mathcal{V})$. Die atomaren Formeln sind nun Wörter über den Alphabet $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) + \mathbf{Pred} + \{(,)\}$, bilden also auch eine abzählbare Menge. Nun greift im Wesentlichen dasselbe Argument, wie für die Aussagenlogik: mittels abzahlbar vieler Junktoren lassen sich nur abzählbar viele endliche Formeln erzeugen. □

Anhang C
Mengenlehre

ZFC

Die übliche Zermelo[19]-Fraenkel[20] Mengenlehre läßt sich z.B. mit der Signatur $\mathcal{S}_{\mathrm{set}} = \{\emptyset_{/0}; \in_{/2}\}$ formulieren und basiert auf 8 Axiom-Schemata:

- Extensionalität:

$$\forall x \, \forall y \, \big(\forall z \, (z \in x \leftrightarrow z \in y) \rightarrow x \doteq y \big)$$

- Leere Menge:

$$\forall x \, \neg (x \in \emptyset)$$

- Paarmengen:

$$\forall x \, \forall y \, \exists z \, \forall w \, \big(w \in z \leftrightarrow (w \doteq x \vee w \doteq y) \big)$$

  Schreibweise: $z = \{x, y\}$.

[19] Ernst Friedrich Ferdinand Zermelo (1871–1953)
[20] Abraham Halevi Fraenkel (1891–1965)

- Vereinigung:

$$\forall x\, \exists y\, \forall z\, \big(z \in y \leftrightarrow \exists w\, (z \in w \wedge w \in x)\big)$$

  Schreibweise: $y = \bigcup x$ oder $y = u \cup v$ falls $x = \{u, v\}$.

- Unendlichkeit:

$$\exists x\, \big(\emptyset \in x \wedge \forall y\, (y \in x \to y \cup \{y\} \in x)\big)$$

- Potenzmengen:

$$\forall x\, \exists y\, \forall z\, \big(x \in y \leftrightarrow \forall w\, (w \in z \to w \in x)\big)$$

- Regularität oder Fundierung:

$$\forall x\, \Big(\neg(x \doteq \emptyset) \to \exists y\, \big(y \in x \wedge \neg\exists z\, (z \in x \wedge z \in y)\big)\Big)$$

- Aussonderung: Falls $\mathbf{FV}(A) \subseteq \{x, z\} \cup \{w_i \,:\, i < n\}$, dann

$$\forall z\, \forall w_0 \cdots \forall w_{n-1}\, \exists y\, \forall x\, (x \in y \leftrightarrow x \in z \wedge A)$$

  Schreibweise: $y = \{\, x \,:\, x \in z \wedge A \,\}$

- Auswahl (Choice), wird von Praktikern oft hinzugenommen:

$$\forall x \Big((\emptyset \notin x) \wedge \forall y\, \forall z\, \big(y \in x \wedge z \in x \rightarrow x \doteq y \vee \neg \exists w\, (w \in x \wedge w \in y)$$
$$\rightarrow \exists w\, \forall u\, (u \in x \rightarrow \exists! v\, (v \in u \wedge v \in w))\big)\Big)$$

  besagt, dass man aus jedem Element u einer Menge x paarweise disjunkter nichtleerer Mengen jeweils genau ein ($\exists!$) Element auswählen kann.

Ein großer Teil der üblichen Mathematik läßt sich in ZFC formulieren, etwa die Konzepte einer natürlichen Zahl, der Menge $\mathbb{N}$, einer Funktion, der Injektivität, der Surjektivität, der Abzählbarkeit, etc.