Basis-SE Logik III (Schurz) Ss 2012 Mi 10:30-12, 23.21/U1.46
Einführung in die mathematische Logik

Literatur:

Einführungen in die Logik:

Bergmann, M. et al. (1998): *The Logic Book*, McGraw Hill, New York, 3. Aufl.

Beckermann, A. (1997): Einführung in die Logik, W. de Gruyter, Berlin (2. Aufl. 2003).

Bühler, A. (2000): *Einführung in die Logik*, Alber, Freiburg i. Breisgau, 3. Aufl.

Essler, W., und Martinez, R. (1991): Grundzüge der Logik Bd. I, Vittorio Klostermann, Frankfurt/M.

Klenk, Virginia (1989): *Understanding Symbolic Logic*, Prentice Hall, Englewood Cliffs, NJ.

Grundkurse in Logik für Fortgeschrittene:

Ebbinghaus, H.D. et al. (1996): Einführung in die mathematische Logik, Spektrum, Heidelberg (4. Aufl.).

Essler, W., Brendel, E., und Martinez, R. (1987): Grundzüge der Logik Bd. II, Vittorio Klostermann, Frankfurt/M.

Machover, M. (1996?): Set Theory, Logic and their Limitations, Cambridge Univ. Press.

Rautenberg, W. (2002): Einführung in die mathematische Logik, Vieweg, Braunschweig.

Hunter, G. (1971): *Metalogic* , Univ. of California Press, Berkeley, 6. Aufl. 1996.

Einführung in die Mengenlehre:

Van Dalen, D., et al. (1978): *Sets. Naive, Axiomatic and Applied*, Pergamon Press, Oxford.

Ebbinghaus, H.-D. (2003): *Einführung in die Mengenlehre*, Spektrum Akad. Verlag, Heidelberg (4. Aufl.).

O. Deiser, *Einführung in die Mengenlehre*, Springer, 3. korr. Aufl. 2010.

1. Einleitung

1.1 (Philosophische) Logik im weiten Sinne = Theorie des korrekten Schließens

Das Grundlegende Muster des Schließens: Ein Argument (ein Schluss)

Präm 1 Präm$_1$, …, Präm$_n$ / Konkl …

||— (semantische Gültigkeit, auch |==)

Präm n |— (syntaktische Beweisbarkeit)

Konkl

Gültigkeits-Kriterium = Wahrheitserhaltung: wenn alle Prämissen wahr sind, ist auch die Konklusion wahr

Klassifikation von Arten logischer Systeme:

Deduktive Logik	*Nichtdeduktive Logik*
(*Logik im engen Sinne*)	*(Logik im weiten Sinne)*
Ein deduktiv korrektes Argument =	induktive (probabilistische) Logik
ein gültiges Argument	nichtmonotone Logik, unsicheres Schließen
Wahrheitsheitserhaltung	Wahrheitserhaltung mit hoher Wahrschein-
mit Sicherheit	lichkeit, Plausibilität, Unsicherheit

Klassische Logik(en):	*Nichtklassische Logik(en):*
(Wahrheitsfunktionale) propositionale Logik	intuitionistische Logik
Prädikatenlogik 1. Ordnung	Quantenlogik
modale (propositionale, Prädikaten-) Logik	Relevanzlogik
(alethische ML, deontische L, epistemische L,	mehrwertige Logik
konditionale L.,…) …	...
Prädikatenlogik zweiter Ordnung	

Eine generelle Charakterisierung eines gültigen Arguments:

Präsupponiert ist eine Unterteilung der Menge aller Symbole der Sprache in:

Nichtlogische Symbole	*Logische Symbole*
elementare Sätze p, q,…	propositionale Konnektive $\neg,\wedge,\vee,\rightarrow,\ldots$
Individuenkonstanten a, b,…	Quantoren $\forall x$, $\exists x$, $\equiv$
Prädikate F, G,…, R,…	Modal-Operatoren $\Box$, $\Diamond$, …
Funktionssymbole f, g, …	
variierende (welt-referierende) Interpr.	*fixierte* (logische) Interpretation

Ein Argument ist gültig gdw. (genau dann, wenn) die Wahrheit übertragen wird (d.h. die Konklusion wahr ist, sofern alle Prämissen wahr sind)

- *in allen Interpretationen seiner nichtlogischen Symbole*

(semantische Charakterisierung)

- *alleine aufgrund seiner logischen Form/Struktur*

(syntaktische Charakterisierung) (Jedes Argument der gegebenen Form ist gültig)

Beispiel für logische Form: $p \rightarrow q$, $p \vdash q$ (Modus Ponens)

Formalisierung = Übersetzung der natürlichen Sprache in formale Sprache:

z.B. p – es regnet, q – die Straße ist nass

Wenn es regnet, ist die Straße nass, es regnet / die Straße ist nass.

Hauptziel eines Argumentes:

- *Positiver Nutzen:* --> Wahrheitstransfer (Voraussage, Erklärung). *Ein gültiges, sowie korrektes Argument:* Ein gültiges Argument mit wahren Prämissen.
- *Negativer Nutzen:* --> Falschheits-Rücktransfer (Falsifikation).

Unterdeterminiertheit der Falsifikation: Ma n kann lediglich schließen, dass *einige* der Prämissen falsch sind (welche?) (Duhem-Problem der Theorienfalsifikation)

Hauptziel der Logik:

Zu wissen • welche Argumente gültig sind und • welche Sätze logisch wahr sind.

Logisch wahre (L-wahre) Sätze:

Zu jedem gültigen Argument gibt es einen korrespondierenden, logisch wahren Satz.

Gültig: $(p\rightarrow q), p \,/\, q$ Logisch wahr: $((p\rightarrow q)\wedge p) \rightarrow q$

Es gibt auch logisch wahre Sätze, die kein korrespondierendes, gültiges Argument haben. z.B. $p\vee\neg p$, $\neg(p\wedge\neg p)$, etc.

Ein Satz ist logisch wahr/falsch, gdw. er wahr/falsch ist ...

- *in allen Interpretationen seiner nichtlogischen Symbole* (semantische Charakterisierung)
- *einzig Aufgrund seiner logischen Form/Struktur* (syntaktische Charakterisierung) (Jeder Satz dieser Form ist logisch wahr/falsch)

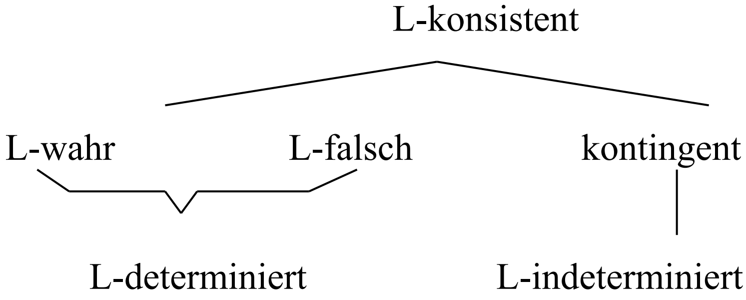
(Ein logisch wahrer Satz wird auch gültig genannt.)

Ein Satz, der logisch falsch ist, wird *kontradiktorisch* genannt.

Ein Satz, der nicht logisch falsch ist, wird *logisch konsistent* genannt.

Ein Satz, der logisch wahr, oder logisch falsch ist, wird *logisch determiniert* genannt.

Andernfalls ist ein Satz *kontingent* (logisch indeterminiert).



Logische vs. extralogisch-analytische Wahrheiten:

Ein Kreis hat Ecken, oder er hat keine Ecken

$\forall x(Kx \rightarrow (Ex \vee \neg Ex))$

Ein Kreis hat keine Ecken

$\forall x(Kx \rightarrow \neg Ex)$

Ein Satz ist *extralogisch-analytisch wahr*, gdw seine Wahrheit durch die Bedeutung seiner nichtlogischen Symbole determiniert ist, unabhängig von Fakten der Welt.
Im Gegensatz zu logischen Wahrheiten ist seine Wahrheit nicht alleine durch die Bedeutung seiner logischen Symbole determiniert.
– Analoges gilt für die Gültigkeit von extralogisch-analytischen Argumenten.

Übungen

1.1: Welches der folgenden Argumente ist logisch gültig: (i) Alle Tiere sind Instinktwesen. Keine Pflanze ist ein Tier. Also ist keine Pflanze ein Instinktwesen. (ii) Alle Tiere sind Instinktwesen. Kein Mensch ist ein Instinktwesen. Also ist kein Mensch ein Tier. (iii) Alle guten Menschen sind vernünftig. Alle Menschen sind gut. Also sind alle Menschen vernünftig. (iv) Alle schlechten Menschen sind unvernünftig. Alle unvernünftigen Menschen sind schlecht. Also sind alle Menschen unvernünftig.

1.2: Welche der folgenden Argumente sind (a) logisch (deduktiv) gültig, (b) extralogisch-analytisch gültig, (c) induktiv oder probabilistisch 'gültig', (d) nichts dergleichen: (i) Alle Menschen sind sterblich. Aristoteles ist ein Mensch. Also ist auch Aristoteles sterblich. (ii) Die meisten Lichtschalter funktionieren. Ich drücke den Lichtschalter. Also geht das Licht an. (iii) Alle verheirateten Personen genießen eine Steuerbegünstigung. Paul und Maria sind ein Ehepaar. Also genießen Paul und Maria eine Steuerbegünstigung. (iv) Bisher hat mein Kühlschrank gut funktioniert. Also kann ich mich auch in Zukunft auf ihn verlassen. (v) Immer wenn Gregor von seinem Bruder spricht, nimmt sein Gesicht gespannte Züge an. Also nimmt Gregors Gesicht auch jetzt, wo er gerade von seinem Bruder spricht, gespannte Züge an. (vi) Immer wenn Gregor von seinem Bruder spricht, nimmt sein Gesicht gespannte Züge an. Also hat Gregor gegenüber seinem Bruder einen Minderwertigkeitskomplex. (vii) Alle Raben sind schwarz. Dieser Vogel ist kein Rabe. Also ist er auch nicht schwarz. (viii) Abtreibung ist vorsätzliche Tötung eines Embryos. Ein Embryo ist ein menschliches Lebewesen. Also ist Abtreibung Mord.

1.3 Welcher der folgenden wahren Sätze ist logisch wahr, extralogisch-analytisch wahr, oder synthetisch (d.h. nicht-analytisch) wahr: (a) Kein unzerlegbarer Gegenstand ist zerlegbar, (b) Jeder unzerlegbare Gegenstand ist atomar, (c) Jedes Atom besteht aus Protonen, Neutronen und Elektronen, (d) stabile Demokratien sind nicht krisenanfällig, (e) Demokratien können krisenanfällig oder nicht krisenanfällig sein, (f) Demokratien können nur stabil sein, wenn sie eine stabile Wirtschaft besitzen.

1.2 Syntax - Semantik (- Pragmatik) (Charles Morris)

Zwei Aspekte von Bedeutung:

	Intension (Bedeutung, Freges Sinn)	*Extension* (Referenz, Freges Bedeutung)	
Satz:	Proposition, Weltzustand	Wahrheitswert -------	AL
Prädikats:	Eigenschaft	Klasse	PL
Individuen-Term:	Charakteristisches Cluster von Eigenschaften	Objekt	

Für die Semantik der formalen Logik werden nur die Extensionen gebraucht.

Ein logisches System besteht aus:

1. *Einer logischen Grammatik:* Definition des formalen Gebrauchs seiner Sprache und seine Formregeln (logische Grammatik) } SYNTAX
2. *Einer Semantik:* Definitionen und Regeln von semantischer Interpretation. Semantische Definition von Logischer Wahrheit und Gültigkeit (s.o.) } SEMANTIK

$\models$ steht für die semantische Gültigkeit eines Argumentes

Semantische Theoreme (z.B. über Entscheidungsverfahren etc.)

3. *Einer Beweistheorie:* Ein deduktives Kalkül: eine Menge von Axiomen, Regeln und /oder Meta-Regeln der Deduktion plus einer Definition von Beweisbarkeit und Ableitbarkeit.

$\vdash$ steht für syntaktische Beweisbarkeit (Ableitbarkeit) eines Argumentes } SYNTAX

Syntaktische Theoreme (z.B. über Entscheidungsverfahren etc.)

4. Ein Beweis der Korrektheit und (wenn möglich) Vollständigkeit. ——— SYNTAX+SEMANTIK

Warum haben wir diese Aufteilung der Logik in Semantik ||— *und Beweis* |—?

… Das ist eine lange Geschichte. Es ist ein grundlegendes Charakteristikum der modernen Logik.

Die meta-mathematische Motivation:

→ Beweistheorie befasst sich mit konkreten/finiten Entitäten: syntaktische Regeln (Algorithmen)

→ Die Semantik befasst sich mit abstrakten Entitäten: (potentiell infinite) mengentheoretische Modelle.

Ist jede mathematische Intuition algorithmisch korrekt u. gültig? (Antinomien?)

Kann mathematisches Schließen komplett computerisiert werden? (KI)

Die philosophische und psychichologische Motivation:

Regelbasiertes Denken und *modellbasiertes Denken* sind zwei grundlegende Arten des Denkens, die manchmal miteinander konkurrieren; doch sie sind eigentlich komplementär.

Definitionen von fundamentalen meta-theoretischen Konzepten:

Korrektheit: Beweisbarkeit ⇒ Gültigkeit/L-Wahrheit

schwach: für Sätze stark: für Argumente

Vollständigkeit: Gültigkeit/L-Wahrheit ⇒ Beweisbarkeit

schwach: für Sätze stark: für Argumente

Entscheidbarkeit: Ein Konzept C (z.B. Gültigkeit) ist entscheidbar gdw es einen *Algorithmus gibt* der eine korrekte ja/nein Antwort auf die Frage "ist x ein C?" hervorbringt, nach einer endlichen Anzahl von Schritten (für alle Entitäten x für die C definiert ist).

Definition eines Algorithmus: jede Prozedur, die in eine arithmetische Prozedur übersetzt werden kann. Eine derartige Prozedur wird auch 'mechanisch' genannt.

1.3 Objektsprache vs. Metasprache, formale Logik vs. informelle Mengenlehre

- Die Objektsprache ist die Sprache, die untersucht wird.
- Die Meta-Sprache ist die Sprache in der wir die Eigenschaften unserer Objektsprache, oder ihre Relation zur Welt-wie-in-Metasprache-beschrieben, ausdrücken.

Tarski, Gödel …

Gebrauch (nicht zitiert) vs. Erwähnung (zitiert):

Objektsprache	*Metasprache*
Schnee ist weiß	"Schnee ist weiß" ist wahr gdw. Schnee weiß ist. "Schnee ist weiß, oder Schnee ist nicht weiß" ist ein logisch wahrer Satz.

Die Theorie der formalen Objektsprachen und ihren logischen Eigenschaften, ausgedrückt mit den Mitteln der informellen Mengenlehre nennt man auch *Metalogik.*

Vereinbarung: Wir sprechen immer in der Metasprache. Alle objektsprachlichen Ausdrücke werden implizit als zitiert gebraucht. Wir vermeiden so alle Anführungszeichen.

Formale Objektspr.	*Natürliche Metasprache*	*Mathemat. Metaspr.*
$p \wedge q$	"$p \wedge q$" ist wahr	$I \models\!= (p \wedge q)$
$(p \to q), p \ / \ q$	"$(p \to q), p \ / \ q$" ist ein gültiger Schluss	$(p \to q), p \ \Vdash\!\!-\ q$

Anmerkung: Unsere Konvention, keine Zitate zu verwenden, bedeutet, dass wir objektsprachliche Ausdrücke in unserer Metasprache als Namen für selbige verwenden. In der Metasprache sind unsere terminologischen Konventionen relativ frei. Wir benutzen in der Metasprache oft dieselben logischen Symbole, wie in der Objektsprache - sofern der Kontext klarstellt, was objekt- und was metasprachlich ist.

Ausnahmen sind:

	Objektsprache	Metasprache
wenn-dann	$\rightarrow$	$\Rightarrow$
Identität	$\equiv$	$=$

1.4 Extensionale und intensionale klassische Logik:

Semantische Grundlagen der klassischen Logik

1 Jeder Satz ist entweder wahr, oder falsch (*Zweiwertigkeit)*

1a: Prinzip des ausgeschlossenen Dritten: $p \vee \neg p$ (Aristoteles:1c:Identität: a=a)

1b: Prinzip des ausgeschlossenen Widerspruchs: $\neg(p \wedge \neg p)$

Arten von Satzoperatoren:

extensional (wahrheitswertfunktional)	*intensional (nicht-wahrheitswertfunkt.)*
nicht p (es ist nicht der Fall, dass p)	es ist notwendig, dass p
p und q	es ist geboten, dass p
…	…

Ein Satzoperator ist *extensional* (wahrheitsfunktional) gdw der Wahrheitswert des gesamten Satzes, in dem er vorkommt, vollständig durch die Wahrheitswerte seiner Argumente bestimmt ist. Ansonsten ist er *intensional* (nicht-wahrheitsfunktional).

Klassische Aussagenlogik = die Logik der extensionalen Satzoperatoren.

Interpretationen/Modelle sind beschränkt auf die Zuordnungen der Wahrheitswerte.

Klassische Prädikatenlogik 1. Ordnung ist extensional im mengentheor, Sinne:

Der Wahrheitswert eines Satzes ist vollständig determiniert durch:

- die Extension von Individuentermen (Objekte)
- die Extension von Prädikatensymbolen (Klassen)
- die Extension des Bereichs "Dm" (Domain) der Quantoren

Fa ist wahr gdw $I(a) \in I(F)$ $\forall x Fx$ ist wahr gdw $\forall d \in Dm: d \in I(F)$ etc.

(I – Die extensionale Interpretations-Funktion)

Modale Aussagenlogik - berücksichtigt auch intensionale Satzoperatoren

$\Box p$ für notwendig p, $\Diamond p \leftrightarrow \neg\Box\neg p$ für möglich p

Interpretationen werden in Bezug gesetzt zu *möglichen Welten*.

$\Box A$ ist wahr gdw A in allen möglichen Welten wahr ist.

Formale Modallogik behandelt mögliche Welten als 'Individuen' ('Punkte');

$\Rightarrow$ in diesem Sinne reduziert sie die Intension auf *Extension über mögliche Welten*.

Klassische Logik: AL und PL AL = wahrheitswertfunktionale AL

Erweiterte klassische Logik: M-AL and M-PL (lässt intensionale Operatoren zu)

Einige wichtige Namen in der Geschichte der Logik:

Aristoteles: um 350 v.Chr. Syllogistik 300 v.Chr. Stoische Logiker

um 1200 n.Chr. Scholastische Logik (kaum Fortschritte...)

AL: um 1850 George Boole Mengenlehre: um 1880 Georg Cantor

PL: um 1880 Gottlob Frege, Charles S. Peirce

um 1900-20 Bertrand Russell, Ludwig Wittgenstein

um 1930 Kurt Gödel, Alfred Tarski, …. (Metalogische Resultate, Semantik)

Modallogik: um 1920 Clarence Irving Lewis, 1945 Rudolf Carnap,

1960 Saul Kripke, Jakkoo Hintikka …

1.5 Beispiele nicht-klassischer (deduktiver) Logiken und nicht-logischer, analytischer Wahrheiten

- *Nichtklassische Logiken:* - Nehmen nicht das Prinzip der Zweiwertigkeit an.

Intuitionistische Logik:

p wird behauptet --> p hat einen konstruktiven Beweis

$\neg$p wird behauptet --> es gibt einen konstruktiven Beweis von p zu einem Widerspruch

intuit. gültig: $\neg(p \wedge \neg p)$, $p \rightarrow \neg\neg p$ intuit. ungültig: $p \vee \neg p$, $\neg\neg p \rightarrow p$

- *Mehrwertige Logiken, Quantenlogik:*

Ein Satz kann einen dritten, “unbestimmten” Wahrheitswert haben {w, u, f}

Übungen:

1.4 Diskutieren Sie das Zweiwertigkeitsprinzip der klassischen Logik.
Was bedeutet die Annahme eines Wahrheitswertes "unbestimmt" für unsere ontologische Auffassung der Welt?

1.5 Wie könnten vernünftige Wahrheitstafeln mit drei Wahrheitswerten {w,u,f} für die Negation, Konjunktion, Disjunktion und materiale Implikation aussehen?

1.6 Überlegen Sie sich eine Methode, die dreiwertige Logik auf die zweiwertige Logik innerhalb einer erweiterten Sprache zurückzuführen, aufgrund der folgenden Beobachtung: p kann wahr, unbestimmt oder falsch sein; aber "p ist unbestimmt" ist entweder wahr oder falsch.

2. Naive und informelle Mengenlehre (in informeller PL !)

2.1 Grundlegende Konzepte, Prinzipien und Definitionen

Eine *Menge* = eine 'Sammlung' von *Objekten/Individuen* (beliebiger Art), die selbst als einzelnes Objekt (als Individuum) betrachtet wird.
Eine Menge lässt sich charakterisieren

– rein extensional, durch Auflisten ihrer Elemente
  (nur bei endlichen Mengen möglich): $\{a_1,\ldots,a_n\}$

– durch eine gemeinsame Eigenschaft: $\{x: Px\}$ = die Menge aller Objekte x,
  für die "Px" gilt.

– durch eine rekursive Definition: *z.B. die natürlichen Zahlen:*
  $0 \in |N$, und wenn $n \in |N$, dann $(n+1) \in |N$; sonst nichts.

Ein Objekt, das keine Menge ist: ein *Urelement.*

Wichtige Charakteristiken von Mengen: sie sind invariant gegenüber Permutationen und Wiederholung ihrer Elemente: $\{a,b\} = \{b,a\} = \{a,a,a,b,b\}$ etc.

Achtung: Die naive Mengenlehre nimmt an, dass es für jede Eigenschaft P(x) eine korrespondierende Menge gibt $\{x:P(x)\}$, genannt: die *Extension* von P.

1.) Naives Komprehensions--Axiom: für alle P: $\exists x(x = \{y: Py\})$.
(Frege's Formalisierung der Cantorschen Mengenlehre.)

Hinweis: $\{a_1,\ldots,a_n\} = \{x: x=a_1 \vee \ldots \vee x=a_n\}$

$$Px := x=a_1 \vee \ldots \vee x=a_n$$

2.) Das zweite Axiom der naiven Mengenlehre: *Axiom der Extensionalität:*

Für alle Mengen A und B: *wenn* für alle x, $x \in A \Leftrightarrow x \in B$, *dann* A = B.

$\forall A,B(\forall x(x \in A \Leftrightarrow x \in B) \Rightarrow A=B)$.

Die Richtung $\Leftarrow$ folgt bereits aus dem *logischen Axiom der Ersetzung von Identischem*, z.B. wenn A=B, dann $\forall x(x \in A \Leftrightarrow x \in B)$.

Extensionsgleiche Eigenschaften:

{x : x ist ein lebender Organismus} = {x: x's Reproduktion basiert auf RNS oder DNS}

Terminologische Konventionen:

A,B (indiziert)… stehen für beliebige Mengen.

a,b (indiziert) … stehen für beliebige Urelemente.

Variablen x, y (indiziert $x_1, x_2,\ldots$) variieren über Mengen *oder* Urelemente.

Ausnahme von der Groß-/Kleinschreibungs-Konvention: f, g (indiziert) … für Funktionen = Mengen.

Die einzigen Prädikate (Relationen) der Mengenlehre sind die logische Relation "=" der Identität und die primitive (in der PL nicht-logische, aber im weiteren Sinne logisch-mathematische) Relation "$\in$":

$a \in A$ – Objekt a ist ein Element der Menge A

$a \notin A$ ist Abkürzung für nicht $a \in A$ $\qquad$ $a \neq b$ ist Abkürzung für nicht a = b.

$a,b \in A$ ist Abkürzung für $a \in A$ und $b \in A$.

$=_{df}$ (oder auch =:) steht für Identität per Definition

$\{x \in A: Px\}$ ist Abkürzung für $\{x: x \in A \wedge Px\}$

$\forall x,y$: Pxy oder $\forall x,y(Pxy)$ – steht für $\forall x \forall y Pxy$ steht für: auf alle x und y trifft P zu.

$\forall x \in A$: Px – steht für $\forall x(Ax \Rightarrow Px)$ steht für: auf alle x in A trifft P zu.

Komprehensionsaxiom:

Russell's Antinomie (1903) zeigt, dass diese Annahme nicht generell zutrifft:

Die Annahme der Existenz einer Menge R := $\{x : x \notin x\}$ führt zu einem Widerspruch.

Um dies zu sehen, frage man sich ob $R \in R$?

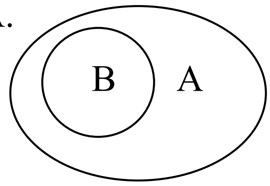
$\rightarrow$ wenn $R \in R$, dann $R \notin R$. Und wenn $R \notin R$, dann $R \in R$. *Widerspruch!*

Der Rest der naiven Mengenlehre sind Definitionen.

Definition (Teilmenge):

$B \subseteq A$ gdw für alle x: $x \in B \Rightarrow x \in A$. (B ist in A enthalten).

Def.: Echte Teilmenge: $B \subset A$ gdw $B \subseteq A$ und $B \neq A$.



Definition (Vereinigungsmenge):

$A \cup B =_{df} \{x: x \in A \vee x \in B\}$ = die Vereinigung von A und B (Skizzen zeichnen!)

Definition (Schnittmenge)*:*

$A \cap B := \{x: x \in A \wedge x \in B\}$ = die Schnittmenge von A und B

Definition (relatives und absolutes Komplement):

$A - B := \{x: x \in A$ und $x \notin B\}$ (auch: $A \setminus B$) ($= A \cap B^c$)

Die mengentheoretische Differenz A minus B = das 'relative' Komplement von B in Bezug auf A.

$A^c =_{df} \{x: x \notin A\}$ ('absolutes' Komplement von A; relativ zu einem Objektbereich D) ($= D - A$)

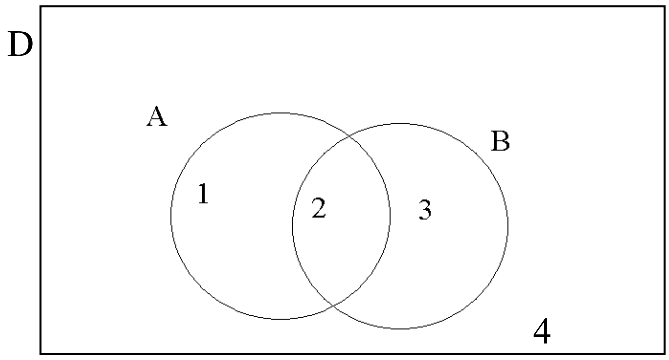
Definition (Potenzmenge):

$\mathbb{P}(A) := \{x: x \subseteq A\}$ = Potenzmenge von A (Menge aller Teilmengen)

Definiton: |A| := die Kardinalität der Menge A = die Anzahl von A's Elementen.
(Beachte: $|\{a,a\}| = |\{a\}| = 1$.)

Definition: Leere Menge $\varnothing$ (= { }): $\forall x$: $x \in \varnothing \Leftrightarrow x \neq x$.
Äquivalent: $\forall x$: $x \notin \varnothing$. (Denn es gilt PL-Axiom: $\forall x(x=x)$).

Übung 2.1: Nehmen Sie die folgenden zwei Mengen an, beide sind Teilmengen eines Objektbereichs D, auf die sich das absolute Komplement bezieht:



2.2 Zeigen Sie auf, auf welche Teilmengen der Grundmenge (1,2,3,4) sich die folgenden Mengen erstrecken: $A \cup B$, $A \cap B$, $A - B$, $B - A$. A^c, B^c, $A^c \cup B^c$, $A^c \cap B^c$.

2.3 Welche Menge ist $A \cap A^c$? Welche Menge ist $A \cup A^c$? Welche Menge ist $A - A^c$? Welche Menge ist $A - A$? Erläutern Sie warum $\varnothing \subseteq A$.
2.4. Was ist die Vereinigung von {1,2,3} und {4,5,3}?

2.5. Beweisen Sie: (a) $(A - B) \subseteq A$. (b) $A \subseteq A \cup B$. (c) $A \cap B \subseteq A$.
2.6. Zeigen Sie: $\max(|A|, |B|) \leq |A \cup B| \leq |A| + |B|$, wenn A und B *endliche* Mengen sind.
2.7. zeigen Sie, für endliche Mengen: $|A \cup B| = |A| + |B| \Leftrightarrow$ A und B sind disjunkt (haben keine gemeinsamen Elemente)

2.8. Es seien $A = \{1,3,4,5,6\}$, $B = \{3,5,7,8\}$, $C = \{2,3,6,9\}$. Konstruieren Sie $A \cap B$, $B \cap C$, $A \cup B$, $A \cup C$, $(A \cap B) \cup (A \cap C)$, $A - B$, $(A - B) - C$, $A - (B \cap C)$, $(A - B) \cup (B - C)$.

2.9. Konstruieren Sie alle Mengen von $|P(\{1,2,3\})$.

2.10. Beweisen Sie:

(a) $A \cup A^c$ = All-Menge (Objektbereich), (b) $A \cap A^c = \emptyset$, (c) $(A \cup B)^c = (A^c \cap B^c)$, (d) $(A \cap B)^c = (A^c \cup B^c)$, (e) $(A^c)^c) = A$, (f) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, (g) $A - B = A \cap B^c$

2.11. Reflektieren Sie die Ergebnisse aus (2.10): welche Beziehung besteht zwischen den Operatoren $\cup$, $\cap$, ^{c} der Mengenlehre und den Konnektiven der Aussagenlogik?

2.12. Beweisen Sie: $B \subseteq A$ gdw $B \in |P(A)$.

2.2 Relationen und Funktionen

Ein geordnetes n-Tupel: $<a_1,\ldots,a_n>$. *Ein geordnetes Paar:* $<a,b>$.

Eine *Liste* von Elementen. Berücksichtigt die Anordnung der Elemente; akzeptiert Wiederholungen der Elemente.

$<a,b> \neq <b,a>$. $<a,a> =$ ein 2-Tupel.

Man kann n-Tupel als *primitiv* verstehen, oder sie ansonsten mengentheoretisch *definieren*.

1) n-Tupel als primitiv: $\rightarrow$ sie müssen erfüllen

$<a_1,\ldots,a_n> = <b_1,\ldots,b_m>$ gdw (i) n=m und (ii) $a_i = b_i$ für alle $1 \leq i \leq n$.

(i) Dieselbe Anzahl von Plätzen der beiden Listen (ii) An jedem Platz steht dasselbe Element in beiden Listen.

2) Es gibt verschiedene Möglichkeiten, n-Tupel zu definieren.

Rekursive Definition von n-Tupeln nach Kuratowski:

Start: $<a,b> := \{\{a\},\{a,b\}\}$.

Rekursion (Iteration): $<a_1,\ldots,a_n,a_{n+1}> =_{df} < <a_1,\ldots,a_n>, a_{n+1}>$.

Spezialfall: $<a> := a$; $< > := \emptyset$.

Iterationen werden schnell kompliziert – *aber man muss niemals die mengentheoretische Definition von n-Tupeln ausformulieren.*

Notation: $<a_i : 1 \leq i \leq n> = <a_1,\ldots,a_n>$.

Mit einem *Glied* eines n-Tupels $<a_i : i=n>$ referieren wir immer auf irgendein a_i.

Die generelle Struktur einer rekursiven (induktiven) **Definition**:

Gegeben: eine so genannte quasi-wohlgeordnete Menge A:

Ihre Elemente sind *angeordnet nach Rängen* durch natürliche Zahlen (Quasi-Ordnung): Elemente des Ranges 0, 1, 2,…

⇒ *Rekursive Definition einer Eigenschaft* $C \subseteq A$ *auf A:*

Startklausel: C(a) ist definiert für alle Elemente a des Ranges 0.

Rekursive Klausel(n): für alle Elemente $x \in A$ des Ranges n wird der Besitz der Eigenschaft C (also C(x)) definiert durch den Besitz der Eigenschaft C durch bestimmte Elemente y also C(y);), deren Rang *niedriger ist* als n.

Darauf bezieht sich: Axiom der starken Induktion.

Spezialfall: C(x) wird definiert mit Hilfe von C(y) für bestimmte Elemente y vom *Rang n–1*. Darauf bezieht sich: Axiom der schwachen Induktion.

Wichtig: Auch wenn das Definiendum-Prädikat im Definiens auftaucht, führt eine rekursive Definition nicht in einen Zirkel oder infiniten Regress.

Beispiel rekursiver Def: Startklausel: Adam und Eva waren Menschen.

Rekursive Klausel: x ist ein Mensch wenn x's Eltern Menschen waren.

Vgl. dazu die nicht-rekurisve Def. (Aristoteles):

Definiendum		Definiens
x ist ein Mensch	$\Leftrightarrow_{df}$	x ist ein rationales Tier

Rekursive Definitionen benötigt man, um die fundamentale Beweistechnik der mathematischen Induktion anwenden zu können

(nicht zu verwechseln mit empirischer bzw. Humeschen Induktion)

Naive Arithmetik: *Vorausgehende* Fakten über **natürliche Zahlen:**

$\mathbb{N}$ - die Klasse aller natürlichen Zahlen 0, 1, 2, …

i, j, n, n_1, n_2… variiert über Elemente von $\mathbb{N}$.

Fakten: 1. < ist eine strikte und totale (lineare) Ordnungsrelation < über $\mathbb{N}$, und ≤ die korrespondierende (totale, oder lineare) schwache Ordnung über $\mathbb{N}$, definiert durch $n \leq m =_{df} n < m \vee n = m$. (Hinweis: metasprachl. Identität, nicht Äquivalenz)

2. 0 ist das kleinste Element von $\mathbb{N}$: $\forall n \in \mathbb{N}, n \geq 0$.

3. Jedes $n \in \mathbb{N}$ hat einen direkten Nachfolger, n+1.

4. Jedes $n \in \mathbb{N}$ verschieden von 0 hat einen direkten Vorgänger, n-1.

Axiom der schwachen Induktion (WI weak induction): Für jede Eigenschaft P:

$$\left.\begin{array}{l} \text{Start:} \quad P(0) \\ \forall n\,(\underbrace{P(n)}_{\text{IH (Induktionshypothese)}} \Rightarrow P(n+1)) \end{array}\right\} \Longrightarrow \forall n P(n)$$

Induktionsschritt (IS)

Anwendung der WI: Auf $\mathbb{N}$, oder auf einer beliebigen unendliche Menge, deren Elemente Ränge besitzen, indiziert durch natürliche Zahlen.

Quasi-Ordnung: mehrere ranggleiche Elemente werden zugelassen.

Die Eigenschaft P allquantifiziet dann über Elemente gleichen Rangs, d.h. $\forall x \in \text{Rang}(n):P(x) \Rightarrow \forall x \in \text{Rang}(n+1):P(x)$.

Übungen 2.13. Beweisen Sie durch schwache Induktion nach n: wenn Menge A n Elemente hat, dann hat $\mathbb{P}(A)$ 2^n Elemente.

2.14 Beweisen Sie durch schwache Induktion, dass $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

2.15 Beweisen Sie durch schwache Induktion, dass $2^{n+1} = \Sigma_{0 \leq i \leq n} 2^i + 1$.

Starke Induktion (strong induiction s.I.): Für jede Eigenschaft P:

$\forall m<n$: $P(m) \Rightarrow P(n)$ $\Longrightarrow$ $\forall nP(n)$

→ *Diese Form wird in induktiven Beweisen der Metalogik häufig angewendet.*

Übung 2.15a: zeige warum s.I. logisch anscheinend stärker ist als wI, indem man zeige: Wenn A ||— A', dann (A→B)→C ||— (A'→B)→C (||— logische Folgerung .:)

Theorem: Schwache und Starke Induktion sind äquivalent.
Achtung: Dieses Theorem gehört in seiner Schwierigkeitsstufe erst ins Ende des Kurses. Es jedoch eine wichtige Voraussetzung, um Metalogik zu betreiben (man erinnere sich an den Zirkel von Logik und Metalogik). Daher stellen wir seinen Beweis schon hier vor, in einer semi-formellen Notation. Wir fassen oft mehrere PL-Schritte in 'einen Schritt' zusammen, in ähnlicher Form wie dies im informellen mathematischen Beweisen geschieht.

Zu informellen Beweisen: in der informellen Logik (Mathematik) wird nicht, so wie in der Logik I, zwischen gebundenen Individuenvariablen (x, y, …) und freien Individuenvariablen (a, b,…) *syntaktisch* unterschieden. Es wird einfach angenommen: wird x (y,...) durch einen Quantor gebunden, so fungiert x als gebundene Iv.,, und wenn nicht, fungiert es wie eine freie Iv. Der Schluss der universellen Instanziierung (UI) kann daher auch die Form ∀xA[x] / A[x] haben, und der Schluss der universellen Generalisierung die Form A[x] / ∀xA[x]. [Hinweis: Die Variablenbedingung aus Logik I für quantifizierte Formeln und Schlüsse der Form ∀xA[x] / A[t/x] wird durch Bedingung für korrekte Termsubstitution "A[t/x]" ersetzt (s. später).]
(in der informellen Logik schreibe ich ⇒ statt →)

Übung 2.16: Strong Induction (SI) ⇒ Weak Induction (WI):

Beweis der Richtung: weak induction (WI) $\Rightarrow$ strong induction (SI):

Der Trick besteht darin, die Eigenschaft "$\forall y<x{:}Py$" als komplexe Eigenschaft "Qx" zu betrachten und darüber schwache Induktion zu betreiben.
In Schritten (6) und (14) wird das Antecedens der schwachen Induktion für die komplexe Eigenschaft "Q" schließlich etabliert.
In den Schritten 4a bis 4e wird exemplarisch gezeigt, wie ein typischer informell-mathematischer Schritt von (4) zu (5) in kleinere Einzelschritte zerlegt werden kann, die Regeln des PL-Kalküls entsprechen, welche wir erst im hinteren Teil dieses Skriptums im Detail entwickeln werden.

(1) (Antecedens-SI:) $\forall x(\forall y<xPy \Rightarrow Px)$	KB-Ann
(2) $Qx :\Leftrightarrow \forall y<x{:}Py$	*Definition* (eliminierbare Prämisse)
(3) $\forall x(Qx \Rightarrow Px)$	1+2, Ersetz. von Äquival., Theorem PL
(4) $\neg\exists y{:}\ y < 0$	**Prämisse** über |N
4a $\neg\exists yA \Rightarrow \forall y\neg A$	*PL-Theorem (beliebige A)*
4b $\forall y{:}\neg\, y<0$	*MP 4, 4a-Instanz*
4c $\neg\, y < 0$	*UI 4b*
4d $\neg A \Rightarrow (A \Rightarrow B)$	*AL-Theorem (beliebige A, B)*
4e $(y<0 \Rightarrow Py)$	*MP 4c, 4d-Instanz*
(5) $\forall y<0{:}\ Py$	UG 4e (mehrere PL-Schritten aus 4)
(6) $Q(0)$	Ersetz v. Äquival. aus (5) und (2)
(7) Qa	KB-Ann
(8) $\forall y < a{:}\ Py$	Ersetz Äquiv (2), (7)
(9) Pa	aus (3), (7) mit UI und MP
(9a) $\forall y=a{:}\ Py$	PL-Schritt aus (9)
(10) $\forall y < (a+1){:}\ y < a \vee y = a$	**Prämisse** über |N
(11) $\forall y<(a+1){:}\ Py$	*durch PL-Schritte aus 8,9a,10*
(12) $Q(a+1)$	Ersetz Äquiv 2, 11
(13) $Q(a) \Rightarrow Q(a+1)$	KB 7-12
(14) $\forall x(Q(x) \Rightarrow Q(x+1))$	UG 13, VB bzgl a erfüllt
(15) $(Q(0) \wedge \forall x(Qx \Rightarrow Q(x+1)) \Rightarrow \forall xQx$	**Präm.** Weak. Ind.
(16) $\forall xQx$	*AL-Schritte aus 6,14 und 15*
(17) $\forall xPx$	PL-Schritte aus 3, 16
(18) $\forall x(\forall y<xPy \Rightarrow Px) \Rightarrow \forall xPx$	KB 1-17, := Strong Ind.

***********************Ende Beweis **********************

Definition (cartesisches Produkt):

1. $A_1 \times \ldots \times A_n =_{df} \{<x_1,\ldots,x_n> \ : x_i \in A_i$ für alle $1 \leq i \leq n\}$.

2. $A^n = \underbrace{A\times \ldots \times A}_{\text{n mal}}$. Also $A^1 = A$, und $A^0 = \{<>\} = \{\emptyset\}$.

$A^2 = A\times A$

Illustration: $A \times B = \{<x,y>: x\in A \wedge y\in B\}$ (Figur)

$A \times B \times C = \{<x,y,z>: x\in A \wedge y\in B \wedge z\in C\}$ etc.

Terminologische Konvention in dieser Definition:

$\{f(x) : x\in A\} := \{y$: existiert x so, dass $y = f(x)$ und $x \in A\}$.

Achtung: das cartesische Produkt ist nicht kommutativ.

Übungen:

2.17. Schreiben Sie die Menge $\{1,3,4\} \times \{2,4,6\}$ auf.

2.18 Zeigen Sie: $A \times (B\cup C) = (A\times B)\cup(A\times C)$.

Zeigen Sie, dass $A\cup(B\times C) = (A\cup B) \times (A\cup C)$ nicht gilt.

2.19. Beweisen Sie durch schwache Induktion: wenn A n und B m Elemente hat, dann hat $A\times B$ $n\cdot m$ Elemente.

Definition (Eigenschaften, Relationen – im extensionalen Sinne):

Eine n-stellige *Relation* R über (auf) einer Klasse A ist eine Klasse von n-Tupeln von Elementen aus A – wir schreiben: $R \subseteq A^n$.

Eine *Eigenschaft* über A ist eine 1-stellige Relation über A – eine Teilmenge von A.

Wir schreiben $R(a_1,\ldots,a_n)$ für $<a_1,\ldots,a_n> \in R$.

Im Falle binärer Relationen schreiben wir aRb für $<a,b> \in R$.

Nb.: Es gibt nur zwei 0-stellige Relationen, $\{\} = \emptyset$, und $\{<>\} = \{\emptyset\}$

(:= Ordinalzahlen 0 und 1; die Wahrheitswerte von 0-stell. Prädikaten = Aussagevar.)

Generalisierung:

Eine n-stellige (typisierte) Relation *zwischen* $A_1,\ldots,A_n$ (in dieser Anordnung) ist eine Eigenschaft über $A_1\times\ldots\times A_n$.

Definition (Funktionen - im extensionalen Sinne): f, g, … (Mengen)

1. Eine (einstellige) Funktion (Abbildung) von A in (nach) B, geschrieben als $f: A \rightarrow B$, ist eine binäre Relation zwischen A und B, $f \subseteq A \times B$, welche die folgenden zwei Bedingungen erfüllt:

(1) *Funktionalität* oder *Rechtseindeutigkeit:* $\forall x,y,z$: $\langle x,y \rangle \in f$ und $\langle x,z \rangle \in f \Rightarrow y=z$.

(2) Der *Argumentbereich (Objektbereich)* von f, $dom(f) := \{x: \exists y(\langle x,y \rangle \in f)\}$, deckt alle Objekte in A: dom(f) = A ab.

– Def.: Der *Wert von f an (der Stelle) x*, geschrieben als fx oder f(x), ist das einzige y so dass $\langle x,y \rangle \in f$ (auch geschrieben: y = f(x)).

– Def.: Der *Wertebereich* von f, $ran(f) := \{y: \langle x,y \rangle \in f$ für irgendein $x\} =_{def}$ $\{f(x): x \in dom(f)\}$.

Anmerkung: $ran(f) \subseteq B$ (ran(f) kann eine echte Teilmenge von B sein).

2. Generalisierung: Eine n-stellige Funktion von $A_1,\ldots,A_n$ nach B, $f: A_1 \times \ldots \times A_n \rightarrow B$, ist eine einstellige Funktion von $A_1 \times \ldots \times A_n$ in B;

– d.h. eine (n+1)-stellige Relation über $A_1 \times \ldots \times A_n \times B$ mit

– $\forall x_1,\ldots,x_n,y,z$: $\langle x_1,\ldots,x_n,y \rangle \in f$ und $\langle x_1,\ldots,x_n,z \rangle \in f \Rightarrow y=z$.

– $dom(f) := \{\langle x_1,\ldots,x_n \rangle: \exists y(\langle x_1,\ldots,x_n,y \rangle \in f)\} = A_1 \times \ldots \times A_n$

3: Wichtige Begriffe: $f: A \rightarrow B$ ist

a) eine Funktion von A *auf* B, oder eine *surjektive* Funktion, gdw ran(f)=B.

b) eine *injektive* Funktion, oder eine eins-zu-eins (1:1) Funktion gdw sie linkseindeutig ist, d.h. gdw $\forall x,y \in dom(f)$: $x \neq y \Rightarrow f(x) \neq f(y)$.

c) eine *bijektive* Funktion gdw sie surjektiv und injektiv ist. Wir schreiben auch $f: A \rightarrow B$.

Die Klasse von Paaren $\{\langle x,y \rangle: x \in dom(f)$ und $y=fx\}$ der *Graph* der Funktion f genannt.

→ *Mengentheoretisch sind eine Funktion und ihr Graph identisch.*

Sonderfall: Eine 0-stellige Funktion von A nach B ist identisch mit einem Individuum $b \in B$

4. Für ein gegebenes $f{:}A \rightarrow B$ und die Teilmenge $C \subseteq A$, wird $f\uparrow C{:}\ C \rightarrow B$ die *Restriktion* von f auf den Argumentbereich C genannt,
und definiert durch $(f\uparrow C)(x) = f(x)$ für alle $x \in C$.

Anm.: Mit Hilfe der Konzepte von Paar und Funktion kann man n-Tupel in einer alternativen, aber äquivalenten Weise wie folgt definieren:

$\langle a_1,\ldots,a_n\rangle$ = die Funktion $f{:}\{1,\ldots,n\} \rightarrow \{a_1,\ldots,a_n\}$ sodass $f(i) = a_i$
für alle $i \in \{1,\ldots,n\}$.

Übungen:

2.19a Was ist die Menge aller Eigenschaften über eine gegebene Menge A? Was ist die kleinste Eigenschaft über A? Was ist die größte Eigenschaft über A?

2.20 Schreiben Sie die (den Graph der) binäre(n) Relationen $x > y$ (größer-als), $x=y$, und $x < y$ über $\{1,2,3,4\}^2$ auf. Zeichnen Sie den Graphen in einer Matrix mit Zeilen 1,2,3,4 und Spalten 1,2,3,4. Interpretieren Sie die 'Geometrie' des resultierenden Bildes.

2.121 Eine binäre Relation $R \subseteq A \times B$ wird *unabhängige Komposition genannt* gdw $\forall \langle x_1,y_1\rangle, \langle x_2,y_2\rangle \in R$: $\langle x_1,y_2\rangle \in R$ und $\langle x_2,y_1\rangle \in R$.
Beweisen Sie: R ist eine unabhängige Komposition gdw $R = \mathrm{dom}(R) \times \mathrm{ran}(R)$,
wobei Argument- und Wertebereich von $R \subseteq A \times B$ wie folgt definiert sind:
$\mathrm{dom}(R) = \{x \in A: \langle x,y\rangle \in R\}$, und $\mathrm{ran}(f) = \{y \in B: \langle x,y\rangle \in R\}$.

2.22 Welche der folgenden Relationen ist eine Funktion:
(a) $\{\langle n,m\rangle \in \mathbb{N}^2: m = \}$, (b) $\{\langle x,y\rangle$: y ist die Mutter of x$\}$, (c) $\{\langle x,y\rangle$: y ist der Sohn von x$\}$, (d) $\{\langle n,n+1\rangle: n \in \mathbb{N}\}$, $\{\langle x,y\rangle$: y ist der Hauptwohnsitz von Person x$\}$.

2.23 Welche der folgenden Funktionen sind injektiv, surjektiv, bijektiv:
(a) $f(n) = n+1$ on $\mathbb{N}$, (b) $f(n) = n+1$ auf Ganze Zahlen, (c) $f(r)$ = die kleinste natürliche Zahl, größer-gleich r auf reelle Zahlen, (d) $f(x)$ = die Mutter von x, auf Menschen, (e) $f(x)$ = der Ehemann von x, auf verheiratete Personen.

2.24 Definieren Sie für eine Funktion $f{:}A \rightarrow B$ ihre *Umkehrung* als die folgende Relation zwischen A und B: $f^{-1} = \{\langle y,x\rangle : \langle x,y\rangle \in f\}$.

Beweisen Sie: (a) f^{-1} ist eine Funktion gdw f injektiv ist.

(b) $dom(f^{-1}) = B$ gdw f surjektiv ist. ($dom(f^{-1}) := \{x: \exists y(\langle x,y\rangle \in f^{-1})\}$)

(c) f^{-1} ist eine bijektive Funktion gdw f eine bijektive Funktion ist,

(d) vorausgesetzt f^{-1} ist eine Funktion: $\forall x \in dom(f)$: $f^{-1}(f(x)) = x$.

3. Aussagenlogik

3.1 Die formale Sprache der Aussagenlogik

$\mathcal{L}$ - die Sprache der Aussagenlogik.

$\mathcal{L}$ wird (für gewöhnlich) mit der Menge ihrer (wohlgeformten) Formeln gleichgesetzt.

Das *Alphabet* von $\mathcal{L}$ besteht aus:

– *nichtlogischen Symbolen:* einer abzählbaren (potentiell unendlichen) Menge $\mathcal{P}$ von Aussagevariablen (propositionalen Variablen, atomaren Sätzen) $p_1, p_2, \ldots, q, \ldots \in \mathcal{P}$.

– *logischen Symbolen:* (Konnektiven, Operatoren): $\neg$, $\vee$, $\wedge$, $\rightarrow$ (als grundlegend verwendet)

– *Hilfssymbolen*: Klammern (,) – sie sind Teil der logischen Symbole.

Formal: das Alphabet $A(\mathcal{L}) := \mathcal{P} \cup \{\neg,\vee,\wedge,\rightarrow,(,)\}$

Hinweis: Für die klassische Logik, würde z.B. $\{\neg,\vee\}$ als Grundlage reichen; in der intuitionistischen Logik (zum Vergleich) sind $\{\neg,\vee,\wedge,\rightarrow\}$ notwendig.

Eine *Zeichenreihe* (*Konkatenation, String*) von $\mathcal{L}$-Symbolen wird $\mathcal{L}$-Zeichenreihe genannt.

Beispiele: $p\rightarrow,$ $\neg p,$ $)\wedge q\neg,$ etc. (die meisten davon sind nicht wohlgeformt!)

Definition: Die *Länge* einer Formel = die Anzahl der Vorkommnisse alphabetischer Symbole in der Formel, inklusive Klammern, und ohne Klammerkonventionen.

Anm.: Eine $\mathcal{L}$-Zeichenreihe kann mengentheoretisch als die Abbildung eines Anfangsmenge natürlicher Zahlen (n+1 = Länge) in das Alphabet $A(\mathcal{L}) =_{df} \mathcal{P} \cup \{\neg,\vee,\wedge,\rightarrow,(,)\}$ von $\mathcal{L}$ definiert werden. Z.B.: $(p\wedge\neg q)$ ist die Abbildung s: $\{0,1,2,3,4,5\} \rightarrow A(\mathcal{L})$ sodass: $s(0) = ($, $s(1) = p$, $s(2) = \wedge$, $s(3) = \neg$, $s(4) = q$, $s(5) =)$. Wir erlauben auch *die leere Zeichenreihe* " ".

$s, s_1, \ldots$ seien Meta-Variablen, die über Zeichenreihen variieren (laufen).

$S(\mathcal{L})$ ist die Menge aller $\mathcal{L}$-Zeichenreihen, inklusive der *leeren* Zeichenreihe.

Definition (wohlgeformte Formel, wff, $\mathcal{L}$): Für alle $s \in S(\mathcal{L})$.

1. (Start): $s \in \mathcal{P} \Rightarrow s \in \mathcal{L}$
2. $s \in \mathcal{L} \Rightarrow \neg s \in \mathcal{L}$
3. $s_1, s_2 \in \mathcal{L} \Rightarrow (s_1 \vee s_2) \in \mathcal{L}$

   $(s_1 \wedge s_2) \in \mathcal{L}$

   $(s_1 \rightarrow s_2) \in \mathcal{L}$

(4. nichts sonst ist eine Formel)

Der *Grad der Komplexität* einer Zeichenreihe = die Anzahl der Vorkommnisse von Konnektiven, die darin enthalten sind. Dieser Grad definiert die Quasi-Wohlordnung für $S(\mathcal{L})$ und für $\mathcal{L}$.

→ *Die obige Definition ist rekursiv über dem Grad der Komplexität.*

Die "nichts sonst"-Bedingung ergibt sich implizit aus einer rekursiven Definition:

$\mathcal{L}$:= die *kleinste* Menge von Zeichenreihen, abgeschlossen unter den Regeln 1., 2. und 3.

Beispiel für eine nicht-rekursive Formregel wäre:

$\neg s \in \mathcal{L} \quad \Rightarrow \quad s \in \mathcal{L}$ ihre Anwendung führt zu einem infiniten Regress

$\ldots \quad \neg\neg s \quad \Leftarrow \quad \neg s \quad \Leftarrow \quad s$: prüfen Sie s!

Anmerkung: Auch wenn $\mathcal{P}$ finit ist, gibt es unendlich viele Sätze.

Aber wir werden später zeigen, dass es in diesem Fall nur endlich viele paarweise logisch nicht-äquivalente Sätze gibt.

-> *Ab jetzt* sind A, B,… (indiziert) Metavariablen, die über Formeln laufen (so genannte *Schemata*). Γ, Δ,… (indiziert) sind Metavariablen, die beliebige (potentiell unendliche) Mengen von Formeln nach Rängen ordnen.

Jede rekursive Definition von $C \subseteq A$ kann, im Prinzip, in eine nicht-rekursive transformiert werden, durch die Methode einer finiten Konstruktion für jedes Element von $C \subseteq A$. Am Beispiel von wffs:

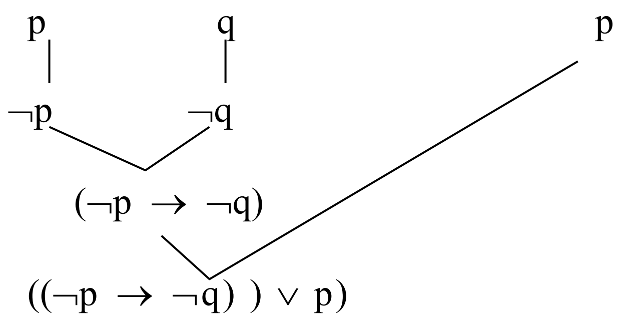
Definition (g-Konstruktion):

Eine g(rammatische)-Konstruktion einer Zeichenreihe s ist eine finite Sequenz $\langle s_1,\ldots,s_n \rangle$ von Zeichenreihen, sodass $s_n = s$ und jedes Glied s_i durch die Startregel 1, oder durch ein vorangegangenes Glied, nach den Regeln 2 oder 3, konstruiert wird. d.h.: für jedes i gibt es j, k < i, sodass entweder $s_i \in \mathscr{P}$ oder $s_i = \neg s_j$ oder $s_i = (s_j \mathbf{o} s_k)$ mit $\mathbf{o} \in \{\vee,\wedge,\rightarrow\}$.

Ferner (*Ausschluss redundanter Elemente & Baumform*): jedes nicht-letzte Glied s_i (i < n) ist Regel-Vorbedingung für ein und nur ein späteres Glied s_j (j>i). (Ergo: Eine Aussagevariable muss so oft eingeführt werden, wie sie in der Formel auftaucht.

G-Konstruktionen können gut als *Strukturbäume* veranschaulicht werden:

Beispiel:



Lineare Notation (v.l.n.r.): $\langle p,q,p,\neg p,\neg q,(\neg p\rightarrow\neg q), ((\neg p\rightarrow\neg q)\vee p)\rangle$.

Metasprachliche Definition: $(A\leftrightarrow B) := ((A\rightarrow B) \wedge (B\rightarrow A))$.

(Frage: warum benutze ich "=" und nicht "$\leftrightarrow$"?)

(Exklusives Oder: $(A \dot{\vee} B) :\leftrightarrow (A\vee B) \wedge \neg(A\wedge B)$ $(\leftrightarrow\ (A\leftrightarrow\neg B)\ )$:

Logische Konstanten: $\top$ für "Verum", eine Tautologie; $\bot$ für "Falsum", eine Kontradiktion.

Oft als primitiv benutzt; oft definiert: Verum $\top := (p\vee\neg p)$, Falsum $\bot := (p\wedge\neg p)$

Konvention für Klammern:

1. Die äußersten Klammern können weggelassen werden (bezügl. binärer Operatoren).

2. Klammern können nach der folgenden Präferenz der Bindung weggelassen werden:

2a: $\wedge$, $\vee$ binden stärker als $\rightarrow$, $\leftrightarrow$

Beispiele: $p\wedge q \rightarrow r$ in Ordnung, $p\wedge q \vee r$ nicht in Ordnung.

Wichtige Anmerkung: Formregeln müssen *mit äußeren* Klammern aufgestellt werden, weil sie auf *Teilformeln angewandt werden*.

Übung 3.1: Welche der folgenden Zeichenreihen sind wohlgeformt, und welche Klammerkonventionen wurden verwendet? Wenn sie wohlgeformt sind, zeichnen Sie ihren Strukturbaum: $\neg(p\rightarrow q)$, $p\vee q\wedge\neg r$, $(\neg(p\rightarrow q))$, $((p\wedge q)\vee r)$, $p\wedge\neg q \leftrightarrow \neg r\wedge s$, $(1\vee p)\wedge A$, $r_1\rightarrow(\neg(r_2\vee s) \wedge s)$, $(\neg p\vee(q\wedge(\neg s)))\rightarrow r$.

Wichtige metalogische Beweismethode: Induktion über der Komplexität von Formeln:

um zu beweisen, dass eine Eigenschaft P für alle Formeln gilt, beweisen wir, dass:
– P für alle $p\in\mathcal{P}$ gilt
– wenn P für $A\in\mathcal{L}$ gilt, P auch für $\neg A$ gilt
– wenn P für A, B $\in \mathcal{L}$ gilt, es auch für $(A\vee B)$, $(A\wedge B)$, und $(A\rightarrow B)$.

In anderen Worten wenden wir die starke Induktion über die Eigenschaft P*(n) für natürliche Zahlen an: "alle Formeln des Grades der Komplexität n haben die Eigenschaft P“

Anmerkung: Induktion ist 'schwach' für Negation, aber 'stark' für zweistellige Konnektive '**o**' (Wenn P(A) und P(B) für alle A, B mit Kompl(A), Kompl(B) < n, dann P((A**o**B)).

Für das folgende Theorem, lassen wir (fettgedruckt) **s** über Sequenzen von Zeichenreihen laufen.

Wenn $\mathbf{s}_1$ und $\mathbf{s}_2$ Sequenzen sind, dann ist $\mathbf{s}_1\mathbf{s}_2$ ihre Konkatenation.

Z.B., $\mathbf{s}_1 = <1,3,4>$, $\mathbf{s}_2 = <4,3,5,>$, dann $\mathbf{s}_1\mathbf{s}_2 = <1,3,4,4,3,5>$.

Hinweis: das folgende Theorem scheint trivial. Man lernt dabei, wie induktives Beweisen funktioniert.

Theorem (g-Konstruktion):

Für alle $s \in S(\mathcal{L})$: $s \in \mathcal{L}$ (gemäß der rekursiven Def.) $\Leftrightarrow$ s hat eine g-Konstruktion.

Beweis:

(Links-nach-Rechts) $\Rightarrow$: Nehmen wir an $s = A \in \mathcal{L}$. Zu beweisen ist, dass A eine g-Konstruktion hat, mittels Induktion nach der Komplexität der Formel A:

Anfangsschritt: Wenn $A \in \mathcal{P}$, dann ist $<A>$ eine g-Konstruktion von A.

Negation: Wenn $A = \neg B$, dann hat B eine g-Konstruktion $\mathbf{s}(B)$ nach IH. Dann ist $\underline{\mathbf{s}(B)<\neg B>}$ eine g-Konstruktion von $\neg B$.

Binäre Konnektive: Wenn $A = (B\mathbf{o}C)$, für $\mathbf{o} \in \{\vee,\wedge,\rightarrow\}$, dann haben B und C g-Konstruktionen $\mathbf{s}(B)$ und $\mathbf{s}(C)$ nach *IH*. Dann ist $\underline{\mathbf{s}(B)\mathbf{s}(C)<(B\mathbf{o}C)>}$ eine g-Konstruktion von $(B\mathbf{o}C)$.

(Right-to-Left) $\Leftarrow$: Nehmen wir an s hat eine g-Konstruktion **s** – dann ist s **s**'s letztes Glied.

Zu beweisen ist, dass s eine Formel ist durch Induktion über dem Komplexitätsgrad von Zeichenreihe s:

1. *Wenn Grad(s) = 0*: dann kann s in **s** nur durch die Regel 1 eingeführt werden. Also $s \in \mathcal{P}$.

2. *Angenommen Grad(s) = k > 0:* Dann muss s in **s** durch die Regeln 2 oder 3 eingeführt werden. Also hat s die Form $\neg s_1$ oder $(s_1\mathbf{o}s_2)$. Da s_1 und s_2 Grade $< k$ haben,

sind sie nach IH Formeln. Also ist s dementsprechend eine Formel, nach der Regel 2 oder 3. Q.E.D.

****VERLAGERN IN DIE ÜBUNG:****************

nur fettgeschriebene Übungen werden gemacht

Weglassen: *Übung 3.2:* Beweisen Sie durch Induktion auf die Komplexität von Formeln:

Die Anzahl der Knoten im Strukturbaum einer Formel (d.h., die Anzahl der Glieder in der g-Konstruktion der Formel) = die Länge der Formel minus 2· die Anzahl der Klammern darin.

Teilformel:

Nicht-rekursive Definition einer Subformel:

B ist eine Teilformel von A gdw die A Form s_1Bs_2 hat.

Anmerkung 1: s_1, s_2 können leer sein.

Anmerkung 2: B muss *mit* äußeren Klammern geschrieben werden. Z.B., p∨q ist keine Teilformel von ¬p∨q.

Nicht-rekursive Definitionen sind häufig einfacher zu verstehen. Für Beweiszwecke muss man sie in rekursive Definitionen überführen:

Rekursive Definition von "B ist eine Teilformel von A" (Rekursion auf A in Relation zu B).

1. A ist Teilformel von A (eine *unechte* Teilformel).
2. Wenn B Teilformel von A ist, dann ist B auch Teilformel von ¬A.
3. Wenn B Teilformel von A ist, dann ist B auch Teilformel von (A**o**C) und von (C**o**A) (**o**∈{∨,∧,→})

Weglassen: *Übung 3.3*: Beweisen Sie, dass die rekursive- und nicht-rekursive Definition von "B ist Teilformel von A" äquivalent sind, durch Induktion auf die Komplexität über A mit gegebenem B (Start: A = B).

Wir unterscheiden zwischen einem Symbol oder einer Teilformel, die in einer Formel vorkommt, und den *Vorkommnissen* dieses Symbols oder dieser Formel (angezeigt durch die Stellenzahl). Beispiel: $(p\rightarrow(q\vee\neg p)) \rightarrow p$. ($\rightarrow$ kommt 2 mal vor, p kommt 3 mal vor.)

Definition (Bereich, äußerstes Operatorvorkommnis)*:*

1. *Der Bereich* eines Operator-Vorkommnisses in einer Formel A ist das kleinste Teilformel-Vorkommnis, das dieses Operator-Vorkommnis enthält.
2. Das *äußerste* Operator-Vorkommnis eines Teilformel-Vorkommnisses X in A ist das Operatorvorkommnis in A, welches X als seinen Bereich hat.

Theorem (eindeutige Lesbarkeit):

Für jedes $A\in\mathcal{L}$: jedes Operator-Vorkommnis **o** in A korrespondiert bijekiv mit einem nicht-atomaren Teilformel-Vorkommnis in A, welches der Bereich von **o** ist.

Bild: $\neg\,((\,p \wedge \neg q\,) \vee r\,) \rightarrow s$

⇒ ***Beweisen**: **Übung 3.4:*** Beweisen Sie das Theorem der eindeutigen Lesbarkeit durch Induktion über die Komplexität von Formeln.

Zur Erinnerung: Die Methode der Wahrheitstafeln beruht auf dem Theorem der eindeutigen Lesbarkeit:

Z.B.	p q r s	$\neg((p \wedge \neg q) \vee r) \rightarrow s$
	0 1 1 0	0 0 0 0 1 1 1 1 0

Übung 3.4a: Die 'polnische Notation' ist eine klammerfreie Notation für Formeln. Der Operator wird vor die (ein oder zwei) Formel(n) geschrieben, die sein(e) Argument(e) ist/sind. Schreiben Sie die folgenden polnisch notierten Formeln in Klammer-Notation um (Achtung: am besten von rechts nach links lesen):
$\neg\rightarrow pq$, $\wedge p\neg q$, $\neg\rightarrow\vee\neg pq\wedge\neg rs$, $\rightarrow\vee\neg p\wedge q\neg sr$.

******ENDE VERLAGERN IN ÜBUNG***********

3.2 Semantik der Aussagenlogik

Definition (Bewertung für Aussagenlogik):

1. Eine *Bewertungfunktion* (Interpretation, Wahrheitsbewertung) von $\mathcal{L}$ ist eine Funktion v:$\mathcal{P}\rightarrow\{0,1\}$
   (1 für wahr, 0 für falsch).
2. Die Bewertung wird rekursiv auf nicht-atomare Formeln wie folgt ausgedehnt:

(v¬)	$v(\neg A) = 1$	wenn $v(A) = 0$,	sonst $v(\neg A) = 0$.
(v∧)	$v(A\wedge B) = 1$	wenn $v(A) = 1$ und $v(B) = 1$,	sonst $v(A\wedge B) = 0$.
(v∨)	$v(A\vee B) = 1$	wenn $v(A) = 1$ oder $v(B) = 1$,	sonst $v(A\vee B) = 0$.
v(→)	$v(A\rightarrow B) = 1$	wenn $v(A) = 1 \Rightarrow v(B) = 1$ (also wenn $v(A)=0$ oder $v(B) = 1$)	– sonst $v(A\rightarrow B) = 0$.

3. Wir schreiben auch v |== A statt v(A)=1 und sagen, v *erfüllt* oder *verifiziert* A, oder, *v ist ein Model für* A.

Wenn v(A) = 0, d.h. v |=/= A, sagen wir, dass v A falsifiziert, oder nicht erfüllt, oder, v ein Gegenbeispiel für A ist.

4. v |== Γ (v erfüllt Γ) gdw v |== A für alle $A\in\Gamma$.

Philosophische Bemerkung: Die Sätze in 2 werden normalerweise als Wahrheitstafeln geschrieben. Die gegebene Formulierung zeigt, dass die Beschreibung dieser Wahrheitsfunktionen der aussagenlogischen Operatoren in der Metasprache bereits diese Operatoren und ihre logische Bedeutung in der Metalogik *präsupponiert. Dies ist ein Beispiel für den Zirkel der Metalogik.*

Da der Konjunktions-Operator der Metasprache dieselbe Bedeutung wie der der Objektsprache haben soll, sagen wir grundsätzlich:

<u>"A und B" ist wahr gdw "A ist wahr" und "B ist wahr".</u>

Dies zeigt uns wie "wahr" über "und" distribuiert.

Wahr(Und(A,B)) ↔ Und(Wahr(A),Wahr(B)).

Aber es kann nicht die Bedeutung von "und" aus dem Nichts definieren.

Mein Ansatz für nichtzirkuläre Rechtfertigung von Logik-Systemen: Optimalitäts-Rechtfertigung – durch universelle Übersetzbarkeit nichtklassischer in die klassische Logik. Verallgemeinert: anderer Logiken in die eigene Logik. (Gehört in eine andere LV).

Für $A \in \mathcal{L}$, definieren wir: $\mathcal{P}(A)$ = die Menge der Aussagevariablen, die (irgendwo) in A vorkommen. Z.B., $\mathcal{P}(\neg(p \rightarrow (q \vee p))) = \{p, q\}$.

Auch das folgende Theorem scheint trivial – ist aber streng genommen zu beweisen.
Theorem (Wahrheitsfunktionalität für Formeln, Extensionalität):
v_1, v_2 seien zwei $\mathcal{L}$-Bewertungen (man erinnere sich an die "Restriktion" $f \upharpoonright D$ von $f{:}A \rightarrow B$ auf $D \subseteq A$")
Wenn $v_1 \upharpoonright \mathcal{P}(A) = v_2 \upharpoonright \mathcal{P}(A)$, dann $v_1(A) = v_2(A)$.

Induktiver Beweis: 1. $A = p \in \mathcal{P}$: nach Voraussetzung.
2. $A = \neg B$: wegen $v_1 \upharpoonright \mathcal{P}(\neg B) = v_2 \upharpoonright \mathcal{P}(\neg B)$ gilt auch $v_1 \upharpoonright \mathcal{P}(B) = v_2 \upharpoonright \mathcal{P}(B)$
nach IH, $v_1(B) = v_2(B)$. Also $v_1(\neg B) = v_2(\neg B)$, weil $\neg$ wahrheitsfunktional ist.
3. $A = (B \vee C)$. wegen $v_1 \upharpoonright \mathcal{P}((B \vee C)) = v_2 \upharpoonright \mathcal{P}((B \vee C))$ gilt auch $v_1 \upharpoonright \mathcal{P}(B) = v_2 \upharpoonright \mathcal{P}(B)$ und $v_1 \upharpoonright \mathcal{P}(C) = v_2 \upharpoonright \mathcal{P}(C.)$
Daher nach IH, $v_1(B) = v_2(B)$ und $v_1(C) = v_2(C)$.
Also $v_1(B \vee C) = v_2(B \vee C)$, weil $\vee$ wahrheitsfunktional ist (genauso für $\wedge$, $\rightarrow$).

Anmerkung: $v \upharpoonright \mathcal{P}(A)$ korrespondiert genau mit einer Wahrheitswertzeile für A.
Definition (logisch determinierte, semantische Eigenschaften):

1. A ist logisch wahr, oder gültig, oder eine Tautologie, kurz $\Vdash A$, gdw A von allen $v{:}\mathcal{P} \rightarrow \{0,1\}$ erfüllt wird.
   A ist erfüllbar gdw A von irgendeinem $v{:}\mathcal{P} \rightarrow \{0,1\}$ erfüllt wird.
   Γ ist erfüllbar gdw irgendein $v{:}\mathcal{P} \rightarrow \{0,1\}$ jedes $A \in \Gamma$ erfüllt.
   A ist logisch falsch gdw kein $v{:}\mathcal{P} \rightarrow \{0,1\}$ A erfüllt.
2. A folgt logisch aus Γ, oder der Schluss Γ / A ist gültig, kurz $\Gamma \Vdash A$, gdw

für alle v:$\mathscr{P}\rightarrow\{0,1\}$, wenn v Γ erfüllt, dann erfüllt v A.

Anmerkungen: ||— A (gemäß 1.) gdw ∅ ||— A (gemäß 2.).

A ist erfüllbar gdw ||-/- ¬A.

Konvention: Wir schreiben:

Γ, A ||— B für Γ ∪ {A} ||— B Γ, Δ ||— B für Γ∪Δ ||— B

Man unterscheidet zwischen Logik, als Menge aller L-wahren Formeln verstanden, und ihrer korrespondierenden Folgerungsrelation!

L steht für Aussagenlogik: = {A: ||— A}.

||— steht für Folgerungsrelation.

Aussagenlogik ist *semantisch entscheidbar*

– durch Wahrheitstafeln

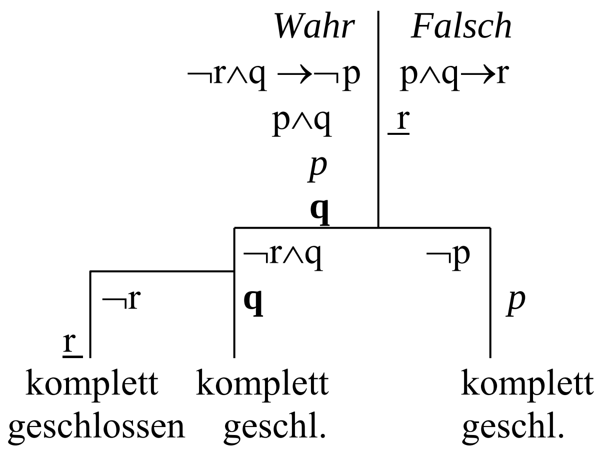
– durch reductio ad absurdum via Wahrheitswertzeilen (Logik I: noch kürzer).

– durch semantische reductio ad absurdum via *Beth-Tableaus* (etwas umständlicher)

*****WIRD WEGGELASSEN*****

Beispiel eines Beth-Tableau: (Berechnung nur durch Dekomposition)

(¬r∧q→¬p) ||— (p∧q→r)



Reductio ad absurdum mit Wahrheitswertzeilen:

$\underline{(\neg r \wedge q \;\rightarrow\; \neg\, p) \Vdash \;\; (p \wedge q \;\rightarrow\; r)}$ (Hier *übertragen* wir W-Werte; das tun
wf w w w w $\underline{\text{f}}$ $\underline{\text{w}}$w w f f wir in Beth-Tableaus nicht)

Wahrheitstafel: hat 8 Zeilen.

Übung 3.5:
Finden Sie den Wahrheitsstatus (L-wahr, kontingent, L-falsch) oder Gültigkeitsstatus (gültig, ungültig) mit Beth-Tableaus heraus:
1) $(\neg p \wedge q) \rightarrow r) \rightarrow s \Vdash s \rightarrow (r \rightarrow (p \vee q))$,
2) $A \rightarrow B, C \rightarrow D \Vdash (A \wedge C) \rightarrow (B \wedge D)$,
3) $(p \wedge q) \rightarrow r, \neg q \rightarrow \neg r \Vdash p \rightarrow r$,
4) $A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$,
5) $((A \rightarrow B) \wedge (C \rightarrow D)) \rightarrow ((A \wedge C) \rightarrow (B \wedge D))$,
6) $(p \vee q) \rightarrow (r \vee s), p \leftrightarrow \neg(r \wedge t), s \leftrightarrow t \Vdash p \rightarrow t$,
7) $((A \rightarrow B) \wedge (C \rightarrow B)) \rightarrow ((A \vee C) \rightarrow B)$
8) $((A \rightarrow C) \wedge (A \rightarrow B)) \rightarrow (A \rightarrow (C \wedge B))$.

*****ENDE WEGLASSEN*****

Substitution:

Logische Wahrheit bzw. Gültigkeit ist eine Eigenschaft von Satz- bzw. Schluss*schemata* $\Leftrightarrow$

Gültigkeit ist geschlossen, bzw. wir erhalten, unter der Operation der Substitution

Definition von Substitution:

1. Eine Substitutionsfunktion s ist eine Funktion s: $\mathcal{P} \to \mathcal{L}$.

Z.B.: $s(p_1) = (p_1 \to p_2)$, $s(p_2) = \neg(p_7 \vee p_5)$, etc.

2.1 *Nicht-rekursive Definition:* Das *Resultat der Anwendung von s auf A, s(A), ist* diejenige Formel, die aus A durch *simultane* Ersetzung aller Vorkommnisse irgendeines $p \in \mathcal{P}$ in A durch s(p) resultiert.

Z.B., $s(p_1 \wedge \neg p_2) = ((p_1 \to p_2) \wedge \neg\neg(p_7 \vee p_5))$, etc.

2.2 *Rekursive Definition*:

a) Für $p \in \mathcal{P}$ ist s(p) direkt durch 1 gegeben.

b) $s(\neg A) = \neg\, s(A)$.

c) $s(A \vee B) = s(A) \vee s(B)$, $s(A \wedge B) = s(A) \wedge s(B)$, $s(A \to B) = s(A) \to s(B)$.

3. Für Mengen von Formeln: $s(\Gamma) = \{s(A): A \in \Gamma\}$

Theorem (Substitution):

1. **L** ist geschlossen unter Substitution, d.h.: $\Vdash A \;\Rightarrow\; \Vdash s(A)$.
2. $\Vdash$ ist *strukturell*, d.h. : $\Gamma \Vdash A \;\Rightarrow\; s(\Gamma) \Vdash s(A)$.

Beweis. Wir entwickeln zuerst das:

Koinzidenz Lemma: Für gegebenes s und v, definiere: $v_S: \mathcal{P} \to \{0,1\}$, sodass $v_S(p) = v(s(p))$.

Dann gilt für alle $A \in \mathcal{L}$: $v_S(A) = v(s(A))$.

Erläuterung am Beispiel:

Annahme: $s(p) = (p \wedge \neg q)$, $s(q) = (\neg p \vee q)$.

Annahme: $\underline{A = p \wedge \neg q}$ Also: $s(A) = (p \wedge \neg q) \wedge \neg(\neg p \vee q)$

Ang. $\underline{v(p) = 1, v(q) = 0.}$ Dann: $v_s(p) = v(p \wedge \neg q) = 1$, und $v_s(q) = v(\neg p \vee q) = 0$.

$v_s(A) = 1 \wedge \neg 0 = 1$. $v(s(A)) = v((p \wedge \neg q) \wedge \neg(\neg p \vee q)) = 1 \wedge \neg 0 = 1$.

Beweis Lemma: 1. A = p atomar: $v_S(p) = v(s(p))$ per Definition.

2. $A = \neg B$: $v_S(\neg B) = 1$ gdw $v_S(B) = 0$ [per rek. Def. von v]

gdw $v(s(B)) = 0$ [per IH]

gdw $v(\neg s(B)) = 1$ [per rek. Def. von v]

gdw $v(s(\neg B)) = 1$ [per rek. Def. von s: $s(\neg B) = \neg s(B)$] .

3. $A = (B\vee C)$: $v_S(B\vee C) = 1$ gdw $v_S(B) = 1$ oder $v_S(C) = 1$ [per rek. Def. v]

gdw $v(s(B)) = 1$ oder $v(s(C)) = 1$

[per IH: $v_S(B) = v(s(B))$, $v_S(C) = v(s(C))$; und AL]

gdw $v(s(B)\vee s(C)) = 1$ [per rek. Def. v]

gdw $v(s(B\vee C)) = 1$ [per Def. s: $s(B\vee C) = s(B) \vee s(C)$].

4. $A = (B\wedge C)$, $(B\rightarrow C)$ gleichermaßen. Q.E.D. Lemma

Beweis des Theorems der Substitution: (Durch Kontraposition)

Für 1.: Annahme des Gegenteils: Angenommen ||-/- s(A). Dann existiert v, sodass $v(s(A))=0$. Aber dann, nach Koinzidenz Lemma, $v_S(A)=0$, was impliziert ||-/- A.

– *Für 2.:* **siehe Übung.** Q.E.D.

Anmerkung: Substitutionsfunktionen sind 'homomorph': man darf niemals dieselbe Aussagevariable durch verschiedene Sätze ersetzen, aber man darf verschiedene Aussagevariablen durch dieselben Sätze ersetzen. Z.B. $A\rightarrow A$ ist eine substitutions-Instanz von $p\rightarrow q$; aber $A\rightarrow B$ ist keine subst.-Inst. von $p\rightarrow p$.

Eine Substitutionsfunktion wird *Umbenennung* (alphabetische Umbenennung) genannt gdw sie injektiv ist und $ran(s) \subseteq \mathcal{P}$. (Sie muss nicht bijektiv sein, wenn $\mathcal{P}$ infinit ist).

Übungen:

3.6 Beweisen Sie Teil 2 des Theorems der Substitution mithilfe des Koinzidenzlemmas: $\Gamma \Vdash A \;\Rightarrow\; s(\Gamma) \Vdash s(A)$.

3.7 Konstruieren Sie ein Gegenbeispiel für: $\Vdash s(A) \;\Rightarrow\; \Vdash A$.

3.8 Konstruieren Sie ein Gegenbeispiel für: A ist erfüllbar $\Rightarrow$ s(A) ist erfüllbar.

Also bleibt Erfüllbarkeit nicht unter Substitution erhalten (letztlich, weil Substitutionen homomorph sind).

3.9 Beweisen Sie: Wenn s(A) erfüllbar ist, dann ist A erfüllbar.

3.10 Beweisen Sie: Wenn s eine Umbenennung ist, dann: $\Vdash A$ gdw $\Vdash s(A)$.

A ist erfüllbar gdw s(A) erfüllbar ist. *Hinweis:* Machen Sie Gebrauch von s^{-1}.

***********Wird nur kurz angesprochen**********

Eine Liste von wichtigen, gültigen Formeln (Axiome oder Theoreme der Objektsprache) und Schlüssen (Regeln 1. Stufe) und Regeln über Schlüsse (Regeln 2. Stufe)

- *Standardschlüsse - Basisregeln 1. Stufe wie Im Kalkül S aus Logik I:*

(MP) $A \to B, A \Vdash B$ — Modus Ponens

(MT) $A \to B, \neg B \Vdash \neg A$ — Modus Tollens

(DS) $A \lor B, \neg A \Vdash B$ | $A \lor B, \neg B \Vdash A$ — Disjunktiver Syllogismus

(ADD) $A \Vdash A \lor B$ | $A \Vdash B \lor A$ — Addition

(SIMP) $A \land B \Vdash A$ | $A \land B \Vdash B$ — Simplifikation

(CON) $A, B \Vdash A \land B$ — Konjunktion

(DN) $A \Vdash \neg\neg A$ | $\neg\neg A \Vdash A$ — Doppelte Negation

- *Abgeleitete Regeln 1. Stufe deduktiver Kalküle :*

(Res) $A \lor B, \neg B \lor C \Vdash A \lor C$ — Resolution

$A \to B, B \to C \Vdash A \to C$ — hypothetischer Syllogismus, $\to$-Verkettung

$A \to C, B \to C \Vdash (A \lor B) \to C$ — $\lor$-Einführung im Antezedens

$A \to B, A \to C \Vdash A \to (B \land C)$ — $\land$-Einführung Im Konsequenz

$A \to (B \to C) \Vdash (A \land B) \to C$ — Importation

$(A \land B) \to C \Vdash A \to (B \to C))$ — Exportation

- (Schlüsse, die Irrelevanzen enthalten:)

$\neg A \Vdash A \to B$	Ex falso quodlibet, materiale Version
$B \Vdash A \to B$	Verum ex quodlibet, materiale Version
$A \wedge \neg A \Vdash B$	Ex falso quodlibet, logische Version
$A \Vdash B \vee \neg B$	Verum ex quodlibet, logische Version

- *Objektsprachliche Theoreme:*

  Theoreme, die zu den obigen Schüssen korrespondieren (durch Ersetzung von "$\Vdash$" durch "$\to$" und Verbindung der Prämissen per Konjunktion) tragen den selben Namen.

– *Des weiteren:*

$A \vee \neg A$	Tertium non datur (ausgeschlossenes Drittes)
$\neg(A \wedge \neg A)$	Nonkontradiktion
$((A \to B) \to A) \to A$	Peirce' Gesetz

- *Äquivalenztheoreme, z.B.* DeMorgan $\neg(A\wedge B)\leftrightarrow(\neg A\vee\neg B)$, etc.$\to$ *siehe später.*

- *Standardregeln über Schlüsse – Regeln 2. Stufe in Kalkülen des natürlichen Schließens:*

Monotonie:

(Mon) $\Gamma \Vdash A \quad \Rightarrow \quad \Delta \cup \Gamma \Vdash A$ (für beliebige Δ)

Schnittregel ist die Grundlage des Prinzips des deduktiven Schließens als Regelverkettung:

(Cut) $\Gamma \Vdash A$ und $A, \Delta \Vdash B \quad \Rightarrow \quad \Gamma \cup \Delta \Vdash B$

Z.B.: $p, p\to\neg q \Vdash \neg q$ und $\neg q, q\vee r \Vdash r \quad \Rightarrow \quad p, p\to\neg q, q\vee r \Vdash r$.

$$\begin{array}{l} p \\ \underline{p \to \neg q} \\ \neg q \end{array} \qquad . \qquad \begin{array}{l} \neg q \\ \underline{q \lor r} \\ r \end{array} \qquad \begin{array}{l} p \\ p \to \neg q \\ \underline{q \lor r} \\ r \end{array}$$

Die Iteration der *“Cut”*-Regel ermöglicht es, jede Schlussregel 1. Stufe in einen Schluss 2. Stufe *mit der selben Prämissenmenge* umzuformen. $\to$ *Die Regeln 2. Stufe sind genereller, als ihre Gegenstücke 1. Stufe* (implizieren deduktiv, dass diese Regel "zwischendrin im Beweis" jederzeit anwendbar ist).

ADD 2. Stufe: $\Gamma \Vdash A \;\Rightarrow\; \Gamma \Vdash A \lor B$.

Beweis. $\dfrac{\Gamma \Vdash A \;\mid\; A \Vdash A \lor B \text{ (=Add 1. Stufe)}}{\Gamma \Vdash A \lor B}$ Cut

MP 2. Stufe: $\Gamma \Vdash A$ und $\Delta \Vdash A \to B \;\Rightarrow\; \Gamma, \Delta \Vdash B$

Beweis: $\begin{array}{l} \underline{\Gamma \Vdash A, \quad A, A \to B \Vdash B} \\ \underline{\Gamma, A \to B \Vdash B, \quad \Delta \Vdash A \to B} \\ \Gamma, \Delta \Vdash B \end{array}$

Konditionalbeweis:

(KB): $\Gamma, A \Vdash B \;\Rightarrow\; \Gamma \Vdash A \to B$.

($\Leftarrow$ ist auch gültig: generalisierter Modus Ponens).

Damit verbunden:

Deduktionstheorem: $\Gamma, A \Vdash B \;\Leftrightarrow\; \Gamma \Vdash A \to B$

$\bigwedge$*-Deduktionstheorem:* Für finite Γ : $\Gamma \Vdash A \;\Leftrightarrow\; \Vdash \bigwedge\Gamma \to A$

Fallunterscheidung – allgemein und speziell:

(aFU): $\Gamma, A \Vdash C$ und $\Delta, B \Vdash C \;\Rightarrow\; \Gamma, \Delta, A \lor B \Vdash C$

(sFU): $\Gamma, A \Vdash C$ und $\Delta, \neg A \Vdash C \;\Rightarrow\; \Gamma, \Delta \Vdash C$

Indirekter Beweis, reductio ad absurdum:

(kIB) $\neg A, P_1, \ldots, P_n \Vdash\!\!— B \wedge \neg B \quad \Rightarrow \quad P_1, \ldots, P_n \Vdash\!\!— A$ (nur klassisch)

(iIB) $A, P_1, \ldots, P_n \Vdash\!\!— B \wedge \neg B \quad \Rightarrow \quad P_1, \ldots, P_n \Vdash\!\!— \neg A$ (auch intuitionistisch)

Übungen: machen

Übung 3.11: *Geben Sie semantische Beweise für folgende Regeln 2. Stufe an :* KB, kIB (evtl. auch aFU). Einmal informell, dann formell – um zu zeigen, wie die metalogische Beweise selbst Objektlogik voraussetzen.

************Ende nur Kurz Ansprechen**********

3.3 Deduktive Kalküle für die Aussagenlogik

! Es gibt verschiedene mögliche Axiomatisierungen der Logik, definiert durch eine Semantik !

Zwei Arten deduktiver Kalküle

- Axiome & Regeln 1. Stufe - Kalküle (Hilbert)
- Kalküle natürlichen Schließens
  Regeln 1. & 2. Stufe - Kalküle

Zwei Wege der Repräsentation von Kalkülen natürlichen Schließens:

Sequezenrepresentation – meta-logisch	*Satzrepresentation – natürlich*
Gentzen style	*Fitch-Style* (oder *Copi-Style*) (Logik I)
Einheiten des Beweises sind Schlüsse = **Sequenzen.**	Einheiten des Beweises sind **Sätze**.
Sie sind Teil der Objektsprache:	
Die *Schittregel* wird explizit angewendet oder implizit in Sequenzen 2. Stufe	Die *Schnittregel* wird **implizit** in der Beweisverkettung verwendet.
	Basisregeln: Regeln 1. Stufe Γ / A, und korrespondierende Regeln 2. Stufe
Sequenzaxiome = Regeln 1. Stufe der Form $\Gamma \vdash$ A.	mit der selben Prämissenmenge (implizit in Verkettung) Γ / A $\Rightarrow$ Γ / B
Sequenzregeln: Regeln 2. Stufe der Form: $\Gamma \vdash$ A, … / $\Delta \vdash$ B.	*Annahmebeweisregeln:* Regeln 2. Stufe mit unterschiedlicher Prämissenmenge

Der Kalkül S* (Approximation Logik I)

Alle Formelmengen in **Beweisen** werden als finit angenommen (Beweise sind konkrete Entitäten.)

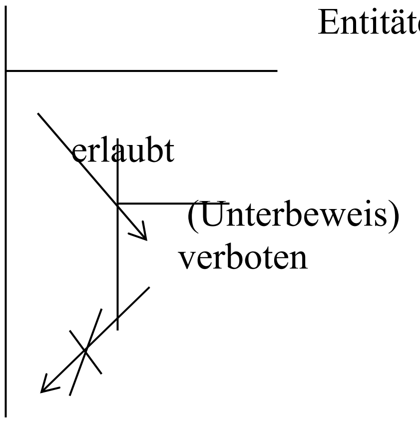
P1

P2

C

Trennlinie zwischen Präm und Abgeleitetem

Bereichsindikator (Bereich der Prämissen)



Neben Fitch-Style gibt es (z.B.):
Copi-Style ; Quine-Stern-Style; Anderson-Belnap explizite Abhängikeitsaufzeichnung

Sequenzenpräsentation: leichte Überführung in Satzpräsentation
Schnittregel implizit

Sequenzen-Präsentation: ***Satz-Präsentation:***

A

A

A

A

Sequenz-Axiome*:** ***Basisregeln:
Reiteration
REIT: $A \vdash A$

Sequenzregeln:
Modus Ponens, →-Beseitigung:
MP: $\Gamma \vdash A$ und $\Delta \vdash A \rightarrow B$ / $\Gamma, \Delta \vdash B$
Anmerkung: Da als Regeln 2. Stufe formuliert, kann die Trennlinie irgendwo über A, A→B liegen

A
$A \rightarrow B$
B

Simplifikation , ∧-Beseitigung:
SIMP: $\Gamma \vdash A \wedge B$ / $\Gamma \vdash A$ | $\Gamma \vdash A \wedge B$ / $\Gamma \vdash B$

$A \wedge B$
A

$A \wedge B$
B

Konjunktion, ∧-Einführung:
KON: $\Gamma \vdash A$ and $\Delta \vdash B$ / $\Gamma, \Delta \vdash A \wedge B$

A
B
$A \wedge B$

Addition, ∨-Einführung:
ADD: $\Gamma \vdash A$ / $\Gamma \vdash A \vee B$, $\Gamma \vdash A$ / $\Gamma \vdash B \vee A$

A
$A \vee B$

A
$B \vee A$

Disjunktiver Syllogismus – ∨-Beseitigung:
DS: $\Gamma \vdash A \vee B$ und $\Delta \vdash \neg A$ / $\Gamma, \Delta \vdash B$
$\Gamma \vdash A \vee B$ und $\Delta \vdash \neg B$ / $\Gamma, \Delta \vdash A$

$A \vee B$
$\neg A$
B

$A \vee B$
$\neg B$
A

Klassische Doppelte Negation – ¬-Beseitigung:
kDN (DN): $\Gamma \vdash \neg\neg A$ / $\Gamma \vdash A$

A
$\neg\neg A$

Annahmebeweisregeln:
Konditionalbeweis - → -Einführung:
KB: $\Gamma, A \vdash B$ / $\Gamma \vdash A \rightarrow B$

A
B
$A \rightarrow B$

intuitionistischer indirekter Beweis - ¬-Einf.:
iIB: $\Gamma, A \vdash B \wedge \neg B$ / $\Gamma \vdash \neg A$

A
$B \wedge \neg B$
$\neg A$

Definition Beweisbarkeit in **S***:

Sequenzen-Präsentation: $\Gamma \vdash A$ ist beweisbar in **S***, kurz $\Gamma \vdash_{S^*} A$, gdw ein Beweis für $\Gamma \vdash A$ *existiert*, d.h. eine endliche Folge von Sequenzen $<\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n>$ sodass die Schlusssequenz die zu beweisende Sequenz ist ($\Gamma_n = \Gamma$, $A_n = A$), und jede Sequenz $\Gamma_i \vdash A_i$ entweder ein Axiom ist, oder aus ein oder zwei voriger Sequenzen nach einer der Regeln folgt.

Satz-Präsentation: $\Gamma \vdash A$ ist beweisbar in **S*** gdw eine endliche Sequenz $<A_1, \ldots, A_n>$ existiert, zusammen mit einer Indikation von Prämissen-/Annahmebereichen, sodass $A_n = A$ und jedes A_i entweder ein Element von Γ oder eine Annahme eines geschlossenen Unterbeweises ist (d.h. ein Unterbeweis, dessen Bereich *vor* dem Ende des gesamten Beweises endet) oder aus früheren Elementen nach einer der Basisregeln folgt oder aus einem geschlossenen Unterbeweis nach einer der Annahmebeweisregeln.

Im System S* sind folgende Desiderata erfüllt:

1) Für jeden AL-Operator gibt es genau eine Einführungs- und eine Ausführungsregel. *Daher:* $\Rightarrow$ Alle Regeln sind voneiander unabhängig (keine Redundanz).

2) Durch Weglassung der Regel cDN entsteht genau der intuitionistische Kalkül.

3) Im System S* lernt man die Parallelität von Sequenzenkalkül und Satzkalkül auf einfachste Weise (weil Regeln 2. Stufe benutzt werden). Siehe unten.

4) System S* ist optimale Approximation an System S von Logik I (welches weder 1 noch 2 erfüllt, aber praktisch und bequem ist), weil folgende Regeln daraus herleitbar sind, die wir im folgenden als *abgeleitete Regeln von S** jederzeit ebenfalls verwenden werden:

Modus Tollens:

MT: $\Gamma \vdash \neg B, \Delta \vdash A \rightarrow B \;/\; \Gamma,\Delta \vdash \neg A$

$A \rightarrow B$
$\neg B$
$\neg A$

intuitionistische DN:

(iDN): $\Gamma \vdash A \;/\; \Gamma \vdash \neg\neg A$

A
$\neg\neg A$

klassischer indirekter Beweis:

kIB (Logik I: IB): $\Gamma, \neg A \vdash B \wedge \neg B \;/\; \Gamma \vdash A$

$\neg A$
$B \wedge \neg B$
A

spezielle Fallunterscheidung:

sFU (Logik I: FU): $\Gamma, A \vdash B$ und $\Delta, \neg A \vdash B \;/\; \Gamma, \Delta \vdash B$

A
B
$\neg A$
B
B

Weitere Notationen:

$\vdash A$, oder A ist ein Theorem von **S***, gdw $\emptyset \vdash_{S*} A$.

Wir dehnen das Konzept $\vdash_{S*}$ wie folgt auf unendliche Prämissenmengen aus:

$\Gamma \vdash_{S*} A$ gdw $\Gamma_f \vdash_{S*} A$ für irgendein endliches $\Gamma_f \subseteq \Gamma$.

$Cn(\Gamma) = \{A: \Gamma \vdash A\}$ = die (deduktive) Konsequenzmenge von Γ

$Cn(A) := Cn(\{A\})$. $Cn(A)$ wird auch der *logische Gehalt* von A genannt.

$Cn(\emptyset) =$ **S***.

Ab jetzt schreiben wir $\Gamma \vdash A$ als Abkürzung für $\Gamma \vdash_{S*} A$, wenn der Kontext klar ist.

⇒ *Bemerkung:* Um *kurze* und *intuitiv transparente* Beweise zu gewährleisten, sind Satz-Kalküle des natürlichen Schließens (Fitch-Kalküle) zu bevorzugen, für metalogische Einfachheit sind Sequenzen-kalküle (Gentzen-Kalküle) oder axiomatische Satzkalküle mit möglichst wenig Regeln (Hilbert-Style-Kalküle, s.u.) vorzuziehen.

Zunächst einige Beweisbeispiele für Regeln 1. Grades; Überführung Satzpräsentation in Sequenzenpräsentation:

Beweis von: $(A \to (B \to C)) \vdash (A \wedge B \to C)$

Satzpräsentation:

1)	$A \to (B \to C)$	Präm
2)	$\vert\ \underline{A \wedge B}$	KB-Ann
3)	$\vert\ A$	Simp 2
4)	$\vert\ B \to C$	MP 1,3
5)	$\vert\ B$	Simp 2
6)	$\vert\ C$	MP 4,5
7)	$A \wedge B \to C$	KB 2-6

Sequenzenpräsentation: man nehme zunächst Reit-Sequenten der Form $A \vdash A$ an:

1)	$A \to (B \to C) \vdash A \to (B \to C)$	Reit
2)	$A \wedge B \vdash A \wedge B$	Reit
3)	$A \wedge B \vdash A$	Simp 2
4)	$A \to (B \to C), A \wedge B \vdash B \to C$	MP 1, 3
5)	$A \wedge B \vdash B$	Simp 2
6)	$A \to (B \to C), A \wedge B \vdash C$	MP 5, 4
7)	$A \to (B \to C) \vdash A \wedge B \to C$	KB 6

Übung 3.12: Beweise: $\neg(A \wedge \neg B) \vdash (A \rightarrow B)$ in Satz- und Sequenzenpräsentation

Beweise: $A \rightarrow C, B \rightarrow C \vdash (A \vee B) \rightarrow C$

1)	$A \rightarrow C$	Präm
2)	$B \rightarrow C$	Präm
3)	$\mid A \vee B$	KB-An
4)	$\mid \quad \mid A$	sFU-An
5)	$\mid \quad \mid C$	MP 1,4
6)	$\mid \quad \mid \neg A$	sFU-An
7)	$\mid \quad \mid B$	DS 3,6
8)	$\mid \quad \mid C$	MP 2,7
9)	$\mid C$	sFU 4-5, 6-8
10	$(A \vee B) \rightarrow C$	KB 3-9

Die Sequenzendarstellung von Annahmebeweisen, welche zwei Annahmen bzw. Subbeweise benötigen, erfordert die Einführung zweier entsprechender Reit-Sequenzen:

1)	$A \vdash A$	Reit
2)	$A \rightarrow C \vdash A \rightarrow C$	Reit
3)	$A \rightarrow C, A \vdash C$	MP 1,2
4)	$\neg A \vdash \neg A$	Reit
5)	$A \vee B \vdash A \vee B$	Reit
6)	$\neg A, A \vee B \vdash B$	DS 4,5
7)	$B \rightarrow C \vdash B \rightarrow C$	Reit
8)	$B \rightarrow C, \neg A, A \vee B \vdash C$	MP 6,7
9)	$A \rightarrow C, B \rightarrow C, A \vee B \vdash C$	sFU 3,8
10)	$A \rightarrow C, B \rightarrow C \vdash (A \vee B) \rightarrow C$	KB 9

Übungsaufgabe 3.13: Herleitung der weiteren Regeln des Systems S aus S*:

iDN: $\Gamma \vdash A \;/\; \Gamma \vdash \neg\neg A$

Modus Tollens:

MT : $\Gamma \vdash A\rightarrow B,\; \Delta \vdash \neg B \,/\, \Gamma, \Delta \vdash \neg A$

Nun zeigen wir, wie kIB aus iIB und kDN folgt:

kIB: $\Gamma, \neg B \vdash A\wedge\neg A \;/\; \Gamma \vdash B$

Übungsaufgabe 3.14: Etwas schwerer ist es, aFU durch DS zu beweisen.

Zeige: $\Gamma, A \vdash C \mid \Delta, B \vdash C \;/\; \Gamma, \Delta, A\vee B \vdash C$

aFU wird per Annahmentechnik *implementiert:*

$A\vee B$

  A

  …

  C

  B

  …

  C

C

Übungsaufgabe 3.15: Um zu zeigen, wie umgekehrt sFU durch IB (kIB) und aFU folgt, müssen wir aber zuerst

TND (Tertium non Datur) $\vdash A\vee\neg A$ (durch kIB) herleiten.

NUR KURZ ANSPRECHEN

Weitere äquivalente Formulierungen unseres Kalküls S*:

⇒ Die Formulierung mittels Regeln 2ter Stufe (2nd degree rules) in der Sequenzenpräsentation ermöglichte leichte Überführung von Satzpräsentation in Sequenzenpräsentation!
CUT (Schnitt) und MON (monotonie) ergeben sich in dieser Version des Sequenzenkalküls als abgeleitete Regeln:
CUT: $\Gamma \vdash A, \quad \Delta, A \vdash B \ / \ \Gamma, \Delta \vdash B$ (ein "generalisierter" MP)

1. $\Gamma \vdash A$	Präm	
2. $\Delta, A \vdash B$	Präm	*keine Notwendigkeit, Cut abzuleiten in*
3. $\Delta \vdash A\rightarrow B$	KB 2	*der Satz-Präsentation; sie ist implizit*
4. $\Gamma,\Delta \vdash B$	MP 1,3	*darin enthalten (Beweisverkettung).*

MON: $\Gamma \vdash A \ / \ \Delta, \Gamma \vdash A$ – mit Hilfe von Cut

1. $\Gamma \vdash A$ Präm *implizit In der Satz-Präsentation enthalten*
2. $\Delta \vdash \bigwedge\Delta$ weil Δ endlich ist, leitet man dies aus endlich vielen Anwendungen von KON her; $\bigwedge\Delta$ = Konjunktion aller Elemente von Δ
3. $\Gamma, \Delta \vdash A\wedge\bigwedge\Delta$ KON 1,2
4. $\Gamma, \Delta \vdash A$ Simp 3

Regeln 1. Stufe ergeben sich in unserer Version des Sqeuenzenkalküls durch Reit-Instanzen: z.b. *Beweis für Kon 1. Stufe:*

1. $A, B \vdash A$	Reit
2. $A, B \vdash B$	Reit
3. $A, B \vdash A\wedge B$	Kon 1,2 (= Kon 1. Stufe)
	Instantiiere: $\Gamma = \Delta = \{A,B\}$

Erste äquivalente Formulierung: Wenn wir die Basisregeln von **S*** als Regeln 1. Stufe festlegen, und Reit 1. Stufe A $\vdash$ A, dann müssen wir Mon und Cut als additionale, so genannte strukturelle Regeln 2. Stufe hinzufügen. Der Kalkül bleibt äquivalent.

Beispiel - vorigere Sequenzenbeweis mit explizitem Cut und Mon:

1) $A, A\to C \vdash C$	MP (1. Grades)
2) $\neg A, A\lor B \vdash B$	DS (1. Grades)
3) $B, B\to C \vdash C$	MP (1. Grades)
4) $\neg A, A\lor B, B\to C \vdash C$	Cut 2,3
5) $\neg A, A\lor B, A\to C, B\to C \vdash C$	Mon 4
6) $A, A\lor B, A\to C, B\to C \vdash C$	Mon 1
7) $A\lor B, A\to C, B\to C \vdash C$	FU 5,6
8) $A\to C, B\to C \vdash (A\lor B)\to C$	KB 7

Weitere S*-äquivalente Axiomatisierung: *Der Kalkul NL von Bergman et al:*

Hier wird DS durch aFU ersetzt.

(Ausserdem kDN durch kIB, aber das ist inessentiell).

Beweis, wie umgekehrt DS aus aFU folgt:

DS: $\Gamma \vdash A\lor B$ und $\Delta \vdash \neg A$ / $\Gamma, \Delta \vdash B$

1. $\Gamma \vdash A\lor B$	Präm
2. $\Delta \vdash \neg A$	Präm
3. $A \vdash A$	Reit
4. $\Delta, A \vdash A\land\neg A$	Kon 2,3
5. $\Delta, A \vdash B$	EFQ 4
6. $\Delta, B \vdash B$	Reit
7. $\Delta, A\lor B \vdash B$	aFU 5,6
8. $\Gamma, \Delta \vdash B$	Cut 1,7

1.	$A\lor B$	Präm
2.	$\neg A$	Präm
3.	$\quad A$	Ass
4.	$\quad A\land\neg A$	Kon 2,3
5.	$\quad\quad \neg B$	Ass
6.	$\quad\quad A\land\neg A$	Reit 4
7.	$\quad B$	kIB5-6
8.	$\quad B$	Ass
9.	$\quad B$	Reit
10.	B	aFU 3-7, 8-9

Weitere äquivalente Axiomatisierung: Anstelle von Axiom- und Regelschemata, hätten wir nur Axiome und und Regeln mit beliebigen Aussagevariablen benutzen, und die additionale Regel der Substitution hinzufügen können:

$\Gamma \vdash A \,/\, s(\Gamma) \vdash s(A)$ (für alle $s{:}\mathcal{P}\rightarrow\mathcal{L}$).

*Übungen 3.16 : **werden ausgelassen***

Beweisen Sie das Folgende (im Gentzen-Style *und:* im Fitch-Style oder Copi-Style):

a) $(A \wedge B \rightarrow C) \vdash (A \rightarrow (B \rightarrow C))$

b) $A \rightarrow B, B \rightarrow C \vdash A \rightarrow C$

c) $A \rightarrow B, A \rightarrow C \vdash A \rightarrow (B \wedge C)$

d) $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$

e) $A \rightarrow B \vdash \neg(A \wedge \neg B)$

f) $((p \rightarrow q) \rightarrow p) \rightarrow p$

g) $p \vee q \vdash \neg(\neg p \wedge \neg q)$

h) $\neg(\neg p \wedge \neg q) \vdash p \vee q$

***Weglassen:* Übungen 3.17**

Beweise durch Induktion auf n: $\{A_1,\ldots,A_n\} \vdash B$ gdw $\vdash \bigwedge\{A_1,\ldots,A\} \rightarrow B$.

****ENDE NUR KURZ ANSPRECHEN*****

4. Weitere Anwendungen und meta-logische Eigenschaften von Theoremen und Beweisen der Aussagenlogik

4.1 Äquivalenzumformungen und Normalformen:

Anmerkung: Zwei Formeln A, B sind logisch äquvalent gdw $\Vdash A \leftrightarrow B$.

Übung 4.1: *Beweisen Sie:* Zwei L-äquivalente Formeln haben die selbe Konsequenzenmenge, oder den selben logischen Gehalt: $\Vdash A \leftrightarrow B$ gdw Cn(A)=Cn(B). *Von zwei L-äquivalenten Formeln sagt man, sie drücken dieselbe Proposition aus.*

Basis-Äquivalenzgesetze des Äquivalenzkalküls:

(DN)	$A \leftrightarrow \neg\neg A$	doppelte Negation
(Komm$\wedge$)	$(A \wedge B) \leftrightarrow (B \wedge A)$	Kommutativität von $\wedge$
(Komm$\vee$)	$(A \vee B) \leftrightarrow (B \vee A)$	Kommutativität von $\vee$
(Ass$\wedge$)	$(A \wedge (B \wedge C)) \leftrightarrow ((A \wedge B) \wedge C)$	Assoziativität von $\wedge$
(Ass$\vee$)	$(A \vee (B \vee C)) \leftrightarrow ((A \vee B) \vee C)$	Assoziativität von $\vee$
(Idem$\wedge$)	$A \leftrightarrow (A \wedge A)$	Idempotenz von $\wedge$
(Idem$\vee$)	$A \leftrightarrow (A \vee A)$	Idempotenz von $\vee$
(Distr$\wedge\vee$)	$(A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$	$\wedge$-$\vee$-Distributivität 1
(Distr$\vee\wedge$)	$(A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$	$\wedge$-$\vee$-Distributivität 2
(DM$\wedge$)	$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$	deMorgan $\wedge$
(DM$\vee$)	$\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$	deMorgan $\vee$
(Def$\rightarrow$)	$(A \rightarrow B) \leftrightarrow (\neg A \vee B)$	Bedeutung von $\rightarrow$
(Def$\leftrightarrow$)	$(A \leftrightarrow B) \leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$	Definition von $\leftrightarrow$
(ÜbTaut)	$A \wedge (B \vee \neg B) \leftrightarrow A$	überflüssige Tautologie
(ÜbKont)	$A \vee (B \wedge \neg B) \leftrightarrow A$	überflüssige Kontradiktion
(GTaut)	$A \vee (B \vee \neg B) \leftrightarrow (B \vee \neg B)$	generelle Tautologie
(GKont)	$A \wedge (B \wedge \neg B) \leftrightarrow (B \wedge \neg B)$	generelle Kontradiktion
($\wedge$Abs)	$A \wedge (A \vee B) \leftrightarrow A$	$\wedge$-Absorption
($\vee$Abs)	$A \vee (A \wedge B) \leftrightarrow A$	$\vee$-Absorption

Übung 4.2: **WIRD ÜBERSPRUNGEN***

Beweisen Sie einige der Basis-Äquivalenzregeln; entweder semantisch, oder im Kalkül **S***.

n-stellige Operationen:

Kommutativität und Assoziativität von $\wedge$ und $\vee$ erlauben uns *konsekutive* n-stellige Konjunktionen und Disjunktionen, ohne Klammern geschrieben, einzuführen.

$(A_1\wedge\ldots\wedge A_n)$ $\qquad$ $(A_1\vee\ldots\vee A_n)$

Durch die Idempotenz können *n-stellige Konjunktionen/Disjunktionen* als n-stellige Operationen auf *endliche* Mengen von Formeln verstanden werden (jedes Konjunkt/Disjunkt kommt lediglich einmal vor):

$\bigwedge\{A_1,\ldots,A_n\}$ $\qquad$ $\bigwedge\Gamma_f$ $\qquad$ $\bigvee\{A_1,\ldots,A_n\}$ $\qquad$ $\bigvee\Gamma_f$

Wir definieren: $\bigwedge\{A\} =_{df} \bigvee\{A\} =_{df} A$. $\qquad$ $\bigwedge\varnothing =_{df} \top$, $\bigvee\varnothing =_{df} \bot$.

Generalisiertze Äquivalenztheoreme – Δ, Γ seien endlich.

GAssoz: $\underbrace{A_1\vee\ldots\vee A_n}_{\text{beliebige Klammerung}} \leftrightarrow \bigvee\{A_1,\ldots,A_n\}$ $\quad$ $\underbrace{A_1\wedge\ldots\wedge A_n}_{\text{beliebige Klammerung}} \leftrightarrow \bigwedge\{A_1,\ldots,A_n\}$

(GTaut) $A \wedge \bigvee\Delta \leftrightarrow A$ gdw für irgendein B, $B\in\Delta$ und $\neg B\in\Delta$.

(Sonderfall: $\bigvee\Delta \leftrightarrow \top$)

(GKont) $A \vee \bigwedge\Delta \leftrightarrow A$ gdw für irgendein B, $B\in\Delta$ und $\neg B\in\Delta$.

(Sonderfall: $\bigwedge\Delta \leftrightarrow \bot$)

(GAbs$\wedge$) $\bigwedge\Gamma \wedge \bigvee\Delta \leftrightarrow \bigwedge\Gamma$ gdw für irgendein $A\in\Gamma$, $A\in\Delta$.

Z.B., $A\wedge B\wedge(A\vee C) \leftrightarrow A\wedge B$

(GAbs$\vee$) $\bigvee\Gamma \vee \bigwedge\Delta \leftrightarrow \bigvee\Gamma$ gdw für irgendein $A\in\Gamma$, $A\in\Delta$.

Z.B., $A\vee B\vee(A\wedge C) \leftrightarrow A\vee B$

(GDistr$\wedge\vee$) $\bigwedge\{\bigvee\Delta_i$: $1\leq i\leq n\} \leftrightarrow \bigvee\{A_1\wedge\ldots\wedge A_n$: $A_i \in \Delta_i$ für alle $1\leq i\leq n\}$

Z.B.: $(A_1\vee\ldots\vee A_m) \wedge (B_1\vee\ldots\vee B_n) \leftrightarrow (A_1\wedge B_1) \vee \ldots \vee (A_m\wedge B_n)$ ($m\cdot n$ Disjunkte)

(GDistr.$\vee\wedge$) $\bigvee\{\bigwedge\Delta_i$: $1\leq i\leq n\} \leftrightarrow \bigwedge\{A_1\vee\ldots\vee A_n$: $A_i \in \Delta_i$ für alle $1\leq i\leq n\}$

Z.B.: $(A_1\wedge\ldots\wedge A_m) \vee (B_1\wedge\ldots\wedge B_n) \leftrightarrow (A_1\vee B_1) \wedge \ldots \wedge (A_m\vee B_n)$ ($m\cdot n$ Konjunkte)

Notation: Wenn B eine Teilformel von A ist, dann kennzeichnet A[B/C] eine Formel, die aus der Ersetzung von einigen Vorkommnisse von B durch C resultiert (*variable Referenz*)

Theorem: *Ersetzung von Äquivalenten:*
(Semantische Version:) Wenn $\Vdash B \leftrightarrow C$, dann $\Vdash A \leftrightarrow A[B/C]$.
(Syntaktische Version: $\vdash$ anstelle von $\Vdash$).

Übung 4.3: Beweisen Sie die semantische Version der Ersetzung von Äquivalenten durch Induktion nach der Komplexität von A. Start: A = B.
4.4 Beweisen Sie die syntaktische Version der Ersetzung von Äquivalenten durch Induktion über Kompl. von A.

Äquivalenzumformungen = sukzessive Anwendung von Äquivalenzregeln auf Teilformeln.

Das Kalkül Ä: Basis-Äquivalenzen, plus Regel der Ersetzung von Äquivalenten:

Beispiel:

Beweis von $\vdash ((\neg p \wedge q) \rightarrow \neg(q \wedge r)) \leftrightarrow (p \vee \neg q \vee \neg r)$ *in* ***Ä:***

$(\neg p \wedge q) \rightarrow \underline{\neg(q \wedge r)}$

| --------------DeM

$\underline{(\neg p \wedge q) \rightarrow (\neg q \vee \neg r)}$

| -------------Def→

$\underline{\neg(\neg p \wedge q)} \vee (\neg q \vee \neg r)$

|-------------DeM

$(\underline{\neg\neg p} \vee \neg q) \vee (\neg q \vee \neg r)$

|-------------DN

$\underline{(p \vee \neg q) \vee (\neg q \vee \neg r)}$

| ------------Ass ∨ (Wegfall von Klammern)

$p \vee \underline{\neg q \vee \neg q} \vee \neg r$

|------------Idem

$p \vee \neg q \vee \neg r$

Übungen:

Beweisen Sie die folgenden Äquvalenzen in E:

4.5 $(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$ Kontraposition

4.6 $\neg(A \rightarrow B) \leftrightarrow (A \wedge \neg B)$ Falsifikation

4.7 $(A \leftrightarrow B) \leftrightarrow (B \leftrightarrow A)$ Kommutativität von ↔

4.8 $(A \leftrightarrow B) \leftrightarrow ((A \wedge B) \vee (\neg A \wedge \neg B))$ Bedeutung von ↔

4.9 $(A \vee B) \wedge \neg(A \wedge B) \leftrightarrow (A \leftrightarrow \neg B)$

4.10 $((\neg p \wedge q) \rightarrow \neg(q \vee r)) \leftrightarrow (p \vee \neg q)$

4.11 $(p \rightarrow \neg p) \leftrightarrow \neg p$

4.12 $(p \rightarrow (q \rightarrow r)) \leftrightarrow (p \wedge q \rightarrow r)$

4.13 $(p \rightarrow (q \rightarrow r)) \leftrightarrow (q \rightarrow (p \rightarrow r))$

4.14 $(A \rightarrow B) \wedge (A \rightarrow C) \leftrightarrow (A \rightarrow B \wedge C))$

4.15 $(A \to B) \vee (C \to B) \leftrightarrow (A \wedge C \to B)$

4.15* $(A \to B) \wedge (C \to B) \leftrightarrow (A \vee C \to B)$

4.16 $A \wedge (A \to B) \leftrightarrow A \wedge B$

4.17 $A \vee (\neg A \to B) \leftrightarrow A \vee B$

4.18 $(\neg p \to (\neg q \to \neg r)) \leftrightarrow (r \to (p \vee q))$

Normalformen:

Eine Aussagevariable oder deren Negation wird *Literal* genannt -
wir schreiben $\pm p_i$.

Definition (Normalformen):

1. Eine *konjunktive Normalform* KNF ist eine (konsekutive) Konjunktion von distinkten (konsekutiven) Disjunktionen von distinkten Literalen.

$$\underbrace{(\pm p_{1,1} \vee \ldots \vee \pm p_{1,n_1})}_{\text{ein elementares Konjunkt.}} \quad \wedge \quad \ldots \quad \wedge \; (\pm p_{m,1} \vee \ldots \vee \pm p_{m,n_m})$$

Beispiel: $(p \vee q) \wedge (r \vee \neg p \vee q)$, aber nicht $\neg(p \vee q)$, $p \wedge (q \vee (r \wedge \neg p))$, usw.

2. Eine *disjunktive Normalform* DNF ist eine (konsekutive) Disjunktion von distinkten (konsekutiven) Konjunktionen von distinkten Literalen.

$$(\pm p_{1,1} \wedge \ldots \wedge \pm p_{1,n_1}) \quad \vee \quad \ldots \quad \vee \; (\pm p_{m,1} \wedge \ldots \wedge \pm p_{m,n_m})$$

Beispiel: $(p \wedge q) \vee (r \wedge \neg p \wedge q)$, aber nicht $\neg(p \wedge q)$, $p \vee (q \wedge (r \vee \neg p))$, usw.

3. B ist eine KNF von A gdw B eine KNF ist, $\Vdash B \leftrightarrow A$ und $\mathscr{P}(B) \subseteq \mathscr{P}(A)$.

4. B ist eine DNF von A gdw B eine DNF ist, $\Vdash B \leftrightarrow A$ und $\mathscr{P}(B) \subseteq \mathscr{P}(A)$.

$\rightarrow$ Eine Formel A kann mehrere verschiedene KNFs von DNFs haben (nicht-äquivalent modulo Permutation von Konjunkten und Disjunkten!):

Z.B., $p \vee q$: KNFs: nur $p \vee q$

DNFs: $p \vee q$, $(p \wedge q) \vee p \vee q$, $(p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q)$

$p \wedge q$: DNFs: nur $p \wedge q$

KNFs: $p \wedge q$, $(p \vee q) \wedge p \wedge q$, $(p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee q)$

Definition: Eine KNF (DNF) einer Formel A wird *irreduzibel genannt,* wenn keine KNF (DNF) von A *kürzer* ist.

Beispiele: $(p \wedge q) \vee p \vee q$ ist keine irreduzible DNF von $p \wedge q$, nur $p \vee q$.

$(p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee q)$ ist keine irreduzible KNF von $p \wedge q$, nur $p \wedge q$.

Hinweis: ist stärkerer Begriff von INF als der der internen DSTreichbarkeit von überflüssigen Gliedern!

Mithilfe der folgenden Prozedur können wir jede Formel A in eine DNF oder KNF von ihr umwandeln:

(1) Wir eliminieren $\rightarrow$ und $\leftrightarrow$ via Def$\rightarrow$ und Def$\leftrightarrow$.

(2) Wir bringen $\neg$'s vor Aussagevariablen via GDM$\wedge$ und GDM$\vee$, DN.

$\rightarrow$ die sog. *Negations-Normalform*.

(3) Wir produzieren eine kurze KNF oder DNF via GAss, GAbs$\wedge$, GAbs$\vee$, GTaut, GKont, Idem$\wedge$, Idem$\vee$ und:

für KNF führen wir GDistr $\vee\wedge$ durch – für DNF führen wir GDistr $\wedge\vee$ durch.

4. Durch die Anwendung weiterer Äquivalenzumformungen, können wir immer eine irreduzible KNF oder DNF produzieren.

Beispiel:

$\underline{(\neg\neg p \wedge \neg q) \rightarrow (q \wedge \neg(r \vee \neg p))}$

|------------------------------ Def→

$\underline{\neg(\neg\neg p \wedge \neg q)} \vee (q \wedge \underline{\neg(r \vee \neg p))}$

|------------------------------ 2 x DM

$(\underline{\neg\neg\neg p} \vee \underline{\neg\neg q}) \vee (q \wedge (\neg r \wedge \underline{\neg\neg p}))$

|------------------------------ 3 x DN

$\underline{(\neg p \vee q) \vee (q \wedge (\neg r \wedge p))}$ (=> Negationsnormnalform)

|------------------------------ 2 x Ass

$\neg p \vee \underline{q \vee (q \wedge \neg r \wedge p)}$ ist eine DNF

|------------------------------ Absorp∨

$\neg p \vee q$ Ist eine DNF und eine KNF

Wenn wir nicht die Abkürzung der Absorption benutzt hätten, sondern mit genereller Distribution fortgefahren wären, wäre die Umformung wie folgt weitergegangen:

$\underline{\neg p \vee q \vee (q \wedge \neg r \wedge p)}$

|----------------------------- GDistr.

$\underline{(\neg p \vee q \vee q)} \wedge (\neg p \vee q \vee \neg r) \wedge \underline{(\neg p \vee q \vee p)}$

|---------------------------1xIdem, 1xGTaut

$\underline{(\neg p \vee q) \wedge (\neg p \vee q \vee \neg r)}$

|---------------------------Absorp

$\neg p \vee q$

Übungen: Produzieren Sie kurze (möglichst irreduzible) KNFs und DNFs der folgenden Formeln:

4.18* $\neg(s \wedge t) \rightarrow \neg(\neg p \vee \neg q)$

4.19 $\neg(p \vee (p \rightarrow q)) \rightarrow \neg(\neg(p \rightarrow r) \rightarrow p)$

4.20 $\neg(p_1 \vee (p_2 \rightarrow p_3)) \rightarrow \neg(\neg(p_1 \rightarrow p_2) \wedge \neg p_3)$

4.21 $(\neg s \wedge \neg r) \rightarrow \neg(\neg p \vee \neg q) \vee \neg r$

4.22 $\neg(s \wedge t) \rightarrow \neg(\neg p \vee \neg q)$

4.23 $\neg(p \vee (p \rightarrow q)) \rightarrow \neg(\neg(p \rightarrow r) \rightarrow p)$

4.24 $\neg\neg(p \rightarrow \neg(q \wedge (r \vee \neg\neg q)))$

4.25 $\neg p \rightarrow \neg((r \rightarrow q) \wedge \neg s)$

4.26 $\neg(p \vee r \rightarrow (s \wedge (\neg q \vee r)))$

4.27 $\neg(p_1 \vee (p_2 \rightarrow p_3)) \rightarrow \neg(\neg(p_1 \rightarrow p_2) \wedge \neg p_3)$

4.28 $(\neg s \wedge \neg r) \rightarrow \neg(\neg p \vee \neg q) \vee \neg r$

4.29 $(\neg(\neg r \rightarrow \neg\neg(s \wedge t)) \vee r) \wedge (\neg s \vee (s \wedge \neg t))$

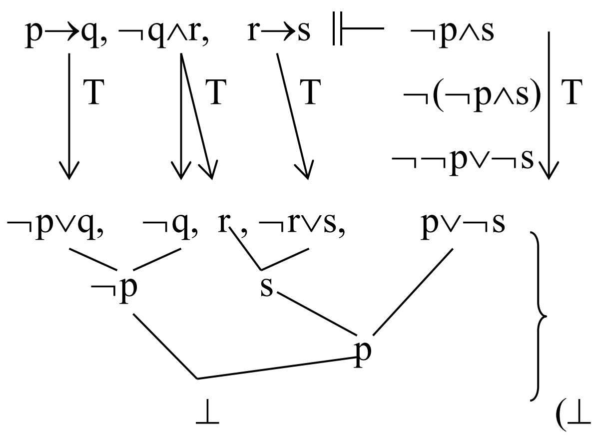
4.30 $(\neg\neg p \wedge \neg q) \rightarrow (q \wedge \neg(r \vee \neg p))$

Normalformen sind wichtig für automatisiertes Theorem-Beweisen durch Resolutions-Widerlegung!

1. Wir wandeln einen Schluss $\Gamma \vdash A$ in $\Gamma, \neg A$ um und versuchen daraus $\perp$ zu beweisen.
2. Wir wandeln $\Gamma, \neg A$ in eine Menge von elementaren Disjunktionen (sog. Klauseln) um:
3. Wir wenden einzeln die Regel der Resolution an, bis wir letztlich $\perp$ produziert haben.

Resolutions-Widerlegung ist ein vollständiges Kalkül.

Beispiel: Beweis von $p \rightarrow q$, $\neg q \wedge r$, $r \rightarrow s$ $\Vdash$ $\neg p \wedge s$ durch Resolutions-Widerlegung:



T : Transformation in Klauseln
Umwandlung in Sätze
(Umwandlungsschritte)

Resolutionsschritte
($\perp$ Abgeleitet: Widerlegungsbeweis erfolgreich!)

Definition (ausgezeichnete Normalform):

1. A ist eine ADNF (eine ausgezeichnete DNF) von B gdw A eine DNF von B ist, deren elementare Disjunkte jedes $p \in \mathcal{P}(B)$ *genau einmal* enthalten, entweder unnegiert, oder negiert.
2. Gleiches für eine AKNF (ausgezeichnete KNF).

Wir können eine DNF von B zu einer ADNF von B durch den folgenden Trick erweitern: wenn die DNF ein Disjunkt D enthält, welches eine Variable $p \in \mathcal{P}(B)$ nicht enthält, dann ersetzen wir es durch

$(D \wedge p) \vee (D \wedge \neg p)$ nach Distr. - gleiches für KNFs.

Beispiel: $\neg p \wedge q$ ist eine ADNF von sich selbst, aber keine AKNF.

Seine AKNF ist $(p \vee q) \wedge (\neg p \vee q) \wedge (\neg p \vee \neg q)$.

- *Theorem* (ausgezeichente Normalform):

1. Jedes A hat eine einzigartige ADNF und eine einzigartige AKNF (abgesehen von $\wedge$- bzw. $\vee$-Permutationen, d.h. formuliert mit $\bigwedge$, $\bigvee$), die wir mit ADNF(A) und AKNF(A) kennzeichnen, und welche im Kalkül E herleitbar ist.
2. Jedes elementare Disjunkt von ADNF(A) korrespondiert mit einer Zeile von A's Wahrheitstafel welche A wahr macht.
3. Jedes A hat eine eindeutig erweitete ADNF und AKNF in Bezug auf jede Menge $\mathcal{P} \supseteq \mathcal{P}(A)$, ableitbar im Kalkül E (d.h. jedes $p \in \mathcal{P}$ taucht in jedem elementaren Disjunkt/Konjunkt genau einmal auf).
4. Es gibt genau $2^{(2^n)}$ (verschiedene) Propositionen ausdrückbar in $\mathcal{L}(\{p_1,\ldots,p_n\})$, die jeweils mit einer eindeutigen ADNF, und AKNF in $p_1,\ldots,p_n$ korrespondieren.

Also: Wenn $\mathcal{P}$ endlich ist, kann $\mathcal{L}(\mathcal{P})$ nur endlich viele Propositionen ausdrücken.

5. *Kalkül E ist korrekt und vollständig.*

Beweis von 5: Angenommen $\Vdash A \leftrightarrow B$. Nach 3 kann jede Formel, also sowohl A wie B, in ihre ADNF umgewandelt werden in Bezug auf $\mathcal{P}(A,B)$ im Kalkül E. Die ADNF von A und die von B müssen identisch sein (modulo $\wedge$–, $\vee$-Permutationen).

Übung 4.31: Zeige anhand des Beispiels

$p \rightarrow q,\ q \rightarrow r, r \rightarrow p$

irreduzible NFs sind nicht immer eindeutig (formuliert mit $\wedge, \vee$)

4.2. Korrektheit und weitere metalogische Eigenschaften des Beweisbegriffs (Induktion nach derLänge von Beweisen)

Strukturalität: $\Gamma \vdash A \quad / \; s(\Gamma) \vdash s(A)$ *für jede beweisbare Sequenz* (und Substitutionsfunktion s)
Gilt, da Axiome und Regeln S*chemata sind*. (Beweis: siehe unten)

Endlichkeit: $\Gamma \vdash A \quad \Rightarrow \Gamma_{finit} \vdash A$ für $\Gamma_{finit} \subseteq \Gamma$ gilt per Definition

Alle deduktiven Schlussrelationen, auch die der nicht-klassischen Logik, besitzen diese Eigenschaften: *Reit, Mon, Cut, Fin, Struct* (Tarski-Eigenschaften).

Eine weitere, wichtige Beweistechnik:
(Starke) *Induktion über der Länge des Beweises einer Formel, oder Sequenz.*
Beweisen Sie eine bestimmte Behauptung für beliebige beweisbaren Formeln bzw. Sequenzen, indem Sie diese Behauptung für jedes Element eines beliebigen Beweises einer beweisbaren Formel bzw. Sequenz beweisen.
Induktionsanfang: Zeigen Sie, dass diese Behauptung für die Axiome gilt.
Induktionsschritt: Zeigen Sie, dass, wenn die Behauptung für die Prämissen einer gegeben Regel gilt, sie auch für die Konlusion der Regel gilt.

Überspringen *Am Beispiel des Strukturalitätstheorems:* $\Gamma \vdash A \quad / \; s(\Gamma) \vdash s(A)$

Lemma: Die Instanzen eines schematischen Axioms oder einer Regel (die erhalten werden durch die Ersetzung von Schemabuchstaben durch Formeln) sind unter der Substitutionsregel geschlossen, d.h. ist A Instanz von X dann ist auch s(A) Instanz von X.

Beweisskizze: Angenommen, die Instanzenfunktion I ordnet den Schemabuchstaben $L_1,\ldots,L_n$ eines der gegeben Formelschemata Aussagen $I(L_i) = A_i$ zu, und die

Substitutionsfunktion s wandelt die Aussagen A_i in die Substitutionsresultate $s(A_i)$ um. Dann erhält man die Substitutionsresultate durch die neue Instanzenfunktion $I^*(L_i) = s(A_i)$. (siehe **Übung 4.31* wird übersprungen).**

Beweis des Strukturalitätstheorems durch Induktion auf die Länge eines Beweises:
(1) Wenn $\Gamma \vdash A$ ein Sequenzaxiom ist, dann ist $s(\Gamma) \vdash s(A)$ ein Sequenzaxiom, wegen des Lemmas.
(2) Nehmen wir an, $\Gamma \vdash A$ ist abgeleitet aus $\Delta_i \vdash B_i$ ($1 \leq i \leq 2$) durch irgendeine Regel (R).
Nach IH sind $s(\Delta_i) \vdash s(B_i)$ beweisbar ($1 \leq i \leq n$); also ist $s(\Gamma) \vdash s(A)$ nach der Regel (R) ableitbar wegen des Lemmas. Q.E.D.
Ende Überspringen

Korrektheit – die semantische Korrektheit eines Kalküls:
Zur Erinnerung: schwache Korrektheit: $\vdash A \Rightarrow \Vdash A$.
starke Korrektheit: $\Gamma \vdash A \Rightarrow \Gamma \Vdash A$

Theorem (Korrektheit): *schwache und starke Korrektheit sind äquivalent.*
Informelle Erklärung: wegen Fin und Mon.
Beweis: $\Leftarrow$: schw.Korr. folgt aus st.Korr. durch Setzung von $\Gamma = \varnothing$.
$\Rightarrow$: $\Gamma \vdash A \Rightarrow \Gamma_f \vdash A$ (nach FIN) $\Rightarrow \vdash (\bigwedge\Gamma_f) \rightarrow A$ (nach $\bigwedge$-Ded.theorem, synt. Version) $\Rightarrow \Vdash \bigwedge\Gamma_f \rightarrow A$ (nach schwacher Korrektheit) $\Rightarrow \Gamma_f \Vdash A$ (nach $\bigwedge$-Ded.theorem, semant. Version) $\Rightarrow \Gamma \Vdash A$ (nach Mon für $\Vdash$). Q.E.D.

$\Gamma_f \vdash A$

....

$\bigwedge\Gamma_f \vdash A$

$\vdash (\bigwedge\Gamma_f) \rightarrow A$ KB

Theorem (starke Korrektheit): **S*** ist stark korrekt.

Lemma: L1: Alle **S***-Axiome (Instanzen von **S***-Axiom-Schemata) sind gültige Schlüsse.

L2: Alle **S***-Regeln (Instanzen von **S***-Regel-Schemata) erhalten Gültigkeit.

(Beweis des Lemmas: siehe Kapitel über Semantik).

*Beweis: Durch Induktion über die Länge eines **S*** -Beweises*

$<\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n>$ von $\Gamma_n \vdash A_n$.

Induktionsanfang: Wenn $\Gamma_i \vdash A_i$ ein Axiom ist, dann ist es gültig, wegen des Lemmas L1.

IS: Nehmen wir an $\Gamma_i \vdash A_i$ ist abgeleitet aus vorigen Gliedern des Beweises, $\Gamma_j \vdash A_j$ und (möglicherweise) $\Gamma_k \vdash A_k$ (mit j, k < i) nach einer der Regeln.

Nach **IH** sind $\Gamma_j \vdash A_j$ und $\Gamma_k \vdash A_k$ gültige Schlüsse.

Also ist wegen des Lemmas L2 $\Gamma_i \vdash A_i$ ein gültiger Schluss. Q.E.D.

Definition (Konsistenz):

1. Eine Logik **L** wird (einfach) konsistent genannt gdw es kein A gibt, sodass $\vdash A \wedge \neg A$.
2. Eine Formelmenge Γ ist (einfach) konsistent gdw es kein A gibt, sodass $\Gamma \vdash A \wedge \neg A$.

Folgt aus dem *Theorem* der *Korrektheit*: **L** ist konsistent.

Beweis: $A \wedge \neg A$ ist nicht L-wahr (also L-falsch), und daher, nach der Korrektheit, unbeweisbar.

Übung 4.32: Beweisen Sie: **L** ist (stark) korrekt ⇔ jede semantisch erfüllbare Formelmenge ist konsistent.

Übung 4.32*: Beweisen Sie: Γ ist konsistent ⇔ $\exists A$: $\Gamma \not\vdash A$ d.h. $Cn(\Gamma) = \{A: \Gamma \vdash A\} \neq \mathcal{L}$. Diese Eiegenschaft nennt man auch: "absolute Konsistenz"

NUR KURZ ANSPRECHEN

Hilbert-Style Kalküle (Tradition nach Frege, Hilbert und Lukasiewicz):

Kalkül **HL:**

Axiome: Alle Instanzen von:

$\rightarrow$KB: $(A \wedge B \rightarrow C) \rightarrow (A \rightarrow (B \rightarrow C))$

$\rightarrow$MP: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

$\rightarrow$SIMP: $(A \wedge B) \rightarrow A$; $(A \wedge B) \rightarrow B$

$\rightarrow$KON: $(A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow (B \wedge C))$

$\rightarrow$ADD: $A \rightarrow (A \vee B)$; $A \rightarrow (B \vee A)$

$\rightarrow$aFU: $(A \rightarrow B) \rightarrow ((C \rightarrow B) \rightarrow ((A \vee C) \rightarrow B))$

$\rightarrow$iIB: $(A \wedge B \rightarrow C \wedge \neg C) \rightarrow (A \rightarrow \neg B)$

$\rightarrow$kIB: $(A \wedge \neg B \rightarrow C \wedge \neg C) \rightarrow (A \rightarrow B)$

Regel: Alle Instanzen von: MP: $A, A \rightarrow B$ / B Modus Ponens.

Metalogische Ökonomie vs. Objektspraschliche Praktikabilität eines Kalküls.

Definition (Beweis in **HL**):

1. $\Gamma \vdash A$ ist beweisbar in **HL**, $\Gamma \vdash_{HL} A$, gdw es einen Beweis von $\Gamma \vdash A$ in **HL** gibt, d.h. eine endliche Sequenz $<A_1,\ldots,A_n>$ von Formeln, sodass jedes A_i entweder ein Axiom von **HL** ist, oder ein Element von Γ oder nach MP aus irgendeinem A_k, $A_j = A_k \rightarrow A_i$ $(j, k<i)$.

2. $\vdash_{HL} A$ gdw $\varnothing \vdash_{HL} A$.

(**HL** = die kleinste Formelmenge, die alle **HL**-Axiome enthält und unter MP geschlossen ist.)

$\rightarrow$Die (starke und schwache) Korrektheit von **HL** ist bewiesen nach Induktion auf die Länge eines **HL**-Beweises, indem man zeigt: 1. Alle **HL**-Axiome sind gültig.
2. MP ist gültigkeitserhaltend.

$\rightarrow$ Die *Theorem-Äquivalenz* von **HL** und **S*** ist bewiesen, indem man zeigt, dass:

(**S*** $\subseteq$ **HL**): alle Regeln 1. und 2. Stufe von **S*** sind beweisbar in **HL**. (Reduktion auf die st./schw. Korrektheit von **S***). Dies ist *mühsam* (durch Induktion auf die Länge des Beweises von HL-Beweisen zeigt sich, dass diverse Regeln 1. und 2. Stufe gelten, z.B. KB: $\Delta, A \vdash_{HL} B \Rightarrow \Delta \vdash_{HL} A \rightarrow B$).

Die andere Richtung, **HL** $\subseteq$ **S*,** gilt nach Korrektheit von **HL** und Vollständigkeit von S*.

4.3 Vollständigkeit

Zur Erinnerung: schwache Vollständigkeit: $\Vdash A \;\Rightarrow\; \vdash A$

starke Vollständigkeit: $\Gamma \Vdash A \;\Rightarrow\; \Gamma \vdash A$.

Schw.V. und st.V. sind nicht (trivial) äquivalent, weil $\Vdash$ nicht per Definiton finitär (bzw. kompakt) ist (wie $\vdash$)!

- *Theorem* (Konsistenz-Version der Vollständigkeit, Gödel):

1. **L** ist schwach vollständig gdw jede konsistente Formel erfüllbar ist.
2. **L** ist stark vollständig gdw jede konsistente Formelmenge erfüllbar ist.

Beweis: Theorem Nr. 2. durch Kontraposition:

$\Rightarrow$: Wir nehmen an Γ ist nicht erfüllbar und zeigen, unter der Annnahme der starken Vollsändigkeit, dass Γ inkonsistent ist.

Wenn Γ unerfüllbar ist, dann $\Gamma \Vdash B\wedge\neg B$, also, nach st. Vollständikeit, $\Gamma \vdash B\wedge\neg B$, also Γ ist inkonsistent.

$\Leftarrow$: Wir nehmen an, dass Γ |-/- A, und zeigen, unter der Annahme, dass jede konsistente Formelmenge erfüllbar ist, dass Γ ||-/- A.

Γ |-/- A impliziert, dass $\Gamma,\neg A$ konsistent ist, denn andernfalls $\Gamma, \neg A \vdash B\wedge\neg B$, was implizieren würde, dass $\Gamma \vdash A$ nach *kIB* (!). Also ist $\Gamma, \neg A$ erfüllbar (weil wir annehmen, dass jede konsistente Formel erfüllbar ist). Und daher Γ ||-/- A. Q.E.D.

– Für Theorem Nr.1 argumentieren wir wie für Nr.2, abgesehen davon, dass wir $\Gamma = \{A\}$ in $\Rightarrow$, und $\Gamma = \varnothing$ in $\Leftarrow$ setzen. Q.E.D.

<u>Kanonischer Vollständigkeitsbeweis: Gödel, Lindenbaum, Henkin</u>

- *Definition* (maximal konsistente Formelmengen)

Δ ist maximal konsistent gdw Δ konsistent ist und keine echte Erweiterung von Δ – d.h. kein Γ, sodass $\Delta \subset \Gamma$ – konsistent ist.

- *Theorem* (maximal konsistente Formelmengen):

Angenommen Γ ist maximal konsistent. Dann gilt für alle A:

(Max $\vdash$): $\Gamma \vdash A \Leftrightarrow A \in \Gamma$ deduktive Abgeschlossenheit

(Max $\neg$): $A \in \Gamma$ oder $\neg A \in \Gamma$ syntaktische Vollständigkeit

(Max $\vee$): $(A \vee B) \in \Gamma \Leftrightarrow (A \in \Gamma)$ oder $(B \in \Gamma)$ Prim-heit

(Max $\wedge$): $(A \wedge B) \in \Gamma \Leftrightarrow (A \in \Gamma)$ und $(B \in \Gamma)$

(Max $\rightarrow$): $(A \rightarrow B) \in \Gamma \Leftrightarrow$ (wenn $A \in \Gamma$, dann $B \in \Gamma$)

Anmerkung: Alle Max-Eigenschaften gelten auch in der intuitionistischen Logik.

Übung 4.33: Beweisen Sie das Theorem über maximal konsistenter Formelmengen und formalisieren Sie den Beweis (im Gentzen-, oder Fitch-Style)

Der Gödel-Henkin Vollständigkeitsbeweis vollzieht sich in zwei Schritten:

- Man zeige, dass jede konsistente Formelmenge in einer maximal konsistenten Formelmenge enthalten ist.
- Man zeige, dass jede maximal konsistente Formelmenge ein Modell hat.

Theorem (Lindenbaum-Lemma): Jedes konsistente Δ kann zu einem maximal konsistenten $\Gamma \subseteq \Delta$ erweitert werden.

Beweis: Wir können alle Formeln effektiv aufzählen (*siehe später*).
Ist eine solche Aufzählung gegeben,
$A_0, A_1, A_2, \ldots$ (i: $|N =_1 \mathcal{L}$) ($=_1$ steht für bijektive Abb.)
dann definieren wir rekursiv die folgende Aufzählung von ansteigenden Erweiterungen von Δ:

$\Gamma_0 := \Delta$

$\Gamma_{n+1} :\begin{cases} = \Gamma_n \cup \{A_n\} & \text{wenn } \Gamma_n \cup \{A_n\} \text{ konsistent ist,} \\ \text{andernfalls } \Gamma_n. \end{cases}$

Es sei: $\Gamma: = \bigcup \{\Gamma_i \mid i \in |N \}$.

Wir zeigen, dass Γ maximal konsistent ist:

1. Γ ist konsistent: Denn, wenn dem nicht so ist, dann $\Gamma \vdash A \wedge \neg A$, also gibt es nach *Fin* ein finites $\Gamma_f \subseteq \Gamma$ sodass $\Gamma_f \vdash A \wedge \neg A$. Sei n die Zahl der Formel in Γ_f mit der höchsten Nummer. Dann $\Gamma_f \subseteq \Gamma_{n+1}$. Also $\Gamma_{n+1} \vdash A \wedge \neg A$ nach Mon, was der Definition widerspricht.
2. Γ ist maximal konsistent: Nehmen andernfalls gibt es ein $A \notin \Gamma$ sodass $\Gamma \cup \{A\}$ konsistent ist. Sei n A's Nummer, also $A = A_n$. Da $\Gamma_n \subseteq \Gamma$, ist $\Gamma_n \cup \{A_n\}$ konsistent. Also $A_n \in \Gamma_{n+1}$ per Def. weshalb $A_n \in \Gamma$, was unserer Annahme wiederspricht.

Q.E.D.

Theorem (Wahrheitslemma):
Jede maximal konsistente Formelmenge hat ein Modell (d.h. eine Bewertung v die all ihre Formeln wahr macht).

Beweis: Wir definieren:
für alle p **v(p) = 1 gdw p $\in \Gamma$** $\dashrightarrow$ Gödel-Henkin-Modell.
Mit dieser Definition zeigen wir durch Induktion auf der Komplexität von Formeln,

dass:

$v \models\!= A$ gdw $A \in \Gamma$ für jedes $A \in \mathcal{L}$.

(1) Für A=p gilt das Theorem per Definition.

(2) $A=\neg B$: $v \models\!= \neg B$ gdw $v \not\models\!= B$ gdw $B \notin \Gamma$ (nach IH) gdw $\neg B \in \Gamma$ (nach Max $\neg$).

(3) $A=B\wedge C$: $v \models\!= B\wedge C$ gdw $v \models\!= B$ und $v \models\!= C$ gdw $B \in \Gamma$ und $C \in \Gamma$ (nach IH) gdw $(B\wedge C) \in \Gamma$ (nach Max $\wedge$).

(4) $A=B\vee C$: $v \models\!= B\vee C$ gdw $v \models\!= B$ oder $v \models\!= C$ gdw $B \in \Gamma$ oder $C \in \Gamma$ (nach IH) gdw $(B\vee C) \in \Gamma$ (nach Max $\vee$).

(5) $A=(B\rightarrow C)$: $v \models\!= B\rightarrow C$ gdw ($v \models\!= B \Rightarrow v \models\!= C$) gdw ($B \in \Gamma \Rightarrow C \in \Gamma$) (nach IH) gdw $(B\rightarrow C) \in \Gamma$ (nach Max$\rightarrow$). - Q.E.D.

Anmerkung : Beachten Sie, dass alle Max-Eigenschaften benutzt wurden.

Theorem (starke Vollständigkeit):

S* ist stark (und damit schwach) vollständig.

Beweis: Nehmen wir an, Δ ist konsistent. Dann ist Δ in einem maximal konsistenten Γ enthalten (nach Lindenbaum-Lemma). Γ hat ein Modell v nach Wahrheitslemma. v ist auch ein Modell von Δ, da $\Delta \subseteq \Gamma$. Also ist Δ erfüllbar. Also ist **S*** stark vollständig, gemäß der Konsistenz-Version. Q.E.D.

Theorem (Kompaktheit): Sei Γ unendlich.

1. Schluss-Version: $\Gamma \Vdash A$ gdw für irgendeine finite Teilmenge $\Gamma_f \subset \Gamma$, $\Gamma_f \Vdash A$.
2. Erfüllbarkeits-Version: Γ ist erfüllbar gdw jede endliche Teilmenge von Γ erfüllbar ist.

Übung 4.34: Beweisen Sie die Kompaktheit (benutzen Sie die Endlichkeit von $\vdash$, Korrektheit und Vollständigkeit).

Da wir die Vollständigkeit bewiesen haben, folgt, dass alle Metatheoreme in semantischer und syntaktischer Version gültig sind: wir dürfen $\vdash$ und $\Vdash$ austauschen.

Theorem (konservative Extension durch eine explizite Definition $p :\leftrightarrow D$):
Nehmen wir an $p \notin \mathcal{P}(\Gamma)$, $\mathcal{P}(D) \subseteq \mathcal{P}(\Gamma)$. Dann gilt für alle A mit $\mathcal{P}(A) \subseteq \mathcal{P}(\Gamma)$:
$\Gamma \cup \{p \leftrightarrow D\} \Vdash\!\!— A$ gdw $\Gamma \Vdash\!\!— A$.

Beweis: $\Leftarrow$ ist trivial.

$\Rightarrow$: Wenn wir rückwirkend $\top$ und $\bot$ für p im linken Schluss substituieren, erhalten wir durch das Theorem der uniformen Substitution und die Aussagenlogik:

(i) $\Gamma \cup \{D\} \Vdash\!\!— A$ und (ii) $\Gamma \cup \{\neg D\} \Vdash\!\!— A$

wodurch wir nach aFu $\Gamma \Vdash\!\!— A$ erhalten. Q.E.D.

Übung 4.35 Es sei $\{p_i \leftrightarrow D_i: 1 \leq i \leq n\}$ eine Menge von Definitionen mit $p_i \notin \mathcal{P}(\Gamma)$ und $\mathcal{P}(D_i) \subseteq \mathcal{P}(\Gamma)$für alle $1 \leq i \leq n$.
Wir nehmen an $\Gamma \cup \{p_i \leftrightarrow D_i: 1 \leq i \leq n\} \Vdash\!\!— A$ (A ist Formel der erweiterten Sprache).
A* sei das Resultat der Ersetzung von jedem p_i in A durch D_i. Beweisen Sie:
$\Gamma \Vdash\!\!— A^*$, durch Verwendung des Theorems der konservativen Extension durch Definition.

5. Prädikatenlogik 1. Ordnung (PL)

5.1 Sprache

In diesem Kapitel ist $\mathcal{L} = \mathcal{L}1$ = die Sprache der PL.

Das Alphabet von $\mathcal{L}$ enthält:

Nichtlogische (extralogsiche Symbole):

– Für jedes n ≥ 0: eine abzählbare Menge $\mathcal{R}_n$ von n-stelligen Prädikat-Symbolen

F, G, …, R, Q,… (indiziert) $\mathcal{R} = \bigcup_{n\in|N} \mathcal{R}_n$

($\mathcal{R}_0$ ist die Menge der Aussagevariablen.)

– Für jedes n≥0: eine abzählbare Menge $\mathcal{F}_n$ von n-stelligen Funktionssymbolen

echte Funktionen: n>0 f, g, … (indiziert) für echte Funktionen

$\mathcal{F} := \bigcup \{\mathcal{F}_n : n\in\omega_+\}$

Ein 0-stelliges Funktionssymbol ist eine Individuen-"konstante" (freie Individuen-variable)

– $\mathcal{C} := \mathcal{F}_0$ die Menge von Individuenkonstanten a, b, … (indiziert)

Logische Symbole:

AL: Konnektive: *primitiv:* ¬, ∨ *definiert:* ∧, →, ↔, ⊥, T

PL: eine abzählbar unendliche Megne von Variablen $\mathcal{V}$ x, y, z, … (indiziert)

Quantoren: *primitiv:* ∀ *definiert:* ∃

Identitätsprädikat: ≡

Abgesehen von ≡, können wir all diese Symbole auch in unserer Metasprache verwenden.

Wie in der AL, überlegen wir uns zuerst alle Zeichenreihen s, s_1,…

Rekursive Definition von "(singulären) Termen von $\mathcal{L}$" : (neu vgl. zu Logik1)

$\mathcal{T}$ bezeichnet die Menge aller Terme $t_1, t_2, \ldots$ sind Metavariablen für Terme

1. $s \in \mathcal{V} \cup \mathcal{C} \Rightarrow s \in \mathcal{T}$
2. $f \in \mathcal{F}_n$ $(n>0)$, $t_1,\ldots,t_n \in \mathcal{T} \Rightarrow ft_1\ldots t_n \in \mathcal{T}$

Klammerkonvention: Wir dürfen auch $f(t_1,\ldots,t_n)$ statt $ft_1\ldots t_n$ schreiben. *Nur* dann kann man obere Indizes bei Funktionszeichen ohne Konfusionsgefahr weglassen.

Rekursive Definition von "Formeln von $\mathcal{L}$" – $\mathcal{L}$ steht für die Menge aller Formeln:

$$\left.\begin{array}{l} 1.\ R \in \mathcal{R}_n,\ t_1,\ldots,t_n \in \mathcal{T} \Rightarrow Rt_1\ldots t_n \in \mathcal{L} \\ \quad t_1, t_2 \in \mathcal{T} \Rightarrow t_1 \equiv t_2 \in \mathcal{L} \end{array}\right\} \text{ atomare Formeln}$$

2. PL: $A \in \mathcal{L} \Rightarrow \neg A \in \mathcal{L}$

   $A, B \in \mathcal{L} \Rightarrow (A \vee B) \in \mathcal{L}$

3. Quant.: $A \in \mathcal{L}$, $x \in \mathcal{V} \Rightarrow \forall xA \in \mathcal{L}$.

Anmerkung: dies definiert die Menge aller offenen, oder geschlossenen Formeln.

Unterschiede zu Logik I:

1) Zu den "freien Individuenvariablen" in Logik I sagen wir nun Individuenkonstanten a, b. Unter freien Individuenvariablen verstehen wir nun frei vorkomenmde x, y in offenen Formeln.

2) In Logik I hatten wir nur Sätze. Nun haben wir auch Formeln mit freien Individuenvariablen: sogenannte *offene Formeln* Fx, Rxy,...

3) Wir erlauben nun $\forall x \exists x Fx$, $\forall x Fa$, etc. Variablenkonfusionen werden nun verhindert durch die Definition der korrekten *Termsubstitution* (s. unten).

4) Wir haben auch Funktionszeichen und Identitätszeichen; daher komplexe Terme.

Definitionen: $\exists xA := \neg\forall x \neg A$

$(A \wedge B) := \neg(\neg A \vee \neg B)$ $\quad \bigwedge\Gamma$ wie zuvor

$(A \rightarrow B) := (\neg A \vee B)$ $\quad \bigvee\Gamma$ wie zuvor

$(A \leftrightarrow B) := ((\neg A \vee B) \wedge (\neg B \vee A))$

Klammerkonventionen – wie zuvor, plus:

Wir dürfen (a≡b) statt a≡b schrieben, $F(t_1,\ldots,t_n)$ statt $Ft_1\ldots t_n$

Wie in AL können wir beweisen:

Jeder Term und jede Formel, hat eine *grammatische Konstruktion*, welche wir in baumartiger Gestalt aufzeigen können.

Obere Indizes von Funktions- oder Prädikatensymbolen geben deren Stelligkeit an.

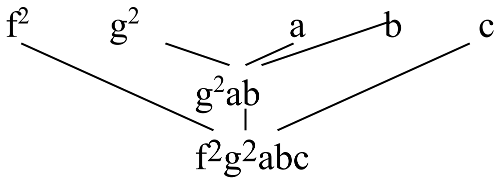
Wir können sie erlassen, aber nur wenn die Lesbarkeit als Formel nicht ambig ist.

Fgax: nicht eindeutig: F(g(a),x) oder F(g(a,x))

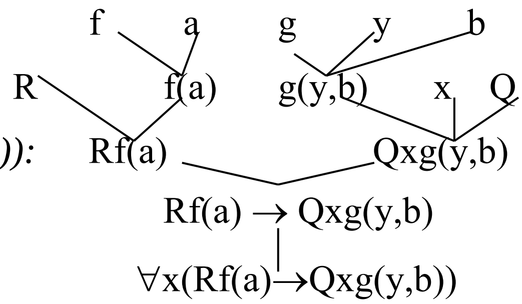
$F^2g^1ax \quad F^1g^2ax$

Beispiele für grammatische Strukturbäume:

f^2g^2abc:



$\forall x(Rf(a)\rightarrow Qxg(y,b))$:



Übung: Welche der folgenden Zeichenreihen sind wohlgeformte Terme oder Formeln (in einer nicht-ambigen Weise lesbar). Wenn sie es sind, zeichenen Sie ihren grammatischen Strukturbaum:

5.1. Terme: f(x,a), g^3af^2yz, g^2aR, f(x,y, g(x,y),h(x,y,z)), ffffa

5.2. Formeln: Rxfyza, Qafb → Gxy,

∀x¬Fx→Ga, ∀x¬(Fx→Ga), ∀x(¬Fx→Ga), ∀x(¬(Fx→Ga)),

∀x ∃y(Ty ∧ (Hxy → Mx)),

∀x∃y(fx→Gy), ∀x(Fx ∧ Gf(y,x)) → ¬∃xWx

→ In induktiven Beweisen auf die Komplexität von Formeln müssen wir häufig mit Induktion auf die Komplexität von Termen beginnen.

Terminologie: Eine Formel ohne Quantoren wird *singulär* genannt.

Eine atomare Formel oder ihre Negation nennt man *Literal*, oder *Basis-Satz* (Carnap).

Eine Formel der Form $\forall x_1 \ldots \forall x_n A$ für singuläres A wird *universell* genannt

Eine Formel der Form $\exists x_1 \ldots \exists x_n A$ für singuläres A wird *existentiell* genannt

Der Begriff der *Teilformel* ist wie in der AL definiert.

Das Theorem der eindeutigen Lesbarkeit wird wie in der AL bewiesen.

Quantorenbereich:

Wir berücksichtigen immer das Bündel aus Quantor plus angehängter Variable

$\forall x$, $\exists x$ $\forall y$ etc.

Der Bereich eines Quantors ist die Formel unmittelbar rechts von der anghängten Variable. Diese Definition ist anders, als die Bereichsdefinition für aussagenlogische Operatoren – denn wir möchten sagen:

$\forall x$, $\exists x$ bindet diejenigen Variablen in seinem Bereich, die *frei* darin sind (siehe unten).

Beispiele:

$\forall x\,(Mx \rightarrow Ex)$ Alle Metalle leiten Strom

$\exists x(Sx \wedge \neg Wx)$ Es gibt einen Schwan, der nicht weiß ist.

$\leftrightarrow \neg\forall x\neg(Sx \wedge \neg Wx) \leftrightarrow \neg\forall x(Sx \rightarrow Wx)$

$\forall x\ \forall y\ L\,x\,y$

$\forall x\forall yLxy$ Jeder liebt jeden

$\leftrightarrow \forall y\forall xLxy$ Jeder wird von jedem geliebt.

Gleichermaßen: $\exists x\ \exists y\ Lxy$ Jemand liebt jemanden.

$\forall x\exists yLxy$ Jeder liebt jemanden.

$\exists x\forall yLxy$ Jemand liebt alle. (Jeder wird von dem selben geliebt)

$\exists x\forall yLxy \ \Vdash\ \forall y\exists xLxy$ Jeder wird von jemandem geliebt.

(stärker) (schwächer)

Definition der Existenz einer Grenze 'lim' einer infiniten Sequenz von positiven, reellen Zahlen $(r_1,r_2,\ldots)$*:*

$\exists lim \in |R^+\ \forall\varepsilon>0\ \exists n\in|N\ \forall m\geq n: |r_m - lim| \leq \varepsilon.$

Abkürzungen: $\forall x,yA$ – steht für $\forall x\forall yA$

$\forall x\in B:A$ steht für $\forall x(x\in B \rightarrow A)$. $\forall x>y: A$ steht für $\forall x(x>y \rightarrow A)$.

Anm.: $\forall xFa$ – dies ist erlaubt: $\forall x$ bindet nichts: $\forall xFa \leftrightarrow Fa$.

Z.B.: Alles ist so, dass die Erde rund ist.

$\forall x\exists xLxx$ – der *innerste* Quantor ($\exists$) bindet zuerst: $\forall x\exists xLxx \leftrightarrow \exists xLxx$.

Notation: Für eine Formel A, seien $\mathcal{V}(A)$, $\mathcal{C}(A)$, $\mathcal{T}(A)$, $\mathcal{R}(A)$, $\mathcal{R}^n(A)$, $\mathcal{F}(A)$, $\mathcal{F}^n(A)$, die Menge aller Individuenvariablen, Individuenkonstanten, Terme, Prädikatensymbole, n-stellige Prädikatensymbole, Funktionssymbole, n-stellige Funktionssymbole, die irgendwo in A vorkommen. *Gleiches für Terme t:* $\mathcal{V}(t)$, $\mathcal{C}(t)$, $\mathcal{T}(t)$, $\mathcal{F}(t)$, $\mathcal{F}^n(t)$ (keine Relationssymbole kommen in t vor) und *für Formelmengen:* $\mathcal{V}(\Gamma)$, $\mathcal{C}(\Gamma)$, $\mathcal{T}(\Gamma)$, $\mathcal{R}(\Gamma)$, $\mathcal{R}^n(\Gamma)$, $\mathcal{F}(\Gamma)$, $\mathcal{F}^n(\Gamma)$.

Definition (Freiheit und Bindung, offene und geschlossene Formeln):

1. Ein *Vorkommnis* einer Variable v in A wird *frei* in A genannt gdw sie nicht im Bereich eines Quantors vorkommt, der v als zugehörige Variable hat ($\forall v$ or $\exists v$).
2. Eine *Variable* ist frei in A gdw sie *mindestens ein* freies Vorkommnis in A hat.
$\mathcal{V}_f(A)$ = Die Menge der Variablen, die frei in A sind.
3. Eine Formel von $\mathcal{L}$ die keine freien Variablen enthält wird auch *geschlossene Formel*, oder *Satz* gennant. Andernfalls ist sie eine *offene Formel*.

Hinweise: 1.) Puristen definieren den Begriff eines "freien Variablenvorkommnisses" rekursiv, und zwar so:

i) Wenn A atomar ist, dann ist das (jedes) Vorkommnis jeder Variable in A frei in A.

ii) Wenn A = $\neg$B, ist ein v-Vorkommnis frei [gebunden] in A gdw sie frei [gebunden, resp.] in B ist.

iii) Wenn A = B**o**C, dann ist ein v-Vorkommnis, dass in der Teilformel B von A vorkommt frei [gebunden] in A gdw sie frei [gebunden, resp.] in B ist, – und gleiches für C.

iv) Wenn A = □$\forall$xB, dann ist ein v-Vorkommnis frei in A gdw v$\neq$x und v frei ist in B, andernfalls (wenn v=x), ist v gebunden in A.

2.) Offene Formeln Fa, Fa$\wedge$Gx, Fx$\wedge\exists$yRxy, Rxz, etc. sind weder wahr, noch falsch! Vielmehr drücken sie (möglicherweise komplexe) Prädikate aus – deren Stelligkeit = die Anzahl der freien Variablen. Deren Interpretation ist kein Wahrheitswert, sondern eine Extension.

3.) Notation: A[x] Bezeichnet eine offene Formel, ein *komplexes Prädikat*, welches x frei enthält (es kann auch andere freie Variablen enthalten):
4.) Gebundene Variablen haben nur syntaktische Funktion: $\forall xA[x] \leftrightarrow \forall yA[y]$
5.) $\forall xA \leftrightarrow \exists xA \leftrightarrow A$ gdw A *geschlossen* ist (keine freien Variablen enthält). Also: $\forall xFa \leftrightarrow Fa$, und $\forall x\exists xFx \leftrightarrow \exists xFx$ – d.h. der innerste Quantor bindet die Variable.

Übung 5.3: Bestimmen Sie die Quantorenbereiche, die freien und gebundenen Variablenvorkommen, und die freien Variablen, der folgenden Formeln. Welche Quantoren binden nichts? Welche dieser Formeln sind Sätze?
(a) $\exists xRxx \rightarrow Rax$, (b) $\neg Ff(a,z) \rightarrow \forall zFz$, (c) $\forall x\exists y(Ty \vee (Hxy \rightarrow Mxa)) \wedge Rxb)$,
(d) $\forall x(Fa \wedge (\exists yGxz \vee \exists yRybf(x)) \rightarrow Ryx)$, (e) $\forall x\exists y(Fa \wedge Fy \rightarrow \neg Gx) \wedge \exists z(Fu \wedge \neg Gy)$,
(f) $\exists u\forall x\exists z(Ff(x,y,a) \rightarrow Gf(x,z,a))$.

Übung 5.4: Geben Sie eine rekursive Definition für $\mathcal{V}_f(A)$.

5.2 Semantik

Definition (Bewertungen, Interpretationen, Belegungen, Strukturen):

1. Eine $\mathcal{L}$-*Bewertung* ist ein Paar <D, v> wobei $D \neq \varnothing$ eine nicht-leere Menge von Individuen, der so genannte *Objektbereich*, und die Bewertungsfunktion v eine Funktion $\mathcal{R} \cup \mathcal{F} \cup \mathcal{V}$ in mengentheoretische Strukturen von D ist, nach dem *Typ* definiert wie folgt:

$v = v_{\mathcal{R},n} \cup v_{\mathcal{F},n} \cup v_{\mathcal{V}}$

$$\left.\begin{array}{ll} v_{\mathcal{R},n}: \mathcal{R}^n \to \mathbb{P}(D^n) & \text{also für alle } R \in \mathcal{R}^n \ (n \geq 0)\text{: } v(R) \subseteq D^n \\ v_{\mathcal{F},n}: \mathcal{F}^n \to D^{(D^n)} & \text{also für alle } f \in \mathcal{F}^n \ (n>0)\text{: } v(f)\text{: } D^n \to D \\ \text{speziell: } v_{\mathcal{C}} : \mathcal{C} \to D & \text{also für alle } a \in \mathcal{C} : v(a) \in D \end{array}\right\} \text{Interpretation}$$

$v_{\mathcal{V}}$: $\mathcal{V} \to D$ also für alle $x \in \mathcal{V}$: $v(a) \in D$ – eine *Variablen-Belegung*

2. $v{\uparrow}(\mathcal{R} \cup \mathcal{F})$ wird eine Interpretationsfunkiton gennant und <D,I> eine $\mathcal{L}$-*Interpretation*.

Interpretationen interpretieren *nicht-logische Terme* und determinieren die Wahrheitswerte von Sätzen, aber nicht von offenen Formeln.

$v{\uparrow}\mathcal{V}$ wird eine Variablen-Belegungsfunktion genannt, kurz eine $\mathcal{V}$-*Belegung*.

$\Rightarrow$ Eine Interpretation plus eine Variablenbelegung ist eine *Bewertung*. Sie determiniert *hypothetische Wahrheitswerte*, sogar für offene Formeln (Wenn die freien Variablen diese Objekte denotieren *würden*, dann *wären* die Wahrheitswerte des Satzes so-und-so.)

Wenn wir Bewertungen für offene Formeln in Betracht ziehen, dann fungieren freie Variablen wie nicht-logische Symbole. Wir tun das nur 'hypothetisch'.

Hinweis.: Für $p \in \mathcal{P}$, $v(p) \subseteq D^0 = \{\varnothing\}$; was entweder $\varnothing$:=0 oder $\{\varnothing\}$:=1 ist.

<D,I> wird auch eine $\mathcal{L}$-*Struktur* genannt oder $\mathcal{L}$-Modell nach Tarski.

Nehmen wir an, die Relationssymbole sind als *indizierte Mengen*, $\mathcal{R} = \{R_i: i \in <N\}$, gegeben und gleiches gilt für $\mathcal{F}$; dann kann die $\mathcal{L}$-Struktur in der folgenden, ‚expliziten' Form geschrieben werden :

$<D, \{v(R_i): i \in |N\}, \{v(f_i): i \in |N, \text{Stelligkeit}(f_i)>0\}, \{v(c_i): i \in |N, \text{Stelligkeit}(c_i) = 0\}>$.

Solche Strukturen sind mögliche Welten in einer mengentheoretischen Repräsentation.

Oft unterscheiden wir zwischen *sprachlichen Entitäten* als Gegenstück zu *mengentheoretischen Entitäten* wie folgt: a, b … sind Konstanten in $\mathcal{C}$; kursiv *a*, *b*, … sind (zugeordnete) Individuen in D; gleichermaßen R, Q…Relationssymbole; *R*, *Q*,… (zugeordnete) Relationen über D, etc. Aber wenn der Kontext klar ist, werden wir überflüssige Kursivierungen weglassen.

Notation: Für eine gegebene Bewertungsfunkiton v, ist v[x:*d*] wie v außer, dass sie *d* der Variable x zuordnet. Gleichermaßen ist $v[x_1{:}d_1,\dots,x_n{:}d_n]$ wie v außer, dass sie d_i verwendet, statt x_i $(1 \leq i \leq n)$.

(Manchmal erlauben wir diese Notation auch für Individuenkonstanten, z.B. v[a:*d*].)

Definition (rekursive Extension von v auf Terme und Formeln – *D als gegeben angenommen*):

1. *Terme:*

(i) Für $t \in \mathcal{V} \cup \mathcal{C}$: bereits definiert.

(ii) Für $n>0$, $f \in \mathcal{F}^n$, $t_1,\dots,t_n \in \mathcal{T}$: $v(ft_1\dots t_n) = v(f)(v(t_1,\dots,v(t_n))$

Beispiel:

$D = \{1, 2, 3, 4, ...\}$,$v(a) = 1$, $v(b) = 2$, $v(c) = 3$, $v(f) = +$

$v(f^2(a, b)) = v(f^2)(a, b) = (v(a), v(b)) = +(1, 2) = 1 + 2 = 3$

$v(f^2(c, f^2(a, b)) = v(f^2)(v(c), v(f^2(a, b))) = +(3, 1 + 2) = (1 + 2) + 3 = 1 + 2 + 3 = 6$

2. *Formeln:*

(i) *Atomar:* Für n≥0≥m $R \in \mathscr{R}_n$, $t_1,\ldots,t_n \in \mathscr{T}$:

(i.1) $v(Rt_1\ldots t_n) = 1$ gdw $<v(t_1),\ldots,v(t_n)> \in v(R)$ (sonst= 0).

Fortsetzung Beispiel:

$v(R^2) = < = \{<1,2>, <1,3>, <1,4>, \ldots <2,3>, <2,4>, <2,5>, \ldots <3,4>, <3,5>, \ldots\}$

$v(Rab) = 1 \Leftrightarrow <v(a), v(b)> \in v(R) \Leftrightarrow <1,2> \in v(R) \Leftrightarrow 1 < 2$

Daher: $v(Rab) = 1$

(i.2) *Identitätsformeln:* $v(t_1 \equiv t_2) = 1$ gdw $v(t_1)=v(t_2)$ (sonst = 0)

(ii) *AL:* $v(\neg A) = 1$ gdw $v(A)=0$ (sonst 0)

$v(A \vee B) = 1$ gdw $v(A)=1$ or $v(B)=1$ (sonst = 0).

(iii) *Quantoren:* $v(\forall xA) = 1$ gdw für alle $d \in D$, $v[x:d](A) = 1$ (sonst = 0).

Beispiel:

$v(\forall x\, Fx) = 1 \Leftrightarrow \forall d \in D, v[x:d](Fx) = 1 \Leftrightarrow \forall d \in D, d \in v(F)$

Anm.: Dies impliziert: $v(\exists xA) = 1$ gdw es ein $d \in D$ gibt, sodass $v[x:d](A) = 1$.

Referentielle Semantik nach Tarski:

Es darf viel mehr Individuen in D geben, als Individuenkonstanten in $\mathcal{C}$. (Zuvor: ‚substitutionelle' Semantik nach Bolzano; Annahme: für jedes $d \in D$ einen Namen in $\mathcal{C}$ mit $v(n) = d$. Zu eng!!)

Sonderfall für $p \in \mathscr{P}$: $v(p)=1$ gdw $< > = \emptyset := 0 \in v(p)$ gdw $v(p) = \{0\} := 1$.

Wir schreiben <D,v> |== A gdw v(A) = 1 in D gilt.
Wenn <D,v> |== A , nennen wir die $\mathcal{L}$-Struktur <D,v> ein *Modell* für A; wir sagen in diesem Fall auch, dass <D,v> A erfüllt, oder verifiziert.
Wenn <D,v> |=/= A, d.h. <D,v> |== ¬A, dann wird <D,v> ein Gegenmodel für A genannt; und wir sagen, dass <D,v> A falsifiziert, oder widerlegt.
Logische Wahrheit (||— A), logische Falschheit, Gültigkeit von Schlüssen (Γ ||—A), Erfüllbarkeit von Formelmengen etc. *sind wie in der AL definiert*, basieren jedoch jetzt auf *Bewertungsfunktionen* für PL. – *Zu Beachten*: für Sätze hängen diese Eigenschaften alleine vom Interpretationsteil der Bewertung ab.

Anm.: Eine logisch wahre Formel der PL wird nicht länger Tautologie genannt, dieser Name ist für AL-Formeln oder PL-Instanzen selbiger reserviert.

In diesem Kapitel steht **L** = **L1** für alle gültigen Formeln der PL und ||— = $\vdash_{L1}$ für die korrespondierende Ableitungsrelation.

Theorem (Extensionalität von Formeln):
Wenn zwei Bewertungen v_1 und v_2 den selben Objektbereich haben und in allen Variablen, Konstanten, Relations- und Funktionssymbolen, die in A vorkommen, übereinstimmen, $v_1\!\upharpoonright\!(\mathcal{R}(A)\cup\mathcal{F}(A)\cup\mathcal{V}(A)\cup\mathcal{C}(A)) = v_2\!\upharpoonright\!(\mathcal{R}(A)\cup\mathcal{F}(A\cup\mathcal{V}(A)\cup\mathcal{C}(A))$, dann stimmen sie in A, $v_1(A) = v_2(A)$ überein.

Übungen: 5.5 Betrachten Sie eine Sprache $\mathcal{L}$ mit dem Funktionssymbol f(x), drei Prädikaten Fx, Gy, Rxy, und 5 Konstanten a,b,c,d,f. Betrachten Sie das $\mathcal{L}$-Modell <D, I> mit D = {1,2,3,4,5,6,7,8,9,10}, I(a)=1, I(b)=2, I(c)=3, I(d)=4, I(e)=5, I(f) = *f*:D→D sodass *f*(n) = 10–n; I(F) = {1,3,5}, I(G) = {6,8,10}, I(R) = $\{<n,m>\in D^2: n>m\}$.

Bestimmen Sie die Wahrheitswerte von: Fa, Ff(a), Ga∨Gfa, ∀x(Fx∨Gx), ∃x∃y(¬Rxy ∧ ¬Ryx), ∀x(Fx∨Ffx∨Gx∨Gfx), ∀x∃yRxy, ∀x(¬Gx→∃yRxy), ∃x∀y(Ryx∨y≡x), ∀x(¬x≡a → ∃yRyx), ∀x(¬x≡a → ∃yRxy), ∀x(x≡a → Fx), ∀x(x≡a → Ffx), ∀x(Fx∧Ff(f(x)) ↔ x = a ∨ x = c), ∀x(Fx → ¬Gf(x)), ∀x(Fx → ¬Ff(f(x))), ∀x(Fx → ∃y(Gfx), ∀x(Gx∧Gf(f(x)) ↔ x = f(d) ∨ x = f(b)), $\exists x_1,x_2,x_3,x_4(\bigwedge\{\neg x_i{=}x_j{:}1\leq i\neq j\leq 4\}\wedge Fx$, $\exists x_1,x_2,x_3(\bigwedge\{\neg x_i{=}x_j{:}1\leq i\neq j\leq 3\}\wedge Fx$, ∀x,y,z(z ≡ f(x) ∧ z ≡ f(y)) → x≡y).

Tipp: Einfache Bestimmung mittels „*Pseudoformeln“:*

v(Fa) = v(v(a) ∈ v(F)) = v(1 ∈ {1,3,5}) = wahr

v(Ga ∨ Gfa) = v(v(a) ∈ v(G) ∨ v(fa) ∈ v(G)) = v(1 ∈ {6,8,10} ∨ 9 ∈ {6,8,10}) = falsch ∨ falsch = falsch

v(∀x(Fx ∨ Gx)) = v(∀d ∈ {1,2,3,4,5,6,7,8,9,10}: F(d) ∨ G(d)) =

v(∀d ∈ {1,2,3,4,5,6,7,8,9,10}: d ∈ {1,3,5} ∨ ∈ {6,8,10}).

v(∀d∈{1,2,3,4,5,6,7,8,9,10} : d ∈ {1,3,5} ∨ d ∈ {6,8,10}) = wahr ⇔

∀d∈{1,2,3,4,5,6,7,8,9,10} : v(d ∈ {1,3,5} ∨ d ∈ {6,8,10}) = wahr ⇔

∀d∈{1,2,3,4,5,6,7,8,9,10} : d ∈ {1,3,5} ∨ d ∈ {6,8,10}.

Dies ist falsch, weil z.B. für d=2: nicht (d ∈ {1,3,5} ∨ d ∈ {6,8,10}).

Übung 5.6: Beweisen Sie das Theorem der Extensionalität durch Induktion übr die Komplexität von Formeln. Tipp: Fangen Sie mit der Festlegung für *Terme* an.

5.3 Substitutionen in PL und Fortsetzung Semantik:

Substitution von Termen für freie Variablen in offenen Formeln

Einleitung: Wir wollen, dass A[x/t] die Formel ist, die aus der korrekten Substitution des Terms t für alle freien Vorkommnisse von x in A ist, in der folgenden Weise:

Die Formel A[x/t] sollte dasselbe über t sagen, das A über x sagt.

Beispiel: Wenn $A = Fx \rightarrow Gyx$, dann $A[x/t] = Ft \rightarrow Gyt$.

In anderen Worten:

$\forall xA$ sollte A[x/t] logisch implizieren für alle $t \in \mathcal{T}$.

Gleichermaßen sollte A[x/t] $\exists xA$ implizieren.

Problem der Variablenkonsfusion: Wenn t eine Variable y enthält, die durch irgendeinen Quantor $\forall y$ oder $\exists y$ in A nach der Substitution gebunden ist, dann wird unsere semantische Intention für A[x/t] nicht länger gültig sein.

Beispiel für Variablenkonfusion:

Angenommen $D=\{1,2\}$, $v(F) = \{\langle 1,2\rangle,\langle 2,1\rangle\}$, $v(x)=1$.

Dann $v(\forall x\exists yFxy) = 1$ weil $\langle 1,2\rangle$ und $\langle 2,1\rangle \in v(F)$.

Ebenso $v(\exists yFxy) = 1$ weil $\langle 1,2\rangle \in v(F)$

Aber $(\exists yFxy)[x/y] = \exists yFyy$

Und $v(\exists yFyy) = 0$, da weder $\langle 1,1\rangle$ noch $\langle 2,2\rangle \in v(F)$.

Also $\exists yFyy$ (etwas F't sich selbst) ist keine korrekte Substitutionsinstanz von $\exists yFxy$ (etwas wird von x ge-F-t).

Definition – Substitution für freie Variablen:

Nicht-rekursive Definition:

(1) t ist frei für x (durch x substituiert zu werden) in einer Formel (oder einem Term) A gdw keine freien Vorkommnisse von x in A im Bereich eines Quantors liegen, welcher eine Variable in t bindet. (*Anm.:* wenn A ein Term ist, hat A keine Quantoren, und daher ist t immer frei).

(3) Vorausgesetzt t ist frei für x in A, dann bezeichnet (A)[x/t] das Resultat der simultanen Substitution von t für alle freien x-Vorkommnisse in A.

Andernfalls ist (A)[x/t] *prima facie undefiniert*.

Rekursive Definition:

(1) *Konstanten und Variablen:* Für $u \in \mathcal{V} \cup \mathcal{C}$: u[x/t] = t wenn u=x; sonst u[x/t] = u.

(2) *Komplexe Terme:* $(ft_1 \ldots t_n)[x/t] = f((t_1)[x/t] \ldots (t_n)[x/t])$.

(3) Für *atomare Formeln* ist A_{at}: t frei für jedes $x \in \mathcal{V}(A_{at})$, und $(Rt_1 \ldots t_n)[x/t] = R(t_1[x/t]) \ldots (t_n[x/t])$, und $(t_1 \equiv t_2)[x/t] = (t_1[x/t]) \equiv (t_2[x/t])$

(4) *Propositionale Operatoren:* (4.1) t ist frei für x in $\neg A$ wenn t frei ist für x in A, und $(\neg A)[x/t] = \neg(A[x/t])$; (4.2) t frei ist für x in $A \vee B$ wenn t frei ist für x in A und in B, und $(A \vee B)[x/t] = (A[x/t] \vee B[x/t])$

(5) *Quantoren:* t ist frei für x in $\forall zA$ wenn t nicht z enthält und t frei für x ist in A; und vorausgesetzt, dies ist der Fall, dann: wenn z = x, dann $(\forall zA)[x/t] = \forall zA$, und wenn $z \neq x$, $(\forall zA)[x/t] = \forall z(A[x/t])$; andernfalls ist $(\forall zA)[x/t]$ pima facie undefiniert.

Anm.: (A[x/t]) ist eine metasprachliche Notation. Die Klammer um t oder A wird benötigt, um Ambiguität zu vermeiden. Z.B. $(Fx \wedge Gx)[x/a] = Fa \wedge Ga \neq Fx \wedge (Gx[x/a]) = Fx \wedge Ga$.

In Fällen wo keine Ambiguität auftreten kann, können wir die Klammern um A weglassen. Wir erlauben auch Hilfsklammern, ((A)[x/t]), wenn sie die Lesbarkeit erhöhen.

Übung: 5.7 Führen Sie die Substitutionsoperationen [x/a], [x/f(y)], [x/g(z,a)] für die folgenden Formeln durch – welche Fälle sind prima facie definiert, was ist das Resultat? $\forall xFx$, $\forall xFx \rightarrow Gx$, $\forall y(Fx \wedge \exists xRxy)$, $\exists yFg(y, f(x))$, $\forall zRxz$.

5.8 Beweisen Sie durch Induktion: Wenn y frei ist für x in A, dann ist (a) x frei für y in A[x/y], und (b) (A[x/y])[y/x] = A, vorausgesetzt y ist nicht frei in A.

Das folgende Theorem zeigt, dass die Definition den intendierten Effekt hat, nämlich, dass "A[x/t] über t dasselbe sagt, was A über x sagt“:

Theorem – Koinzedenz von Substitution und Bewertungswechsel

Wenn t frei für x ist in A, dann: $v(A[x/t]) = v[x{:}v(t)](A)$

Beweis:

1. $v(u[x/t])$:= wenn $u = x$: $= v(t) = v[x{:}v(t)](u)$ da $u=x$

wenn $u \neq x$: $= v(u) = v[x{:}v(t)](u)$ da $u \neq x$.

2. $v((ft_1 \ldots t_n)[x/t]) = v(f(t_1)[x/t] \ldots (t_n)[x/t])$

$= v(f)(v(t_1[x/t]), \ldots ,v(t_n[x/t]))$

$= v[x{:}v(t)](f)(v[x{:}v(t)](t_1),\ldots,v[x{:}v(t)](t_n))$ nach IH und da $v[x{:}v(t)](f) = v(f)$

$= v[x{:}v(t)](ft_1 \ldots t_n)$.

3. $v((Rt_1 \ldots t_n)[x/t] = 1 \Leftrightarrow v(R(t_1)[x/t] \ldots (t_n)[x/t]) = 1 \Leftrightarrow$

$\Leftrightarrow (v(t_1[x/t]), \ldots ,v(t_n[x/t])) \in v(R)$

$\Leftrightarrow (v[x{:}v(t)](t_1),\ldots,v[x{:}v(t)](t_n)) \in v(R)$, da nach IH $v[x{:}v(t)](t_i) = v(t_i[x/t])$

und da $v[x{:}v(t)](R) = v(R) \quad \Leftrightarrow \quad v[x{:}v(t)](Rt_1 \ldots t_n)$.

4. $\rightarrow$ *Übung unten:* induktive Schritte für $A = \neg B$ und $A = B \vee C$.

5. Für $\forall zB$: Wir nehmen an, dass t frei für x ist in $\forall zB$, also $z \notin \mathcal{V}(t)$.

<u>Wenn x=z:</u> $v((\forall zB[x/t])) = v(\forall zB) = v[x{:}v(t)](\forall zB)$, weil x nicht frei ist in $\forall zB$ (und Extensionalitätstheorem).

Wenn <u>x≠z:</u> $v((\forall zB[x/t])) = 1 \Leftrightarrow v\big(\forall z(B[x/t]) \big) = 1 \Leftrightarrow \forall d \in D{:}\ v[z{:}d](B[x/t]) = 1$

$\Leftrightarrow \forall d \in D{:}\ v[z{:}d, x{:}\ v[z{:}d](t)](B) = 1$ nach IH

$\Leftrightarrow \forall d \in D{:}\ v[z{:}d, x{:}v(t)] (B) = 1$ weil $v[z{:}d](t) = v(t)$ da $z \notin \mathcal{V}(t)$

$\Leftrightarrow v[x{:}v(t)] (\forall zB) = 1$. Q.E.D.

Wir zeigen, dass unsere Definition von Substitution das gewünschte Resultat hat:

Theorem (UI): $\Vdash \forall xA \rightarrow A[x/t]$ (vorausgesetzt A[x/t] ist definiert.)

Beweis: Durch Kontraposition. Angenommen, es existiert <D,v>, sodass v(A[x/t]) = 0. Dann, nach Koinzidenzlemma, v[x:v(t)](A) = 0. Also gibt es $d \in D$, sodass v[x:*d*](A)=0. Also, v(∀xA) = 0. Q.E.D.

Übungen: 5.9 Beweisen Sie die Induktionsschritte für A = ¬B und A = B∨C im Koinzidenztheorem.

5.10 Beweisen Sie (EG): $\Vdash A[x/t] \rightarrow \exists xA$ mit dem UI-Theorem ("∃" ist *definiert* durch "∀").

Korrekte Umbenennung von gebundenen Varaiblen und alphabetische Varianten:

∀yA[x/y] ist sofern keine Konfusion passiert) eine (logisch äquivalente alphabetische Variante von ∀xA

z.B. ∀yFy ∀xFx

→ *nicht zu vergessen*, dass wir *Variablenkonfusion* verhindern müssen, die in zwei Fällen auftreten kann:

i) y ist nicht frei für x in A:

Beispiel: ∀x∀yRxy wird umbenannt in ∀y∀yRyy ↔ ∀yRyy: *eine andere Aussage!*

Im Kontrast dazu ist ∀z∀yRzy eine *korrekte* alphabetische Variante von ∀x∀yRxy.

ii) y hat freie Vorkommnisse in ∀xA:

Beispiel: ∀xRxy wird umbenannt in ∀yRyy: eine andere Aussage! ∀zRzy ist korrekt.

Definition (alphabetsiche Variante):
1. Wenn y nicht frei ist in A, aber y frei für x ist in A, dann ist $\forall yA[x/y]$ eine *unmittelbare alphabetische Variante* von $\forall xA$ – sie entsteht aus der korrekten Umbenennung gebundener Variablen in $\forall xA$.
2. A ist eine alphabetische Variante von B gdw A aus B durch eine endliche Anzahl unmittelbarer alphabetischer Varianten-Schritte entsteht, angewandt auf *Teilformeln* von B.

Übung *5.11*: *Beweisen Sie:* Wenn A' eine unmittelbare alphabetische Variante von A ist, dann ist A eine unmittelbare alphabetische Varainte von A' (benutzen Sie Übung 5.8!).

Anm.: "eine alphabetische Variante von" ist eine Äquivalenzrelation (siehe später).

Diese Definition von alphabetischen Varianten hat das gewünschte Resultat:
Theorem: Wenn A eine alphabetische Variante von B ist, dann $||\!\!-\, A \leftrightarrow B$.

Beweis: 1. Wenn A eine unmittelbare alphabetische Variante von B ist, dann hat B die Form $\forall xC$, also $A = \forall yC[x/y]$ wobei y frei ist für x in C aber nicht frei in C.
Nach Koinzidenzlemma, $v(C[x/y]) = v[x{:}v(y)](C)$ für alle v.
Daher: $v[y{:}d](C[x/y]) = v[y{:}d][x{:}v(y)](C) = v[x{:}d,y{:}d](C) =$
$= v[x{:}d](C)$, weil y nicht frei ist in C.
Also, $v(\forall yC[x/y]) = 1 \Leftrightarrow \forall d\in D\colon v[y{:}d](C[x/y])=1 \Leftrightarrow \forall d\in D\colon v[x{:}d](C)=1 \Leftrightarrow v(\forall xC)=1$.
2. Wenn A eine alphabetische Variante von C ist, dann folgt die Behauptung durch das *Theorem der Ersetzung von Äquivalenten* (Man erinnere sich an AL, Beweis für PL folgt später). QED.

Übung 5.12: Welche der folgenden Formeln sind alphabetische Varianten von welchen?
$\forall x(Fx \rightarrow \exists yRxy)$, $\forall z(Fz \rightarrow \exists xRzx)$, $\forall y(Fy \rightarrow \exists zRyz)$, $\forall u(Fu \rightarrow \exists vRvv)$,
$\forall y(Fy \rightarrow \exists yRyy)$, $\forall u(Fu \rightarrow \exists yRyx)$

Substitution für freie Variablen in prima facie undefinierten Fällen – erweiterte Definition:
Nicht-rekursive Definition:
Wenn t nicht frei ist für x in A, dann $A[x/t] := A^*[x/t]$ wobei A^* die erste alphabetische Variante von A ist, ensprechend der gegebenen Aufzählung von Variablen (voranschreitend von innen nach außen und links nach rechts), sodass t frei ist für x in A^*.
Beispiele: $(\exists x_2Rx_1x_2)[x_1/f(x_2)] := (\exists x_3Rx_1x_3)[x_1/f(x_2)] = \exists x_3Rf(x_2)x_3$.
$(\exists x_2 \exists x_3Rx_1)[x_1/f(x_2,x_3)] = (\exists x_5\exists x_4Rx_1)[x_1/f(x_2,x_3)] = \exists x_5\exists x_4Rf(x_2,x_3)$.
$(\forall x_2Fx_1x_2 \wedge \exists x_4Gx_3x_4))[x_1/x_2, x_3/f(x_4)] = (\forall x_5Fx_1x_5 \wedge \exists x_6Gx_3x_6))[x_1/x_2, x_3/f(x_4)]$
$= \forall x_5Fx_2x_5 \wedge \exists x_6Gf(x_4)x_6)$.
Rekursive Definition: Die "ist-frei-für"-Bedingung der alten Definition verschwindet, und *nur* Satz (5) wird verändert erweitert, wie folgt: wenn z = x, dann $(\forall zA)[x/t] = \forall zA$; wenn $z \neq x$ und t enthält nicht z, dann $(\forall zA)[x/t] = \forall z(A[x/t])$; und wenn $z\neq x$ und t nicht z enthält, dann $(\forall zA)[x/t] = \forall z^*((A[z/z^*])[x/t])$, wobei z^* die erste Variable ist, sodass (i) z^* nicht frei ist in A, (ii) z^* frei für z ist in A, und (iii) t nicht z^* enthält.

Anm.: Das Koinzidenztheorem lässt sich einfach zu der folgenden, erweiterten Definition erweitern.

Simultane Substitution für verschiedene Variablen – Definition:
Wenn t_i frei ist für x_i in A für $1 \leq i \leq n$, dann bezeichnet $A[x_1/t_1,\ldots,x_n/t_n]$ das Resultat der simultanen Substitution von t_i für x_i in A - d.h. die simultane Ersetzung aller freien x_i-Vorkommnisse durch t_i, für alle $1 \leq i \leq n$.

Unterschied zwischen simultaner und sukzessiver Substitution:
$(Fx \wedge Gy)[x/fy, y/fy] = Ffy \wedge Gfy$
$((Fx \wedge Gy)[x/fy])[y/fy] = Fffy \wedge Gfy$

Übung 5.13: Beweisen Sie das Koinzidenztheorem für den generalisierten Begriff der Substitutution. Zeigen Sie einfach, was neu/anders in diesem Beweis ist.
5.14 Geben Sie eine rekursive Definition für "simultane Substitution" in Analogie zu der obigen Definition; erklären Sie einfach was neu/anders in dieser Definition ist.

Substitution für Prädikate (Kleene):
Wie in der AL benutzen wir Axiom,- und Regelschemata in der PL.
Z.B., nicht nur $\forall xFx \rightarrow Fa$ ist semantsich gültig, sondern auch
$\forall xA \rightarrow A[x/t]$ ist semantisch gültig, für jede Formel A und jeden Term t.

Abschließende Bemerkung zu Substitution:
PL ist geschlossen, unter der folgenden *<u>Regel für Substitution von Prädikaten:</u>*
Wenn $\Vdash A$, dann ist, für jedes n-stellige Prädikat $Fz_1\ldots z_n$ in den 'Namens-Form Variablen' $z_1, \ldots, z_n$, und Formel (= komplexes Prädikat) B, auch $\Vdash A[F/B]$, wobei:
A[F/B] ist das Resultat der Ersetzung jedes Vorkommnises von $Ft_1\ldots t_n$ in A* durch $(B[z_1/t_1,\ldots,z_n/t_n])$, wobei A* die erste alphabetische Variante von A ist, sodass keine *anonyme* Variable von B (= keine freie Variable von B, welche keine Namens-Form Variable ist) in A*[F/B] gebunden wird.

Theorem (AL ist in PL enthalten): ($\mathcal{L}1$ PL $\mathcal{L}0$ AL)

Ein Schluss Γ |— A ist PL-gültig, wenn er eine Substitututionsinstanz eines gültigen AL-Schlusses ist. Wir nennen solch einen Schluss *propositional* oder *tautologsich* gültig. (Gleiches für Formeln.)

Formal: $\Gamma \Vdash_0 A \Rightarrow s(\Gamma) \Vdash_1 s(A)$, wobei s: $\mathcal{P} \rightarrow \mathcal{L}1$.

Beiweis: Es sei v1 eine $\mathcal{L}_1$-Bewertung. Wir definieren die korrespondierende v0-Bewertung zu $\mathcal{P}$ durch: v0(p) = v1(s(p)).

Koinzidenzlemma für AL-PL: Für alle $A \in \mathcal{L}_0$: v0(A) = v1(s(A)).

Beweis: Übung.

Also: per Kontraposition: Wenn es ein v1 gäbe, welches $s(\Gamma) \Vdash_1 s(A)$ widerlegen würde, dann würde das gemäss Koinzidenzlemma definierte v0 aufgrund Koinzidenzlemma $\Gamma \Vdash_0 A$ widerlegen (v0 |== Γ aber v0(A)=0). QED.

Notation: (1) Eine PL-Formel wird *elementar* genannt, wenn sie nicht propositional zusammengesetzt ist. (2) Die *propositionale Form* einer PL-Formel A ist diejenige AL-Formel A_0 welche aus A durch Ersetzung der Teilformeln von A durch Aussagevariablen entsteht. (Gleiches für Schlüsse.)

Übungen:

5.14: Beweisen Sie das obige Koinzidenzlemma für AL-PL.

5.15: Was ist die propositionale Form der folgenden Formeln und/oder Schlüsse: (a) $\forall x(Fx \wedge \neg Gx) \rightarrow (\exists xFx \wedge Qy)$, (b) $Fa \rightarrow \exists z(\forall xRxz \wedge \forall y(Fy \vee Gyz))$, (c) $\neg(\neg Fa \wedge Ga)$ / $(Fa \vee \neg Ga)$, (d) $(Fa \rightarrow \neg \exists xGx) \rightarrow (\forall xRx \wedge \exists x(Fx \vee \neg Gx))$, (e) $(\forall xFx \wedge \forall xGx) \rightarrow \forall xFx$, (f) $\forall x(Fx \wedge Gx) \rightarrow \forall xFx$, (g) $\neg(\forall x \exists yFxy \wedge \neg \forall x \exists yFxy)$.

5.16: Welche der folgenden Theoreme von Schlüssen der PL sind propositional gültig? Wenn sie es sind, was ist ihre propositionale Form?

$(\forall xFx \wedge \forall xGx) \Vdash\!\!-\!\!- \forall xFx$, $\forall x(Fx \wedge Gx) \Vdash\!\!-\!\!- \forall xFx$,

$\forall xFx$, $\forall xFx \rightarrow (\exists xGx \wedge Hx)$, $\neg\exists xGx \vee Qa \Vdash\!\!-\!\!- Qa$

$\forall xFx$, $\forall xFx \rightarrow (\exists xGx \wedge Hb)$, $\neg\exists xGx \vee Ha \Vdash\!\!-\!\!- Ha \vee Hb$.

6. Deduktive Kalküle für die PL

Kalkül S*≠ für PL: (S* Abkürzung für S*1; S*0 für AL S*).

Sequenzen Präsentation — Satz Präsentation

AL-Regeln:

Jedes Axiom und jede Regel von S*0

In Addition – als eine 'Abkürzung von PL-Beweisen':

(Taut): $\Gamma_1 \vdash A_1, \ldots, \Gamma_n \vdash A_n \,/\, \bigcup\{\Gamma_i{:}1\leq i\leq n\} \vdash B$

wenn $A_1,\ldots,A_n \vdash B$ tautologisch gültig ist

	⋮
i_1	A_1
	⋮
i_n	A_n
	B Taut $i_1,\ldots,i_n$

Unkritische Quantor-Regeln:

Universelle Instantiierung - ∀-Beseitigung:

UI: $\Gamma \vdash \forall xA \,/\, \Gamma \vdash A[x/t]$ (für jedes $x\in\mathcal{V}$, $t\in\mathcal{T}$)

⋮
$\forall xA$
$A[x/t]$
⋮

Beispiel von Instanzen:

$\Gamma \vdash \forall x\forall yRxy \,/\, \Gamma \vdash \forall yRay$ x->x, t->a, A->∀yRxy, A[x/t]->∀yRay

$\Gamma \vdash \forall yRay \,/\, \Gamma \vdash Rab$ x->y, t->b, A-> Ray, A[x/t] -> Rab

Durch Reit und KB kriegen wir die Version 1. Stufe $\forall xA \vdash A[x/t]$) und das Theorem $\vdash \forall xA \rightarrow A[x/t]$

Existentielle Generalisierung - ∃-Einführung:

EG: $\Gamma \vdash A[x/t] \,/\, \Gamma \vdash \exists xA$ (für jedes $x\in\mathcal{V}$, $t\in\mathcal{T}$)

1. Stufe: $A[x/t] \vdash \exists xA$; Theorem $\vdash A[x/t] \rightarrow \exists x$

⋮
$A[x/t]$
$\exists xA$
⋮

Übungen:

6.1.Was ist die Instanziierungsfunktion für $Rab \vdash \exists xRxb$, $\exists xRxb \vdash \exists y\exists xRxy$

6.2. *Leiten Sie das Definiens von EG ab:* $\Gamma \vdash A[x/t] \,/\, \Gamma \vdash \neg\forall x\neg A$

(In anderen Worten, zeigen Sie, dass EG aus UI folgt, per Defininiton von ∃)

Kritsiche Quantor-Regeln: (haben Restriktionen *R*)

Universelle Generalisierung - $\forall$-Einführung:

(UG): $\Gamma \vdash A[x/a]$ / $\Gamma \vdash \forall xA$ (für jedes $x \in \mathcal{V}$, $a \in \mathcal{C}$)

R: a kommt nicht in Γ oder A vor!

A[x/a]

$\forall xA$ *R:* a nicht in A, oder einer Prämisse, oder offenen Annahme

Beispiele von Instanzen:

$\Gamma \vdash Rac$ / $\Gamma \vdash \forall xRxc$ Instanz: x->x, a->a, A->Rxc, A[x/a]->Rac

$\Gamma \vdash \forall xRxc$ / $\Gamma \vdash \forall y \forall xRxy$ Instanz: x->y, a->c, A->$\forall$xRxy, A[x/a]->$\forall$xRxc

Intuition: Wenn wir A[a] für irgendeine Konstante a beweisen können, ohne irgendetwas darüber anzunehmen, dann können wir dieselbe Behauptung für alles beweisen.

Wir können auch über Variablen generalisieren (s.u.) aber wir *dürfen nicht* über Terme mit Funktionssymbolen generalisieren.

$\rightarrow$ *Gegenbeispiel 1:* A = Fx, t=f(a).

$\forall x(Fx \rightarrow Ff(x)), Fa \vdash Ff(a)$ – der Term f(a) taucht nicht in der Prämissenmenge auf.

Aber $\forall x(Fx \rightarrow Ffx), Fa \not\vdash \forall xFx$!

Anm.: a *darf nicht* in A vorkommen: A resultiert aus A[x/a] durch Ersetzung von jedem a durch x!

(In Logik I schrieben wir A[a] und A[x], und mussten ebenfalls fordern: a nicht in A[x].) $\rightarrow$ *Gegenbeispiel:* Sei A = Fa$\rightarrow$Fx, A[x/a] = Fa$\rightarrow$Fa.

$\varnothing \vdash Fa \rightarrow Fa$ aber $\varnothing \not\vdash \forall x(Fa \rightarrow Fx) \dashv\vdash Fa \rightarrow \forall xFx$ (s. u.).

∃-Einführung in der Prämisse:

Auch genannt: Existentielle Instantiierung - ∃-Beseitigung:

(EI): Γ, A[x/a] $\vdash$ B / Γ, $\exists$xA $\vdash$ B (für alle x$\in\mathcal{V}$, a$\in\mathcal{C}$)

vorausgesetzt, a taucht nicht in Γ oder B oder A auf

$\exists$xA

A[x/a]

B

B *R* wie oben

Übung: 6.3 Warum können wir A[x/a] $\vdash$ $\forall$xA nicht mit (UG) beweisen?

6.3 a) Beweisen Sie das Definiens von EI durch UG.

6.4 Beweisen Sie, dass UG – im Kontext der AL-Regeln – äquivalent mit seiner KB-Version (oder 'Hilbert-Style Version): $\vdash$ B $\rightarrow$ A[x/a] / $\vdash$ B $\rightarrow$ $\forall$xB, ist, vorausgesetzt, a ist nicht in A, B.

6.5 Beweisen Sie, dass EI äquivalent ist, mit: $\vdash$ A[x,a]$\rightarrow$B / $\exists$xA $\rightarrow$ B, vorausgesetzt, a ist nicht in A, B.

Theorem: UG kann äquivalent ersetzt werden durch:

(UGv): Γ $\vdash$ A / Γ $\vdash$ $\forall$xA vorausgesetzt, x ist nicht frei in Γ

(Gleichermaßen, EI durch EIv: Γ, A $\vdash$ B / Γ, $\exists$xA $\vdash$ B; vorausgesetzt, x ist nicht frei in Γ, B)

Anm.: der Beweis von UG a$\Leftrightarrow$ UGv ist aufwendig, aber notwendig, weil beide Regeln in verschiedenen Systemen benutzt werden. Der einfachere Weg wäre es, UG durch die folgende, generellere Regel zu ersetzen: (UGg:) Γ $\vdash$ A[x/t] / Γ $\vdash$ $\forall$xA vorausgesetzt, t$\in\mathcal{C}\cup\mathcal{V}$ ist nicht frei in Γ, A (kann t eine Variable *oder* Konstante sein!; Und Gleiches gilt für EIg).

Beweis: In beide Richtungen, *nach Induktion auf die Länge des Beweises.*

(UGv) $\Rightarrow$ (UG):

Angenommen <Γ_1 $\vdash$ A_1,…,Γ_n $\vdash$ A_n> ist ein Beweis von Γ $\vdash$ A[x/a], sodass a nicht in Γ oder A vorkommt.

Wir ersetzen in jeder Sequenz die Variable (Individuenkonstante) a durch eine Variable y welche nirgendwo anders in diesem Beweis auftaucht. Wir zeigen, dass die modifizierte Sequenz immer noch ein Beweis ist (denn dann können wir darauf UGv) anwenden). Wir versehen die modifizierten Formeln mit Sternchen. Also $\Gamma_i^*[y/a] = \Gamma_i$. Wir zeigen, dass

i) wenn $\Gamma_i^*[y/a] \vdash A_i^*[y/a]$ ein Axiom ist, dann ist es auch $\Gamma_i^* \vdash A_i^*$.

ii) wenn $\Gamma_i^*[y/a] \vdash A_i^*[y/a]$ aus $\Gamma_k^*[y/a] \vdash A_k^*[y/a]$, $\Gamma_j^*[y/a] \vdash A_j^*[y/a]$ (k,j<i) nach einer der Regeln folgt, dann folgt $\Gamma_i^* \vdash A_i^*$ aus $\Gamma_k^* \vdash A_k^*$, $\Gamma_j^* \vdash A_j^*$ nach der selben Regel.

→ i) gilt, da unser einziges Axiom Reit ist.

→ ii) gilt für alle aussagenlogischen Regeln, weil die propositionale Form eines Schlusses nach Substitution einer Konstante durch eine Variable unverändert bleibt.

→ ii) gilt für UI: wenn $\Gamma_i^*[y/a] \vdash (\forall x A_i^*)[y/a]$ / $\Gamma_i^*[y/a] \vdash (A_i^*[y/a])[x/b]$ eine UI-Instanz ist, dann ist auch $\Gamma_i^* \vdash \forall x A_i^*$ / $\Gamma_i^* \vdash A_i^*[x/b]$ eine UI-Instanz.

→ ii) gilt für UGv-Schritte: wenn $\Gamma_i^*[y/a] \vdash A_i^*[y/a]$ / $\Gamma_i^* \vdash \forall x A_i^*[y/a]$ eine UGv-Instanz ist, dann ist auch $\Gamma_i^* \vdash A_i^*$ / $\Gamma_i^* \vdash \forall x A_i^*$ eine UGv-Instanz.

Also ist die modifizierte Sequenz von Sequenzen $<\Gamma_1^* \vdash A_1^*,\ldots,\Gamma_n^* \vdash A_n^*>$ein Beweis von $\Gamma \vdash A[x/y]$, denn: a ist nicht in Γ, also $\Gamma = \Gamma_n = \Gamma_n^*$; und a ist nicht in A, also ist, nach der 'a-durch-y'-Ersetzung in A[x/a] gleich A[x/y]. Daraus gewinnen wir $\Gamma \vdash \forall y A[x/y]$ nach vUG, und daraus $\Gamma \vdash A[x/y, y/y]$ =A nach UI, und daraus wiederum $\Gamma \vdash \forall x A$ nach vUG .

(UG) ⇒ (UGv):

Angenommen $<\Gamma_1 \vdash A_1,\ldots,\Gamma_n \vdash A_n>$ ist ein Beweis von $\Gamma \vdash A$ mit x nicht frei in Γ. *Wir ersetzen uniform alle Vorkommnisse der Variable x in der Ableitung durch eine Konstante a welche nicht in* Γ vorkommt. Wir zeigen, dass die modifizierte Sequenz $<\Gamma_1^* \vdash A_1^*,\ldots,\Gamma_n^* \vdash A_n^*>$ erneut ein Beweis von $\Gamma \vdash A[x/a]$ ist (denn dann können wir UG anwenden).

Wie oben wird ein Axiom zu einem modifizierten Axiom und eine aussagenlogische Regel zu einer modifizierten aussagenlogischen Regel.

Wenn $\Gamma_i \vdash \forall zA$ / $\Gamma_i \vdash A[z/b]$ eine Instanz von UI ist, wird auch die Modifikation eine Instanz von UI sein, weil entweder $z \neq x$ wodurch nichts durch die Anwendung von [x/a] passieren kann, oder z=x, wodurch $\forall zA^* = \forall zA$ und $(A[z/b])^* = A[z/b]$.
Wenn $\Gamma_i \vdash A[z/b]$ / $\Gamma_i \vdash \forall zA_i$ (wobei b nicht in Γ_i) eine Instanz von UG ist, dann wieder entweder $b \neq a$, oder b=a wodurch a nicht in Γ_i ist. Durch Anwendung eines UG-Schrittes erhalten wir $\Gamma \vdash \forall xA$, denn $\Gamma^* = \Gamma$ hat kein freies x.
Q.E.D.

Theorem (Lemma zu neuen Konstanten): $\Gamma[x/a] \vdash A[x/a] \Rightarrow \Gamma \vdash A$ wenn $a \notin \mathcal{C}(\Gamma,A)$

Übung 6.6: Beweisen Sie das Theorem. Beweisen Sie auch die andere Richtung, trivial nach UI.

Übung 6.7: Beweisen Sie einige der folgenden Theoreme und Formeln (nach Wahl).

****

Wichtige Äquivalenztheoreme der PL:
(ebenfalls sehr wichtig für logische Äquivalenzumformung in Normalformen):
(AV): $A \leftrightarrow B$ Wenn B eine alphabetische Variante von A ist
(Def∃): $\forall xA[x] \leftrightarrow \neg\exists x\neg A[x]$
$\exists xA[x] \leftrightarrow \neg\forall x\neg A[x]$

(RDist) Vorausgesetzt x ist nicht frei in A: beschränkte Distribution

$A \vee \forall xB \leftrightarrow \forall x(A \vee B)$	$(A \to \forall xB) \leftrightarrow \forall x(A \to B)$
$A \wedge \forall xB \leftrightarrow \forall x(A \wedge B)$	$(\forall xB \to A) \leftrightarrow \exists x(B \to A)$
$A \wedge \exists xB \leftrightarrow \exists x(A \wedge B)$	$(A \to \exists xB) \leftrightarrow \exists x(A \to B)$
$A \vee \exists xB \leftrightarrow \exists x(A \vee B)$	$(\exists xB \to A \leftrightarrow (\forall xB \to A)$

(UDist) $\forall x(A \wedge B) \leftrightarrow \forall xA \wedge \forall xB$ unbeschränkte

$\exists x(A \vee B) \leftrightarrow \exists xA \vee \exists xB$ Distribution

(Zur Erinnerung: wir haben Distr. für $\forall$-$\vee$ und für $\exists$-$\wedge$ *widerlegt*.)

(QE) Austausch der Quantoren

$\exists x\exists yA \leftrightarrow \exists y\exists xA$ $\forall x\forall yA \leftrightarrow \forall y\forall xA$

Einseitige Implikationen:

$\forall xA \vee \forall xB \rightarrow \forall x(A \vee B)$ $\forall x(A \rightarrow B) \rightarrow (\forall xA \rightarrow \forall xB)$

$\exists x(A \wedge B) \rightarrow \exists xA \wedge \exists xB$ $\exists x\forall yA \rightarrow \forall y\exists xA$

**************************Ende-der-Liste**************************

Zusätliche Regeln und Axiome für ***S****$^{=}$ *(S** mit Identität):

$t=t$

Identität - ≡-Einführung:

(Id): $\Gamma \vdash t\equiv t$ für jedes $t\in\mathfrak{T}$

(*Anm:* Id ist äquivalent mit $\Gamma \vdash \forall x(x=x)$.)

Extensionaliät (Substitution von Identischem, Gleichheit) - ≡-Beseitigung:

(Ext≡): $\Gamma \vdash t_1\equiv t_2$ / $\Gamma \vdash A[x/t_1] \rightarrow A[x/t_2]$ für alle $x\in\mathfrak{V}$, $t_i\in\mathfrak{T}$

$t_1\equiv t_2$

$A[x/t_1]\rightarrow A[x/t_2]$

Einige Instanzen von (Ext):

$\Gamma \vdash a\equiv b$ / $\Gamma \vdash \forall xRxa \rightarrow \forall xRxb$

wir wählen x -> y, A->$\forall$xRxy, t_1->a, t_2->b, also $A[x/t_1]$->$\forall$xRxa, $A[x/t_2]$ -> $\forall$xRxb

Wichtige abgeleitete Identitätstheoreme und -regeln:

1. *Symmetrie:* $\Gamma \vdash t_1\equiv t_2$ / $\Gamma \vdash t_2\equiv t_1$

Beweis:

1. $\Gamma \vdash t_1\equiv t_2$	Präm
2. $\Gamma \vdash t_1\equiv t_1 \rightarrow t_2\equiv t_1$	Ext aus 1, es sei A -> ($x\equiv t_1$)
3. $\Gamma \vdash t_1\equiv t_1$	Id
4. $\Gamma \vdash t_2\equiv t_1$	MP 2,3

2. *Transitivität:* $\Gamma \vdash t_1\equiv t_2$, $\Gamma\vdash t_2\equiv t_3$ / $\Gamma \vdash t_1\equiv t_3$. *Beweis: Übung unten*

3. (Ext↔): $\vdash \bigwedge\{ t_i\equiv t_i' : 1\le i\le n\} \rightarrow (A[x_1/t_1,\ldots,x_n/t_n] \leftrightarrow A[x_1/t_1',\ldots,x_n/t_n'])$

Beweis: $\rightarrow$ *Richtung von* $\leftrightarrow$*:* zuerst ersetzen wir die Variablen $x_1,\ldots,x_n$ in A durch neue Variablen $z_1,\ldots,z_n$ die nicht in A, oder in $t_1, \ldots, t_n$ vorkommen, und erhalten A*. Dann führen wir die sukzessive Substitution zu A*: $A^*[z_1/t_1]$, $A^*[z_1/t_1][z_2/t_2]$, …, $A^*[z_1/t_n]\ldots[z_n/t_n]$ durch. Jede dieser Formeln wird logisch impliziert, durch $\bigwedge\{ t_i \equiv t_i' : 1 \leq i \leq n\}$ via (Ext) und AL. $A^*[z_1/t_n]\ldots[z_n/t_n]$ ist identisch mit A.

$\leftarrow$Richtung von $\leftrightarrow$: folgt aus der Symmetrie von $\equiv$ und AL. QED.

Übungen:

6.8: Zeigen Sie, dass der obige Beweis von UG $\Leftrightarrow$ vUG auch funktioniert, wenn die Identitätsaxiome hinzugefügt werden.

6.9: Beweisen Sie die *Transitivität* von $\equiv$.

6.10: Beweisen Sie:

a) $\exists x(x \equiv t)$

b) $\vdash Ft \leftrightarrow \exists x(Fx \wedge x \equiv t)$

c) $\vdash Ft \leftrightarrow \forall x(x \equiv t \rightarrow Fx)$

} diskutieren Sie die Bedeutung für Ontologie und Wissenschaftstheorie

Anm.: Ein Satz wird *essentiell* quantifiziert genannt gdw er quantifiziert ist und nicht L-äquivalent mit einem singulären Satz. (Gleiches gilt für "essentiell universell" und "essentiell existentiell").

<u>*Ausdrücken von Zahlen, Teil von Frege's Programm:*</u>

$\exists_n x := \exists x_1 \ldots \exists x_n \bigwedge\{\neg x_i \equiv x_j : 1 \leq i < j \leq n\}$ D hat mindestens n Elemente

$\exists_n x Fx := \exists x_1 \ldots \exists x_n(\bigwedge\{Fx_i : 1 \leq i \leq n\} \wedge \bigwedge\{\neg(x_i \equiv x_j) : 1 \leq i < j \leq n\}$

v(F) hat mindestens n Elemente

$\exists^n x := \forall x_1 \ldots \forall x_{n+1}(\bigwedge\{\neg(x_i \equiv x_j) : 1 \leq i < j \leq n\} \rightarrow \bigvee\{x_i \equiv x_{n+1} | : 1 \leq i \leq n\})$

D hat höchstens n Eemente

$\exists^n x Fx :=$

$\forall x_1 \ldots \forall x_{n+1}(\bigwedge\{Fx_i : 1 \leq i \leq n+1\} \wedge \bigwedge\{\neg(x_i \equiv x_j) : 1 \leq i < j \leq n\} \rightarrow \bigvee\{x_i \equiv x_{n+1} | : 1 \leq i \leq n\})$

v(F) hat höchstens n Elemente

$\exists ! n x =_{df} \exists_n x \wedge \exists^n x$ D hat genau n Elemente

$\exists!nxFx =_{df} \exists_n xFx \wedge \exists^n xFx$ v(F) hat genau n Elemente

Übung 6.11: Beweisen Sie:

a) $\exists!nx \leftrightarrow \exists x_1 \ldots \exists x_n \forall y(\bigwedge\{\neg(x_i \equiv x_j) : 1\leq i<j\leq n\} \wedge \bigvee\{x_i \equiv y \mid 1\leq i\leq n\})$

b) $\exists!nxFx \leftrightarrow \exists x_1 \ldots \exists x_n \forall y(\bigwedge\{Fx_i \wedge \neg(x_i \equiv x_j) : 1\leq i<j\leq n\} \wedge (Fy \rightarrow \bigvee\{x_i \equiv y \mid 1\leq i\leq n\})$

c) $\exists!nxFx \leftrightarrow \exists x_1 \ldots \exists x_n(\bigwedge\{Fx_i \wedge \neg(x_i \equiv x_j) : 1\leq i<j\leq n\} \wedge \forall y(Fy \leftrightarrow \bigvee\{x_i \equiv y \mid 1\leq i\leq n\}))$

Definition: $\exists!xFx := \exists!1xFx$.

Nach b), $\exists!xFx \leftrightarrow \exists x \forall y(Fx \wedge (Fy \rightarrow x\equiv y))$

Und nach c), $\exists!xFx \leftrightarrow \exists x \forall y(Fy \leftrightarrow x\equiv y)$. Russell's Definition

Russell's Beseitigungsmethode fürEigennamen durch definite Beschreibung :

Für jeden Namen "a" nimmt Russell eine *definite Beschreibung* $D_a x$ an.

Definition von Namen: a := $\urcorner x D_a x$, vorausgesetzt $\exists!xD_a x$ ($\urcorner$ dasjenige x, welches...)

$Ga = G(\urcorner(D_a x)) := \exists x(Gx \wedge \forall y(D_a y \leftrightarrow x\equiv y)) \leftrightarrow \exists x(Gx \wedge D_a x) \wedge \exists!yD_a y$

Übung 6.12: Diskutieren Sie die resultierende Ambiguität von "$\neg$Ga" – was sind die zwei möglichen Lesarten in Russell's Theorie der Namen? (vs. Strawson: Wahrheitswertlücken)

Frege's Idee der Reduktion von Arithmetik zu Logik:

Übung 6.13: Beweisen Sie:

a) $\forall x(Fx \leftrightarrow \neg Gx) \wedge \exists_n x\, Fx \wedge \exists_m xGx \rightarrow \exists_{(n+m)} x(Fx \vee Gx)$

b) $\exists^n x\, Fx \wedge \exists^n xGx \rightarrow \exists^{(n+m)} x(Fx \vee Gx)$

c) $\forall x(Fx \leftrightarrow \neg Gx) \wedge \exists n!xFx \wedge \exists!mxGx \rightarrow \exists!(n+m)x(Fx \vee Gx)$.

$\rightarrow$ Dies deckt jedenfalls nur den finiten Teil der Arithmetik ab. Wir können nicht über „alle“ natürlichen Zahlen in dieser Weise sprechen.

Korrektheit von S*1*:*

Diese wird gezeigt wie in der AL: wir zeigen, dass alle Sequenzaxiome gültig sind und alle Sequenzregeln Wahrheit erhalten, oder zumindest Gültigkeit von Sequenzen. Gültigkeitserhaltung von Taut, und Gültigkeit von Id ist offensichtlich.

Für UI haben wir Wahrheitserhaltung im Kapitel über Semantik gezeigt; EG folgt aus UI.

Gültigkeitserhaltung von UG:

Angenommen $\Gamma \Vdash$A[x/a] mit a $\notin \mathcal{C}(\Gamma$,A) und (per reductio ad absurdum) wird angenommen, dass für irgendein <D,v>, v |== Γ und v($\forall$xA) = 0. Also für irgendein *d*$\in$D, v[x:*d*](A)=0.

Wir verwenden die Bewertungsfunktion v* := v[a:*d*].

v*(A[x/a]) = v*[x:*d*](A) nach Koinzidenztheorem, da v*(a)=*d*.

v*[x:*d*](A) := v[a:*d*, x:*d*](A) = v[x:*d*](A) nach Extensionalität, da a $\notin \mathcal{C}$ (A).

Also v*(A[x/a]) = 0, da nach Ann. v[x:*d*](A) = 0. Aber v* |== Γ, da a $\notin \mathcal{C}$ (Γ). Dies widerspricht unserer Annahm $\Gamma \Vdash$ A[x/a]. Q.E.D.

Übung 6.14: Beweisen Sie die Gültigkeitserhaltung für irgendeine Regel (Ext≡) (Induktion auf die Komplexität).

7.Weitere Metatheoreme und Anwendungen der Prädikatenlgik 1. Ordnung

7.1 Äquivalenzumformungen und Normalformen

Theorem (Ersetzung von Äquivalenten): Wenn C $\dashv\Vert\ \Vert\!\vdash$B, dann A $\dashv\Vert\ \Vert\!\vdash$ A[B/C]

Beweis: Wie in AL. Es gibt nur einen neuen Beweisschritt für quantifizierte Formeln. Wir müssen zeigen:
Wenn $\Vert\!\vdash B \leftrightarrow C$, dann $\forall xA \leftrightarrow \forall xA[B/C]$
Nach IH haben wir: wenn $\Vert\!\vdash B \leftrightarrow C$, dann $A \leftrightarrow A[B/C]$.
Wir zeigen: $\vdash A \leftrightarrow A[B/C] \Rightarrow \vdash (\forall xA \leftrightarrow \forall xA[B/C])$
Nach UGv, $\vdash A \leftrightarrow A[B/C] \Rightarrow \vdash \forall x(A \leftrightarrow A[B/C])$.
Wir wenden das Theorem $\forall x(A \to B) \vdash \forall xA \to \forall xB$ in beide Richtungen an, und erhalten daraus, plus AL $\vdash (\forall xA \leftrightarrow \forall xA[B/C])$. QED.

Definition (*pränexe Normalform*):

Eine pränexe DNF (pränexe KNF) ist eine Formel von $\mathcal{L}1$, die eine Zeichenreihe von Quantoren enthält, gefolgt von einer quantorenfreien DNF (oder KNF, respektive).

Schematische Struktur: $\substack{\forall\\ \exists} x_1 \ldots \substack{\forall\\ \exists} x_n \ ((Fx_1 \wedge \neg Rx_1x_2) \vee (Gx_1x_3 \wedge \neg Fx_2) \vee \ldots)$

Gleiches für PKNF (pränexe NF *:* $\substack{\forall\\ \exists} x_1 \ldots \substack{\forall\\ \exists} x_n\, A$ – quantorenfrei)

Beispiel von **E1**-Umformung (**E1** = Äquivalenzkalkül der PL):

$\exists x(\exists yRxy \rightarrow ((\exists z(Qxz \rightarrow \forall tFxat) \vee \exists zGxz))$

|--- Def$\rightarrow$

$\exists x(\neg\exists yRxy \vee (\exists z(Qxz \rightarrow \forall tFxat) \vee \exists zGxz))$

|--- Def$\rightarrow$

$\exists x(\neg\exists yRxy \vee (\exists z(\neg Qxz \vee \forall tFxat) \vee \exists zGxz))$

|--- Def $\exists$, DN

$\exists x(\forall y\neg Rxy \vee (\exists z(\neg Qxz \vee \forall tFxat) \vee \exists zGxz))$

|--- UDist $\exists$

$\exists x(\forall y\neg Rxy \vee \exists z((\neg Qxz \vee \forall tFxat) \vee Gxz))$

|--- Ass $\vee$

$\exists x(\forall y\neg Rxy \vee \exists z(\neg Qxz \vee \forall tFxat \vee Gxz))$

|--- RDist$\forall$

$\exists x\forall y(\neg Rxy \vee \exists z(\neg Qxz \vee \forall tFxat \vee Gxz))$

|--- RDist$\exists$

$\exists x\forall y\exists z(\neg Rxy \vee (\neg Qxz \vee \forall tFxat \vee Gxz))$

|--- Ass $\vee$

$\exists x\forall y\exists z(\neg Rxy \vee \neg Qxz \vee \forall tFxat \vee Gxz)$

|---RDist$\forall$

$\exists x\exists y\exists z\forall t(\neg Rxy \vee \neg Qxz \vee Fxat \vee Gxz)$ (eine PDNF und PKNF)

Hinweis: hätte $\exists x(\exists yRxy \rightarrow ((\exists z(Qxz \rightarrow \forall yFxay) \vee \exists zGxz))$ dagestanden, hätten wir zu erst „$\forall yFxay$“ gebunden in „$\forall tFxat$“ umbenennen müssen.

Übungen: 7.1 Beweisen Sie Rdist

7.2 Formen Sie die folgenden Formeln in eine PDNF, oder PKNF um:

(1) $\neg\forall x(Fx \rightarrow(\exists yRxy \wedge \neg \forall zQxaz))$

(2) $\exists x((\forall yRxy \vee \neg\exists z\neg Qxz) \rightarrow \neg(\exists z(Rxz \vee Fz))$

(3) $\neg\exists x((\neg\exists yTxya \vee \forall zSxz) \rightarrow (\exists y\neg Txy \wedge \neg\neg\neg Rxxx))$

(4) $\exists x\forall y(Fxy \rightarrow Gxy) \wedge \exists x\forall y(Hxy \rightarrow Gxy)$

(5) $\forall x\exists y(\neg Rxy \vee \neg\forall z(Qyz \rightarrow Szx))$

(6) $\exists x(\forall y(Fxy \rightarrow Gxy) \wedge \forall z(Hxz \vee \neg Gxz))$

Im Foglenden ist Qx die Abkürzung für $\forall x$ oder $\exists x$, und Q*x ist das duale Qx (d.h. $\forall^*x = \exists x$, und $\exists^*x = \forall x$). Gleichermaßen kürzt **Qx** eine Zeichereihe $Q_1x_1\ldots Q_nx_n$ von Quantoren ab; und **Q*x** die Zeichenreihe von dualen Quantoren.

Theorem: Jede Formel A ist PL-äquivalent mit einer PNF(A).

Beweis: Durch Induktion auf die Komplexität von A. Wir nehmen $\rightarrow$ als eliminiert an.

1) A atomar: offensichtlich.

2) $A = \neg B$: Angenommen $B \dashv\vdash \mathbf{Qx}C$ in PNF nach IH. Dann $A \dashv\vdash \mathbf{Q^*x}\neg C$.

3) $A = B\mathbf{o}C$. wobei $\mathbf{o} \in \{\wedge,\vee\}$. Angenommen $B \dashv\vdash \mathbf{Q_1x}B^*$ in PNF, und $C \dashv\vdash \mathbf{Q_2y}C^*$ in PNF, nach IH.

Dann benennen wir zuerst die gebundenen Variablen in $\mathbf{Q_1x}B^*$ und $\mathbf{Q_2y}C^*$ neu, sodass sie disjunkt werden, und kommen bei $\mathbf{Q_1^*x}B^*$ und $\mathbf{Q_2^*y}C^*$ an. Jetzt wenden wir sukzessive Rdist an, erhalten z.B. $\mathbf{Q_1^*x}\ \mathbf{Q_2^*y}(B^*\mathbf{o}C^*)$, oder irgendeine Permutation der Ordnung von Quantoren, welche die Ordnung *in* $\mathbf{Q_1^*x}$ und $\mathbf{Q_1^*y}$ erhält. Also $A \dashv\vdash \mathbf{Q_1^*x}\ \mathbf{Q_2^*y}(B^*\mathbf{o}C^*)$.

4) $A = QxB$. Nach IH, $B \dashv\vdash \mathbf{Qy}C$ in PNF, und wir präsupponieren durch Umbennenung, dass alle Variablen in $\mathbf{Qy}C$ verschieden von x sind; dann, nach Äquivalenztheorem $A \dashv\vdash \forall x\mathbf{Qy}C$.

QED.

Anm.: In der Praxis wird man PNFs in einer schöneren Weise als im obigen, induktiven Beweis produzieren.

Definition (Skolem Normalform):

1. Eine Skolem-Form (SF) von A wird erreicht, indem man erst A in eine pränexe Normalform A* umwandelt, und dann jedem Existenzquantor $\exists x$ in A* einzeln ein *neues* n-stelliges Funktionssymbol $f_{\exists x}$ zuweist und jede Variable x in A*, die durch $\exists x$ gebunden ist, durch den Term $f_{\exists x}(y_1,\ldots y_n)$ ersetzt, wobei $y_1,\ldots y_n$ alles Variablen sind, die durch Allquantoren gebunden sind, welche $\exists x$ in A*'s Zeichenreihe von Quantoren *vorausgehen*. Wenn n=0, ist das neue Funktionssymbol einfach eine Konstante.
2. Die duale Skolem-Form (DSF) von A wird wie oben erreicht, außer, dass man die Rolle von "$\exists$" und "$\forall$" vertauscht.

Beispiele:

Pränexe Formel:	Skolem-Form SF(A):	Duale Skolem-Form DSF(A):
$\exists x\forall yRxy$	$\forall yRxy$	$\exists xRxf(y)$
$\forall x\exists yRxy$	$\forall xRxf(x)$	$\exists yRxy$
$\forall x\exists y\forall z(Rxy \vee Qyz)$	$\forall x\forall z(Rf(x)y \vee Qf(x)z)$	$\exists y(Rxy \vee Qyf(y))$
$\exists x\forall y\exists z\forall u(Rxy\vee Qzu)$	$\forall y\forall u(Rxy\vee Qf(y)u)$	$\exists x\exists z(Rxf(x)\vee Qzg(x,z))$

Eine Skolem-Normalform ist nicht mehr äquivalent mit der ursprünglichen, pränexen Form. - Aber:

Theorem (Skolem-Normalform):

1. Wenn A* eine Skolem-Normalform von A ist, dann sind A und A* co-erfüllbar.
   (d.h., $\|\text{-/-} \neg A \Leftrightarrow \|\text{-/-} \neg A^*$).
2. Wenn A* eine duale Skolem-Normalform von A ist, dann sind A und A* co-gültig.
   (d.h., $\|\!\!\vdash\!\!\!- A \Leftrightarrow \|\!\!\vdash\!\!\!- A^*$).

Beweis: Anspruschvolle Übung 7.2: Beweisen Sie semantisch, dass $\forall x_{1\text{-}n}\exists yA(x_{1\text{-}n},y)$ erfüllbar ist, gdw $\forall x_{1\text{-}n}A(x_{1\text{-}n},f(x))$ erfüllbar ist, für entsprechendes, neues f. Der Rest kann durch Induktion auf Quantoren erledigt werden.

Theorem über konservative Extension, durch explizite Definition:

Angenommen, dass n-stelliges f, R $\notin \mathcal{R}(\Gamma)$; aber, dass t $\in \mathcal{T}(\Gamma)$, $\mathcal{L}(D) \subseteq \mathcal{L}(\Gamma)$. Dann für alle A mit $\mathcal{L}(A) \subseteq \mathcal{L}(\Gamma)$:

1. Wenn $\mathcal{V}_f(t) \subseteq \{x_1,\ldots,x_n\}$: $\Gamma \cup \{\forall x_1\ldots\forall x_n(fx_1\ldots x_n = t)\} \vdash A$ gdw $\Gamma \vdash A$.
2. Wenn $\mathcal{V}_f(D) \subseteq \{x_1,\ldots,x_n\}$: $\Gamma \cup \{\forall x_1\ldots\forall x_n(Rx_1\ldots x_n \leftrightarrow D)\} \vdash A$ gdw $\Gamma \vdash A$.

Anm: In 1. ist die Funktion f explizit definiert, in 2. die Relation R. t ist der *definierende Term* und D die *definierende Formel*.

Ohne die Bedingung $\mathcal{V}_f(t) \subseteq \{x_1,\ldots,x_n\}$, $\mathcal{V}_f(D) \subseteq \{x_1,\ldots,x_n\}$, würde die Definition nicht konservativ sein! (E.g., $\forall x,y$: $Rx \leftrightarrow D(x,y)$ impliziert $\exists yD(x,y) \rightarrow \forall yD(x,y)$).

Beweis: $\Leftarrow$ ist trivial. $\Rightarrow$: Durch Kontraposition. Angenommen $\Gamma \not\vdash A$. Dann gibt es ein Modell <D,v> definiert nach $\mathcal{L}(\Gamma,A)$, welches Γ verifiziert und A falsifiziert. Wir *erweitern* dieses Modell zu einem Modell $<D^+, v^+>$ $\mathcal{L}(\Gamma,A,R,f)$, sodass auch die explizite Definition verifiziert wird (wir wählen frei v(R) und v(f), sodass die Definition gilt.) Also $\Gamma \cup \{\forall x_1\ldots\forall x_n(fx_1\ldots x_n = t)\} \not\vdash A$.

Wichtige Notation:

Eine ***prädikatenlogische Theorie*** ist einfach eine Menge von nicht logisch wahren (d.h. synthetischen) Sätzen, die als Axiome einer Theorie angesehen werden, (ihre "Eigenaxiome") plus die daraus folgenden logischen Kosequenzen oder Theoreme. Jene nichtlogischen Symbole, welche durch Axiome der Theorie näher charakterisiert werden (d.h. in diesen Axiomen vorkommen) nennt man auch die *Eigensprache* (oder kurz: Sprache) der Theorie.

Z.B. ist die *naive Mengenlehre eine PL-Theorie* mit der speziellen binären Relation $\in$, welche nur folgendes Axiom enthält:

Naives Verständnis: Für alle P: $\exists x(x = \{y: Py\})$ –

formale Version 1. Stufe: $\exists x(\forall y(y \in x \leftrightarrow A[y]))$

Extensionalität: $\forall x,y: (\forall z(z \in x \leftrightarrow z \in y) \leftrightarrow x=y)$. (ist bereits die formale Version)

Alle anderen mengentheoretischen Notationen sind *Abkürzungen*, welche ersetzbar sind durch reine PL-Ausdrücke. Die Regeln für die Elimination sind folgende:

Umformung informeller Sprache in formale Sprache:

Ersetzen Sie: $y \in \{x: Px\}$ durch Py $y = \{x: Px\}$ durch $\forall z(z \in y \leftrightarrow Pz)$

Das Studium von PL-Theorien, der Arithmetik, der reellen Zahlen, der Mengenlehre; aber auch PL-formalisierte Axiomatisierungen von Theorien der Naturwissenschaften, ist eine *wichtige Anwendung* der Prädikatenlogik!

7.2 Äquivalenz- und Ordnungsrelationen

Wir benutzen im folgenden wieder einige abkürzende Notationen der Mengenlehre, können nun aber alles aus der PL verwenden, was wir bisher einführten. Z.B. schreiben wir $\forall x,y$: $A \rightarrow B$ kurz für $\forall x \forall y(A \rightarrow B)$; usw.
Wie erläutert, lassen sich alle folgenden Ausführungen als Darstellungen von PL-Theorien verstehen. Insbesondere benutzen wir nicht mehr die metasprachliche ($\Rightarrow$) sondern die objektsprachliche Implikation ($\rightarrow$). Wir schreiben häufig R sowohl für das Relationszeichen wie für die von "R" bezeichnete Relation über D.

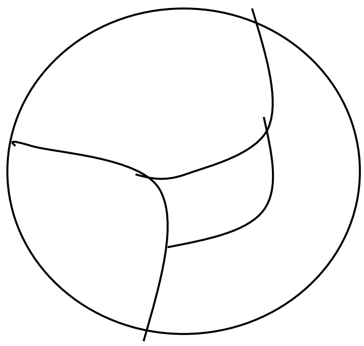
Definition (Äquivalenzrelation):
R ist eine Äquivalenzrelation über die Domäne D gdw R eine binäre Relation ist, sodass für alle x, y, z $\in$A: 1. Reflexivität: $\forall x$: Rxx

2. Symmetrie: $\forall x,y$: Rxy $\rightarrow$ Rxx
3. Transitivität: $\forall x,y,z$: Rxy $\wedge$ Ryz $\rightarrow$ Rxy

Eine spezielle Äquivalenzrelation: Die Identitäts- (oder diagonale) Relation,
Definiert durch $R_{\equiv} = \{<x,x>: x \in D\}$. (die feinste Äquivalenzrelation über D)

Definition (Partition):
Eine Partition einer Klasse D ist eine Klasse von paarweise disjunkten und (alles in allem) erschöpfenden Teilmengen von D – auch genannt: eine Klassifikation von D, eine Nominalskala von D - d.h., eine Klasse Π von Teilmengen von D, sodass:

- Disjunktheit: für alle x, y $\in$ B, $x \cap y = \emptyset$, und
- Erschöpfend-heit: $\bigcup \Pi = D$ *Bild:*



Anm.: für Π, eine Klasse von Mengen, bezeichnet $\bigcup \Pi$ die Vereinigung aller Mengen in Π.
Definition (Äquivalenzklassen).

Wenn R eine Äquivalenzrelation über D ist, dann:

1. Für jedes $a \in D$, $[a]_R =_{df} \{x \in D: xRa\}$ ist die R-*Äquivalenzklasse* von a (in D), oder die Äquivalenzklasse eines modulo R.
2. $D/R =_{df} \{[a]_R: a \in D\}$ ist die *Quotienzmenge* von D modulo R, oder die *R-Partition von D*.

Theorem (Äquivalenzklassen)*:* Sei R eine Äquivalenzrelation über D.

1. Für alle $x,y \in D$:
   1.1 Rxy gdw $[x]=[y]$
   1.2 entweder $[x]=[y]$ oder $[x]\cap[y]=\varnothing$
   1.3 $\bigcup D/R = D$.
2. D/R ist eine Partition von D.

Beweis: Übung.

Äquivalenzklassen sind eine wichtige Konstruktionsmethode in Philosophie, Ontologie, und Mathematik. – Beispiele:

Entität	*identifiziert mit der Äquivalenzklasse von:*
Mathematik:	
Rationale Zahl	Klasse aller Erweiterungen einer Bruchzahl
Reelle Zahl	Klasse aller Folgen rationaler Zahlen mit gleichem Grenzwert
Kardinalzahl	Klasse gleichmächtiger Mengen
Logik:	
Proposition	Klasse logisch äquivalenter Sätze
Ontologie:	
Universal	Klasse alle typidentischen Tropen (=Eigenschaftsinstanzen)
Individuum	Maximale Klasse von existenziell interdependenten Tropen
Physik:	
Zeitpunkt	Klasse zeitgleicher Punktereignisse
Raumpunkt	Maximale Klasse von sich überdeckenden Körpern

Weltlinie: Klasse aller genidentischen Ereignisse

Definition (partielle Ordnungsrelation):

1. Eine *strikt partielle Ordnung* über D ist eine binäre Relation über D, die die folgenden Konditionen erfüllt:

[a. Irreflexivität: $\forall x$: $\neg Rxx$ $\Rightarrow$ folgt aus b!]

b. Anti-Symmetrie: $\forall x,y$: $Rxy \rightarrow \neg Ryx$

c. Transitivität (wie oben)

2. Eine *schwach partielle Ordnung* über D ist eine binäre Relation über D, die folgendes erfüllt:

a. Reflexivität (wie oben)

b. Asymmetrie (schwache anti-Symmetrie): $\forall x,y$: $Rxy \wedge x \neq y \rightarrow \neg Ryx$

d.h.: $Rxy \wedge Ryx \rightarrow x=y$

c. Transitivität.

Wir schreiben $x <_R y$ (oder $x < y$) für R als strikt partielle Ordnung, und $x \leq_R y$ ($x \leq y$) für R als schwach partielle Ordnung.

Strikte und schwache Ordnungen sind interdefinierbar:

Angenommen $<_R$, $\leq_R$ definiert durch D:

$\forall x,y \in R$: $x \leq_R y$ gdw $x <_R y$ oder $x=y$.

$x <_R y$ gdw $x \leq_R y$ und $x \neq y$.

Eine partiell geordnete Menge $<D, \leq>$ wird auch *poset* genannt.

Definition (totale Ordnungen):

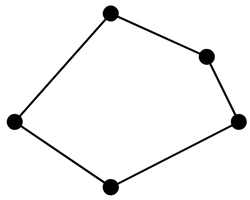
1. Eine strikt partielle Ordnung R über D ist eine strikt totale (oder lineare) Ordnung gdw sie zusätzlich *schwache Konnektivität* erfüllt: $\forall x,y \in D$: $x <_R y \vee y <_R x \vee x = y$.

Anm.: Wegen der Irreflexivität und anti-Symmetrie kann das inklusive Oder zu einem exklusiven Oder verstärkt werden.

2. Eine schwach partielle Ordnung R über A ist eine schwach totale (oder lineare) Ordnung gdw sie zusätzlich *Konnektivität* erfüllt: $\forall x,y \in A$: $x \leq_R y \vee y \leq_R x$.

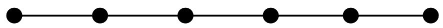
In einer partiellen Ordnung können Elemente unvergleichbar sein. Sie können als *Netz* dargestellt werden.

(Bild)



Totale Ordnungen haben keine unvergleichbaren Elemente – ihre Struktur ist linear

(Bild)



In empirischen Anwendungen, haben wir normalerweise keine (partiellen oder totalen) Ordnungen, aber (partielle oder totale) *quasi-Ordnungen*: hierbei können zwei verschiedene Objekte den selben Rang auf der Ordinalskala haben. Daher gilt weder $a < b$, $b < a$ noch $a = b$.

Definitionen und Fakten bezüglich (schwacher) quasi-Ordnungen:

1. R über D ist eine ***schwach partielle quasi-Ordnung*** wenn R reflexiv und transitiv ist.

2. R über A ist eine schwach totale quasi-Ordnung gdw sie reflexiv, transitiv und konnex ist.

3. Wir definieren die Relation $\equiv_R$ den gleichen Rang zu haben bezügl. R durch:

   $x \equiv_R y$ gdw $x \leq_R y$ und $y \leq_R x$.

4. Wir definieren eine **strikte quasi-Ordnung** durch: $x <_R y$ gdw $x \leq_R y$ und nicht $y \leq_R x$.

Anm.: eine strikte quasi-Ordnung ist anti-symmetrisch und schwach konnex, bezügl. $\equiv_R$.

5. Wir können jede quasi-Ordnung über D in eine Ordnung umwandeln, indem wir die Äquivalenzpartition von D bezügl. $\equiv_R$ anwenden:

   Wir definieren für alle $[a], [b] \in D/\equiv_R$: $[a] \leq_R [b]$ gdw $a \leq_R b$. Dann ist $\leq_R$ eine Ordnung über $D/\equiv_R$ - d.h., es ist eine Ordnung der Äquvialenzklassen bezügl. $\equiv_R$.

(Bild: man zeichnet das Netz mit Kreisen statt Punkten)

Anm.: str. qu-O. $<_R$ ist definierbar mit schw. qu.-O. $\leq_R$, aber $\leq_R$ ist nur definierbar mit $<_R$ und $\equiv_R$.

Weitere Terminologie: Wenn R eine a totale Ordnung über A und $a \in A$ ist, dann wird b der (unmittelbare) R-Nachfolger von a (in A) genannt gdw $a<b$ und $\neg\exists x$: $a<x<b$. Gleichermaßen ist b der (unmittelbare) R-Vorgänger von a gdw $b<a$ und $\neg\exists x$: $b<x<a$.

Übungen:

7.3. Welche der folgenden Relationen ist eine Äquivalenzrelation? Erläutern Sie wieso (nicht).

x lebt weit weg von y, x hat das selbe Geschlecht wie y, x ist ein Geschwister von y, x ist ein Nachbar von y, x hat die selbe Farbe wie y, x hat annähernd dasselbe Gewicht, wie y.

7.4. Beweisen Sie, dass die folgenden Klassen $\{A_r: r \in \mathbb{R}\}$ eine Partition von $\mathbb{R} \times \mathbb{R}$ sind, d.h. eine Partition der reellen Ebene ($\mathbb{R}$ für reele Zahlen a) $A_r = \{<x,y>: y = x+r\}$. b) $A_r = \{<x,y>: x^2+y^2 = r\}$.

7.5. Für eine gegebene Menge A, welche ist die gröbste (extensional die größte, bezügl. Õ) und welche ist die feinste (extensional die kleinste bezügl. Õ) Äquivalenzrelation über A, und was ist die korrespondierende Partition von A?

7.6. Welche der folgenden Relationen ist (i) eine quasi-Ordnungsrelation, (ii) eine Ordnungsrelation - und wenn eines von beiden, ist sie (iii) partiell oder total?

x wiegt mehr als y (physische Dinge), x ist mehr Geld wert als y, x ist annähernd 20 cm größer als y, x ist mindestens 20 cm größer als y, Ich mag Person x mehr als Person y, Handlung x is moralisch zu bevorzugen gegenüber Handlung y.

- Anahnd von $\mathbb{N}$: x ist ein Teiler von y, x ist kein Teiler von y.

Besonderes Problem: Partei x hat mehr Wähler als Partei y. (i) Nehmen Sie eine Wahl für alle Parteien zusammen an. (ii) Nehmen Sie mehrere Wahlen für jedes Paar an.

7.7. Betrachten Sie folgende quasi-Ordnung R über A = {a,b,c,d}: R = {a≤a, a≤b, a≤c, a≤d, b≤b, b≤c, b≤d c≤c, c≤b, c≤d, d≤d}. Konstruieren Sie die Äquivalenzklassen bezügl. $\equiv_R$ und die totale Ordnung über $A/\equiv_R$.

Fakten über totale Ordnungen:

Jede *endliche,* total geordnete Menge hat ein einziges größtes und ein einziges kleinstes Element und jedes seiner Elemente hat einen einzigen Vorgänger und Nachfolger. Keine dieser Eigenschfaten muss für total geordnete, unendliche Mengen gelten.

Beispiele unendlicher totaler Ordnungen:

- die Menge der natürlichen Zahlen hat ein kleinstes, aber kein größtes Element:

  0 1 2 3 .... n n+1 ....

- Die Menge der ganzen Zahlen hat kein größtes und kein kleinstes Element:

  .... −2 −1 0 1 2 ......

In dieser Menge hat jedes Element einen Vorgänger und einen Nachfolger.

- Wenn wir zur Menge der ganzen Zahlen ein einzigartiges, kleinstes Element $-\omega$ hinzufügen und ein einzigartiges größtes Element ω (dies sind keine natürlichen Zahlen mehr), dann hat $-\omega$ keinen Vorgänger und ω keinen Nachfolger.

  $-\omega$ ...... −2 -1 0 1 2 .... $+\omega$

- Rationale Zahlen: keine rationale Zahl hat einen Vorgänger, oder Nachfolger, weil rationale Zahlen *dicht* sind. Dasselbe gilt für reelle Zahlen.

  ..... q_i .... q_j ....

Definition (Wohlordnung):

Eine (strikte, schwache) totale Ordnung R über D ist eine Wohlordnung gdw jede nichtleere Unterklasse $B \subseteq A$ ein kleinstes Element bezügl. R hat.

Anm.: 1. Die rationalen und die reellen Zahlen sind nicht wohlgeordnet - in der Standardordnung! – offene Intervalle haben keine minimalen und maximalen Elemente:

$(3,4) = \{x: 3 < x < 4\}$ geschlossene Intervalle: $[3,4] = \{x: 3 \leq x \leq 4\}$

2. In einer wohlgeordneten Menge hat jedes Element einen *einzigartigen Nachfolger*, weil die Menge der Elemente, größer als a ein kleinstes Element hat.

Es muss keinen einzigartigen Vorgänger geben.

Bild: die Wohlordnung der so genannten Ordinalen:

$0 \ 1 \ 2 \ \ldots\ldots \omega_0 \quad \omega_0 +1, \ \omega_0+2 \ \ldots\ldots \omega_1 \ \ \omega_1+1 \ \ldots. \ \ \omega_i \ \ \omega_i +1 \ \ \ldots..$

Wohlordnung ist so bedeutend, weil sie mit dem Prinzip der (transfiniten) Indukiton äquivalent ist. D.h. Induktion gilt weil die natürlichen Zahlen wohlgeordnet sind.

7.3 Axiomatische Mengenlehre *(nach Zermelo-Fraenkel)*

Das naive Verständnisaxiom wird aufgegeben.

Über das Extensionalitätsaxiom hinaus werden zusätzliche Axiome angegeben, was alles (antinomienfreie) Mengen sind.

Eine *Klasse* = eine Sammlung oder Familie von *Objekten/Individuen* (irgendeiner Art).

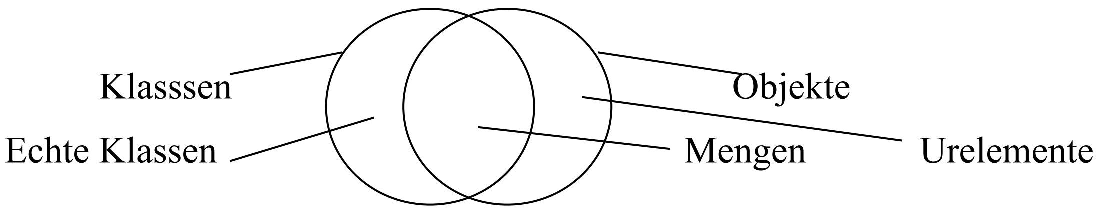
Eine *Menge* = eine Klasse, die als (existentes) einzelnes Objekt angesehen wird, ein Individuum.

Eine *echte* Klasse – eine Klasse, die keine Menge ist. Z.B. die Klasse aller Objekte, $\{x : x{=}x\}$.

Obwohl wir auf eine Klasse im Singular referieren, ist dies nur eine Sprechweise.

(Zur Erinnerung: Elemente von Klassen sind immer Objekte; Also haben wir keine Klassen, die echte Klassen enthalten.)

Zusammenfassendes Bild:



Transformation informeller Spache in Formalsprache:

Man ersetze: $y = \{x: A\}$ durch $\forall z(z\in y \leftrightarrow z\in \{x:A\})$

$y \in \{x: A[x]\}$ durch $A[x/y]$

$y \in \{x_1,\ldots,x_n\}$ durch $y = x_1 \vee \ldots \vee y = x_n$

x ist eine Menge durch $\exists y(x{=}y)$.

Man schreibe Großbuchstaben jeglicher Art in Variablen um x, y, z, x_i ...

Immer die richtigen Quantoren Hinzufügen.

Axiome für Mengen:

Axiom 1: Extensionalität

Für alle Mengen A und B: *wenn* für alle x, $x \in A \Leftrightarrow x \in B$, *dann* A = B.

Formal: $\forall x,y: (\forall z: z \in x \leftrightarrow z \in y) \rightarrow x=y$.

Axiom 2: Paarmenge: Für alle (Objekte) x, y: $\{x,y\}$ ist eine Menge.

Formal: $\Leftrightarrow\ \forall x,y \exists z: z = \{x,y\}\ \ \Leftrightarrow\ \ \forall x,y \exists z: \forall u(u \in z \leftrightarrow u=x \vee u=y))$

Theoreme (alle ohne Beweis aufgestellt): $\{a\} = \{a,a\}$ ist eine Menge, die einelementige Menge von a.

Axiom 3: Teilmengen, Aussonderung:

Wenn $B \subseteq A$ und A eine Menge ist, dann ist B eine Menge.

Kann in dieser Form nicht formalisiert werden. Einzig wie folgt:

$\forall x \exists y \forall z:\ \ z \in y\ \leftrightarrow\ (z \in x \wedge A[z])$ für beliebige Formel A.

Theorem (Aussonderung, leere Menge):

1.Wenn A eine Menge ist, dann ist $\{x \in A: Px\}$ eine Menge.

2. $\varnothing$ ist keine Menge, vorausgesetzt, es gibt zumindest ein Objekt.

Theorem (Universum des Diskurses): Die Klasse aller Objekte (das Universum des Diskurses) und die Klasse aller Menge sind echte Klassen.

Beweis: Weil Russell's (echte) Klasse eine Unterklasse dieser Klassen ist und nach axiom Teilmenge. *(--> Philosophische Reflektion)*

Axiom 4: Vereinigungsmenge: Wenn A eine Menge ist, dann ist es auch $\bigcup$ A.

Übung 7.8 Schreiben Sie dies in eine formale Version um.

Theorem (Vereinigung)*:* A und B sind Mengen $\Rightarrow$ $A \cup B$ ist eine Menge .

Beweis: Per Def. *Vereinigungsmenge* und Axiom *Paarmenge*.

Theorem: Für jede natürliche Zahl $n \in \mathbb{N}$ und Objekte $a_1,\ldots,a_n$, ist $\{a_1,\ldots,a_n\}$ eine Menge.

Beweis durch schwache Induktion auf n

Axiom 5. Potenzmenge: Wenn A eine Menge ist, dann ist $\mathbb{P}(A)$ auch eine.

Übung 7.9: Schreiben Sie dies in formale Version um.

Theorem: 1. $A \times B$ ist eine Menge gdw sowhol A als auch B Mengen sind.

2. Wenn A eine Menge ist und R eine n-stellige Relation über A, dann ist R auch eine Menge.

3. f ist eine Menge gdw sowohl dom(f) als auch ran(f) Mengen sind.

Axiom 6: Ersetzung:

Wenn f eine Funktion ist, und dom(f) eine Menge, dann ist auch ran(f) eine Menge.

Übung 7.10: Schreiben Sie dies in eine formalisierte Version um, als Axiom-Schema.

Konstruktion von Ordinalzahlen:

Die Konstruktion von Ordinalen nimmt keine Urelemente an, sondern setzt sich von der leeren Menge als Anfangspunkt fort.

$\mathbb{N}$:	Ord:	
0	$\emptyset$ $\{\,\}$	0
1	$\{\emptyset\}$	$1 = \{0\}$
2	$\{\emptyset, \{\emptyset\}\}$	$2 = \{0, 1\}$
3	$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$	$3 = \{0,1,2\}$
⋮	$o^+ =_{df} o \cup \{o\}$	Definition eines nachfolgenden Ordinals

(Stop) $\omega = \omega_0 = \{o_i : i \in \mathbb{N}\}$ Das erste Grenzordinal

$=$ die kleinste Klasse O, sodass das kleinste infinite Ordinal

i) $\emptyset \in O$ und wenn $o \in O$, dann $o^+ \in O$ $o = \bigcup o$ - Def. eines Grenzordinals

(= die kleinste Nachfolgermenge, oder die kleinste 'induktive' Menge)

$\omega_0 + 1 = \omega_0^{+} = \omega_0 \cup \{\omega_0\}$ (Nachfolger-Ordinal)

$\omega_0 + 2 = \omega_0^{++} = \omega_0 \cup \{\omega_0\} \cup \{\omega_0 \cup \{\omega_0\}\}$

⋮

ω_1, zweites Grenzordinal auch $\omega \cdot 2$ genannt (dann ω_1 1. überabzählbare)

⋮ etc.

Ord ist die Klasse aller Ordinale. $o_1, o_2 \ldots$ ordnen Ordinale nach Rängen (man benutzt auch: ξ)

Zwei alternative Definitonen von ω = die Menge der natürlichen Zahlen als Ordinale gezeigt:

= Klasse aller endlichen Ordinale, oder

= das kleinste Nachfolgerordinal.

Axiom 7 Unendlichkeit: ω ist eine Menge.

Formal: $\exists x\colon\ \varnothing \in x \wedge \forall y(y \in x \rightarrow \{y\} \in x\} \wedge \forall z\colon (\varnothing \in z \wedge \forall y(y \in z \rightarrow \{y\} \in z\}) \rightarrow x \subseteq z\}$

Definition von Kardinalen:

Zwei *Mengen* a, b haben die selbe Kardinalität, oder sind *äquipollent*, kurz $a \equiv_c b$, gdw es eine Bijektion von a nach b gibt.

$|A|$ bezeichnet die Kardinalität einer Menge A. D.h., $A \equiv_c B$ gdw $|A| = |B|$.

Für endliche Mengen: $|A| = |B| \Rightarrow$ nicht: $A \subset B$. *Gilt nicht für unendliche Mengen!*

Für endliche Ordinale, $|o_1| = |o_2| \Rightarrow o_1 = o_2$. *Gilt nicht für unendliche Ordinale!*

Beispiele von Kardinalitäten von unendlichen Mengen:

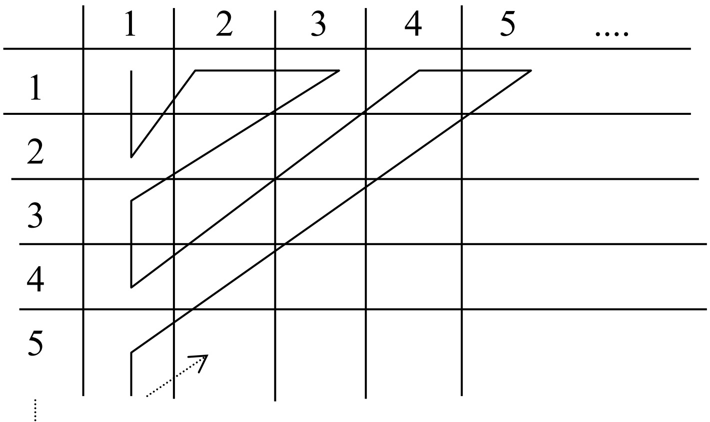
Die Menge der graden Zahlen E ist äquipollent mit der Menge der natürlichen Zahlen ω.

0 1 2 3 4… eine Bijektion

0 2 4 6 8…

Sogar die Menge der rationalen Zahlen ist *abzählbar* – z.B. auf diese Weise:

Also $|\omega\times\omega| = |\omega|$.



Die Menge endlicher Sequenzen (Listen) natürlicher Zahlen ist *abzählbar*.

- Also ist $\bigcup\{\omega^n\colon n \in \omega\}$ abzählbar $\neq$ ω^ω (!!).

Cantor's berühmter Beweis, dass $| \mathbb{P}(A) | >_c |A|$ *- visualisiert:*

Für $B \subseteq A$ wird die Funktion *$f: A \rightarrow \{0,1\}$ sodass $f(x) = 1$ gdw $x \in B$*

die *charakteristische Funktion* von B auf A genannt.

Wir können Teilmengen $B \subseteq A$ durch ihre charakteristische Funktion ersetzen.

Also: $| \mathbb{P}(A) | = | 2^A |$.

	0	1	2	3	....
0	0	1	0	0	....
1	0	1	1	1	....
2	1	0	1	0	....
3	0	1	0	0	....
⋮	......				
	1	0	0	1	....

eine abzählbare Liste

Begrenzende Resultate
die Methode der Diagonalisierung

= Differenz zwischen Zeile i und i-ter Position der anti-Diagonale

Auf dieselbe Weise hat Cantor die Unabzählbarkeit der reellen Zahlen bewiesen.

Die Kardinalität von $\mathbb{P}(\omega)$ gleicht der des Kontinuums – die Menge der reellen Zahlen.

Zusammenfassung der Axiome für ZF wie bis hierhin vorgestellt, wir hatten:

1. Extensionalität

2. Paarmenge

3. Teilmenge

4. Vereinigungsmenge

5. Potenzmenge

6. Ersetzung

7. Unendlichkeit

(8. Leere Menge --> wurde aus der Existenz von zumindest einem Objekt abgeleitet)

All diese Axiome sind voll akzeptiert. Zwei weitere Axiome werden zusätzlich akzeptiert.

9. Axiom der Wahl (AW): Für jede Menge A nicht-leerer Mengen gibt es eine *Auswahlfunktion*, d.h., eine Funktion $f{:}A \to \bigcup A$ sodass $\forall x \in A{:}\ f(x) \in x$.

Theorem: Unter den Axiomen 1-8 sind die folgenden Konditionen äquivalent:

1. AW
2. Für jede Menge A gibt es eine Wohlordnung über A.
3. *Zorn's Lemma*

Peano lehnte 1890 AW als unhaltbar ab.

Gödel bewies 1938, dass AC relativ zu den Axiomen von ZF konsistent ist.

1963 bewies Cohen, dass $\neg$AC konsistent ist, relativ zu den anderen Axiomen von ZF.

10. Axiom der Gleichmäßigkeit (oder Grundlage):

Jede nicht-leere Menge hat ein $\in_a$-minimales Element.

Konsequenzen: - keine Menge enthält sich selbst $\forall a{:}\ a \notin a$ – keine $\in$-Zyklen $a_1 \in \ldots \in a_n \in a_1$

- keine infinit absteigenden Ketten von $\in$-Sequenzen $\ldots a_n \in a_{n-1} \in \ldots \in a_2 \in a_1$.

Dieses Axiom ist unabhängig von den anderen Axiomen der Mengenlehre.

Peter Aczel und Jon Barwise entwickelten eine Mengenlehre, die selbstenthaltende Mengen zulässt. (Wichtig für das so genannte Lügner-Paradox.)

7.4 Vollständigkeit der Prädikatenlogik 1. Ordnung

--> Wie für die AL im Henkin-Style.

--> Die Idee: Wir konstruieren ein Modell für Γ_{max} aus der Sprache heraus - ein so genanntes *kanonisches* Modell. Wir wünschen, die Vollständigkeit durch ein Wahrheitslemma zu beweisen, welches besagt, dass eine Formel in Γ_{max} ist gdw sie wahr ist im kanonischen Modell von Γ_{max}. Es gibt zwei Probleme:

1. Wenn Γ Identitätsformeln $t_1 \equiv t_2$ enthält, dann $v(t_1)=v(t_2)$.

   Aber $t_1 \neq t_2$! (metasprachliche Bedeutung: t_1 und t_2 sind verschiedene Variablen).

   Lösung: wir verstehen die *≡-Äquivalenzklassen* [t] von Termen als unsere Objekte.

2. Wenn Γ eine Formel der Form $\exists xA$ enthält, brauchen wir zumindest ein Objekt [a] in unserem Objektbereich, sodass v[x:a] $\exists xA$ wahr macht. Eine Formelmenge, die diese Eigenschaft erfüllt, wird ω-vollständig genannt. Also brauchen wir eine *neue* Konstante a für jedes der unendlich vielen $\exists xA$ in Γ_{max}. Wir fügen eine unendliche Menge $\mathcal{C}$ * von neuen Konstanten zu $\mathcal{L}$ hinzu.

   (Wir brauchen es nicht wie in dem Machover Buch zu machen, wo eine unendliche Zahl unendlicher Mengen von neuen Konstanten hinzugefügt wird.)

Definition (ω-Vollständigkeit, Saturiertheit):

1. Γ ist ω*–vollständig* gdw ($\exists xA \in \Gamma \;\Rightarrow\; A[x/t] \in \Gamma$ für irgendein $t \in \mathcal{T}$)
2. Γ ist *saturiert* gdw Γ maximal konsistent und ω–vollständig ist.

Übung 7.12: Beweisen Sie für maximal konsistentes Γ:

($\exists xA \in \Gamma \Rightarrow A[t/x] \in \Gamma$ für irgendein $t \in \mathcal{T}$) $\Leftrightarrow$ ($A[t/x] \in \Gamma$ für alle $t \in \mathcal{T} \Rightarrow \forall xA \in \Gamma$).

($\exists$-Version der ω-Vollständigkeit) ($\forall$-Version der ω-Vollständigkeit)

Gesättigte Formelmengen erfüllen alle Max-Eigenschaften, die wir in der AL bewiesen haben.

Theorem (Saturierung):

Jede konsistente Formelmenge Γ in einer gegebenen Sprache $\mathcal{L}$ kann zu einer saturierten Formelmenge Δ erweitert werden, in einer Sprache $\mathcal{L}^*$ die aus $\mathcal{L}$ durch das Hinzufügen einer unendliche Menge $\mathcal{C}^+$ *neuer* Konstanten entsteht.

$\mathcal{C}^* = \mathcal{C} \cup \mathcal{C}^+$ $\qquad$ $\mathcal{L}^*$ ist wie $\mathcal{L}$, außer, dass sie $\mathcal{C}^*$ satt $\mathcal{C}$ hat

Saturierungslemma:

Wenn $\Gamma \cup \exists xA$ konsistent ist und a nicht in Γ oder $\exists xA$ vorkommt, dann ist auch $\Gamma \cup \{\exists xA, A[x/a]\}$ konsistent.

Beweis: Andernfalls (i) $\Gamma \cup \{\exists xA\} \vdash \neg A[x/a]$ (nach iIB), woher $\Gamma \cup \{\exists xA\} \vdash \forall x \neg A$ (nach UG aus (i) da $a \notin \mathcal{C}(\Gamma \cup \{\exists xA\})$), was bedeuten würde, dass $\Gamma \cup \{\exists xA\}$ inkonsistent ist (da $\forall x \neg A = \neg \exists xA$, per Def. $\exists$), was der Annahme widerspricht.

Beweis Theorem: Wir konstruieren Δ wie folgt, unter der Annahme einer gegebenen Nummerierung aller Formeln A_o, $A_1 \ldots$ in $\mathcal{L}^*$ (!) und aller Konstanten in $\mathcal{C}^+$ wie folgt:

$\Delta_o := \Gamma$

$\Delta_{n+1} =:$ $\quad \Delta_n \cup \{A_n, B[x/a]\}$, wobei a die erste Konstante in $\mathcal{C}^+ - \mathcal{C}(\Delta_n, A_n)$ ist
wenn $\Delta_n \cup \{A_n\}$ konsistent ist und A_n die Form $\exists xB$ hat

$\Delta_n \cup \{A_n\}$ wenn $\Gamma_n \cup \{A_n\}$ konsistent ist und nicht die Form A_n $\exists xB$ hat

Δ_n $\quad$ wenn $\Gamma_n \cup \{A_n\}$ inkonsistent ist

$\Delta := \bigcup \{\Delta_i \mid i \in \omega\}$

Für jedes n, gibt es unendlich viele neue Konstanten die in $\mathcal{C}^+ - \mathcal{C}(\Delta_n, A_n)$ verbleiben.

Wir beweisen, dass: Δ eine saturierte Erweiterung von Γ ist.

1. $\Delta \supseteq \Gamma$, also ist Δ eine Erweiterung von Γ.
2. Δ ist konsistent: Nach dem Saturierungslemma wissen wir, dass für jedes n, Δ_{n+1} konsistent sein muss, wenn $\Delta_n \cup \{A_n\}$ konsistent ist; und wenn $\Delta_n \cup \{A_n\}$ inkonsistent ist, ist Δ_{n+1} per Def. konsistent. Also argumentieren wir wie im Vollständigkeitsbeweis der AL.
3. Dass Δ maximal konsistent ist, zeigt man wie im Vollständigkeitsbeiweis der AL.
4. Dass Δ ω-vollständig ist, gilt, da jede Formel $\exists xA$ eine feste Anzahl n in der Nummerierung hat und in diesem Schritt eine Formel der Form $A[x/a]$ zu $\Delta_n \subseteq \Delta$ hinzugefügt worden ist.

Q.E.D.

- *Theorem* (kanonisches Modell):

Jede saturierte Formelmenge Γ hat ein Modell (das so genannte kanonische Modell, wie unten definiert).

Beweis: Angenommen Γ ist saturiert. Wir definieren:

Definition des kanonischen Modells:

Für jedes $t \in \mathcal{T}$, $[t] = [t]_{\equiv\Gamma} =_{df} \{t' : t \equiv t' \in \Gamma\}$ (die Äquivalenzklasse von t)

(d.h. $\equiv_\Gamma$ ist eine Äquivalenzrelation über $\mathcal{T}$, $t_1 \equiv_\Gamma t_2$ gdw $t_1 \equiv t_2 \in \Gamma$)

$Dm = \mathcal{T}/\equiv_\Gamma =_{df} \{[t] : t \in \mathcal{T}\}$ der kanonische Objektbereich

1. $v(x) = [x]$ für alle $x \in \mathcal{V}$ die kanonische
2. $v(a) = [a]$ für alle $a \in \mathcal{C}$ Bewertungsfunktion
3. Für alle $f \in \mathcal{F}^n$, $n > 0$: $v(f)([t_1],\ldots,[t_n]) = [ft_1\ldots t_n]$ (dies definiert $v(f)$)
4. Für alle $R \in \mathcal{R}^n$, $n > 0$: $<[t_1],\ldots,[t_n]> \in v(R)$ gdw $Rt_1\ldots t_n \in \Gamma$ (dies definiert $v(R)$)

Wir haben gezeigt, dass unsere Definition für Bewertungsfunktionen *konsistent* ist. Dafür müssen wir zeigen, dass bei jeder Wahl von t, $t^* \in [t]$, das folgende gilt:

Wenn $t_i, t_i^* \in [t]$, dann: $v(ft_1\ldots t_n) = v(ft_1^*\ldots t_n^*)$

$$v(Rt_1\ldots t_n) = v(Rt_1{}^*\ldots t_n{}^*).$$

Beweis: Wenn t_i, $t_i{}^* \in [t]$, dann $t_i \equiv t_i{}^* \in \Gamma$, also $\Gamma \vdash t_i \equiv t_i{}^*$, daher folgen $\Gamma \vdash ft_1\ldots t_n \leftrightarrow ft_1{}^*\ldots t_n{}^*$ und $\Gamma \vdash Rt_1\ldots t_n \leftrightarrow Rt_1{}^*\ldots t_n{}^*$ aufgrund von Ext$\leftrightarrow$.

- *Wahrheitslemma:* Es sei M = <D,v> das kanonische Modell von Γ.

Dann gilt für alle A: $M \models A$ gdw $\models A \in \Gamma$

Beweis: (1) $A = Rt_1\ldots t_n$: per Definition.

$A = t_1 \equiv t_2$: $t_1 \equiv t_2 \in \Gamma \Leftrightarrow t_1, t_2 \in [t_1] \Leftrightarrow v(t_1) = v(t_2) = [t_1] \Leftrightarrow M \models (t_1 \equiv t_2)$.

(2) $A = \neg B$, $A = B \vee C$ werden bewiesen wie in AL, durch die Eigenschaften Max$\vdash$, Max$\neg$ und Max$\vee$.

(3) $A = \forall xB$: $\forall xB \in \Gamma \Leftrightarrow \forall t \in \mathcal{T}: B[x/t] \in \Gamma$

[$\Rightarrow$ nach UI und Max$\vdash$; $\Leftarrow$ nach ω-Vollständigkeit von Γ in der ∀-Version]

$\Leftrightarrow \forall t \in \mathcal{T}: M \models B[x/t]$ (nach IH)

$\Leftrightarrow \forall t \in \mathcal{T}: v[x:[t]](B) = 1$ (Koinzidenzlemma, da $v(t)=[t]$)

$\Leftrightarrow \forall d \in D: v[x:d](B) = 1$ (da $D = \mathcal{T}/\equiv_\Gamma$) $\Leftrightarrow M \models \forall xB$. Q.E.D.

- *Theorem* (starke Vollständigkeit):

S*1 ist stark (und daher schwach) Vollständig.

Beweis: Wir argumentieren wie in AL: Eine gegebene, konsistente Γ, kann erweitert werden zu einer saturierten Δ (in erweitertem $\mathcal{L}$*) nach dem Saturierungstheorem. Δ und daher $\Gamma \subseteq \Delta$, sind damit erfüllt von dem kanonischen Modell nach dem kanonischen Modell-Theorem. Q.E.D.

Theorem (Kompaktheit): S***1** ist kompakt, d.h. für alle $\Gamma \subseteq \mathcal{L}$ (Erfüllbarkeitsversion): Jede endliche Teilmenge Γ_f von Γ ist erfüllbar $\Leftrightarrow$ Γ ist erfüllbar.

Beweis: Wie in der AL.

7.5 Die Frage der Entscheidbarkeit in der PL:

Ein Problem ist mengentheoretisch reduzibel auf eine Frage der Form:
Ist ein gegebenes $x \in A$ ein Element von $B \subseteq A$ (hat es eine spezielle Eigenschaft B)? Z.B. ist eine Zeichenreihe $s \subseteq \mathbf{S}$ eine wff ($\mathcal{L} \subseteq \mathbf{S}$); oder ist eine wff ein logisches Theorem ($\mathbf{L} \subseteq \mathcal{L}$) , etc.

Definition (Entscheidbarkeit):
$B \subseteq A$ ist *entscheidbar* (oder *rekursiv*) *in A* gdw es einen *Algorithmus* α gibt, welcher für jedes $x \in A$ nach einer *endlichen Anzahl von Schritten* korrekt entscheidet, ob $x \in B$ oder nicht – d.h. eine korrekte ja-oder-nein Antwort gibt.
Dadurch wird ein Algorithmus als ein berechenbarer Mechanismus beschrieben, welcher rekursive Funktionen realisiert, die alleine mit Hilfe einfacher, arithmetischer Operationen definiert sind, so wie "ersetze ein Numeral durch ein anderes", "vergleiche, welches von zwei Numeralen das größere ist", "addiere 1", "subtrahiere 1"., etc.
Anm.: Entscheidbarkeit impliziert nicht nur die Korrektheit des Algorithmus, sondern auch die Eigenschaft des *Voranschreitens* für selbigen– der Algorithmus α tritt niemals in einen Zirkel, oder infiniten Regress ein.

Die AL war entscheidbar. Z.B. semantisch.

Für die PL haben wir kein generelles, semantisches Entscheidungsverfahren. Wir haben nur ein generelles, deduktives Kalkül!
→ Unsere Auffassungen von "x ist eine Instanz eines Axiom-Schemas, oder eines Regelschemas", "x ist ein Beweis von y", und "x ist ein Beweis von irgendetwas" sind entscheidbar.
→ *Aber:* die Auffassung "y ist beweisbar", "es gibt einen Beweis für y" ist nur semi-entscheidbar.
→ *Denn:* die deduktiven Regeln MP, Simp, iIB und kIB sind <u>nicht rekursiv</u>, weil ihre

Prämissen-Sequenzen nicht kleiner im Grad der Komplexität sind.

Z.B.: *Beweisziel:*

$$\ldots \left.\begin{array}{l} \Gamma \vdash B_2 \\ \Gamma \vdash B_2 \rightarrow B_1 \\ \Gamma \vdash B_1 \rightarrow A \end{array}\right\} \Rightarrow \left.\begin{array}{l} \Gamma \vdash B_1 \\ \Gamma \vdash B_1 \rightarrow A \end{array}\right\} \Rightarrow \Gamma \vdash A$$

Anm.: Es gibt rekursive (daher: entscheidbare) Sequenzenkalküle für die AL – die so genannten *Schnittregel-freien Kalküle.* Aber diese Kalküle sind unpraktisch. Für die PL gibt es keine rekursiven, deduktiven Systeme.

Genereller: ein deduktives Kalkül (mit nicht-rekursiven Regeln) *bietet kein Entscheidungsverfahren:*

→ es gibt *lediglich* einen Algorithmus – den so genannten Algorithmus der *rekursiven Nummerierung* – welcher einen Beweis für eine Formel A findet, WENN die Formel A beweisbar IST. Diese Eigenschaft wird *semi-Entscheidbarkeit* genannt.

– aber WENN eine Formel unbeweisbar ist, wird der Algorithmus der Nummerierung → d.h. t *für immer* ohne Resultat weitergehen.

Definition (rekursive Nummerierbarkeit, r.N.; rekursive Axiomatisierbarkeit)*:*

(1) Eine abzählbar unendliche Menge S wird als rekursiv (oder 'effektiv') nummerierbar bezeichnet gdw es eine berechenbare bijektive Funktion $f{:}|N \rightarrow S$ gibt.

(2) Eine Logik **L** und ihre Schlussrelation wird *rekursiv nummerierba*r (r.n.) genannt gdw es eine effektive Nummerierung aller Theoreme und Ableitungen von **L** gibt.

(3) Eine Logik **L** und ihre Schlussrelation sind *rekursiv axiomatisierbar* gdw sie eine *korrekte und vollständige Axiomatisiserung hat,* die aus entscheidbaren Regel- und Axiomschemata X besteht (d.h., es ist entscheidbar, ob eine Formel/Sequenz eine Instanz von X ist) und eine finitäre Auffassung von Beweisen (wie oben definiert).

Anm.: Man spricht von *finiter Axiomatisierbarkeit* gdw die Menge der Axiom- und Regelschemata endlich ist.

Fakt: Nicht jede abzählbar unendliche Menge ist effektiv numerierbar.

Beweis: Es gibt unabzählbar viele abzählbar unendliche Teilmengen von $\mathbb{N}$,
Aber es gibt lediglich abzählbar unendlich viele berechenbare Funktionen,
da (nach der Church-These) jede solche Funktion als eine Formel der Arithmetik ausdrückbar ist und die Sprache der Arithmetik hat nur abzählbar viele Formeln. QED.

Die Verbindung zwischen Entscheidbarkeit und rekursiver Nummerierbarkeit (r.N.):

Theorem: Angenommen A ist abzählbar unendlich und B $\subseteq$A. Wenn sowohl B als auch (A-B) r.n. sind, dann ist B entscheidbar in A.

Korollar 1: Es sei **L** $\subseteq$ $\mathcal{L}$. Wenn **L**'s Theoreme und **L**'s nicht-Theoreme rekursiv nummerierbar sind, dann ist **L** entscheidbar (in $\mathcal{L}$).

Korollar 2: Angenommen, das Deduktionstheorem (Version $\wedge$) gilt für **L**, dann: wenn **L** entscheidbar ist, dann sind **L**'s Schlüsse mit finiter Prämissenmenge entscheidbar (Richtung $\Leftarrow$ ist trivial).

Beweis: Eine der r.n. hat ein Resultat nach einer endlichen Zeit. QED.

Gödelisation – wie man Formeln und Sequenzen natürliche Zahlen zuordnet:

Theorem (r.n.): Eine rekursiv axiomatisierte Logik ist r.n. (Gleiches gilt für Schlussrelationen.)

Beweis: Das Theorem generalisiert sogar zu r.n.-axiomatisierbaren Logiken, deren Menge von Axiomen und Regel-Instanzen lediglich rekursiv nummerierbar ist, aber wir beschränken unseren Beweis auf den üblicheren Fall von entscheidbaren Regeln und Axiomen.

Wir präsupponieren die Mengen $\mathcal{V}$, $\mathcal{R}^n$, $\mathcal{F}^n$, $\mathcal{C}$ als nummeriert (angefangen bei 1). Man bemerke, dass wir abzählbar unendlich *viele* Mengen $\mathcal{R}^n$, $\mathcal{F}^n$ haben, von denen jede abzählbar unendlich viele Symbole haben kann ($R_1{}^n$, $R_2{}^n$,…).

Wir benutzen *Gödel's Methode der Primzahlen* (aber es gibt auch andere Methoden; cf. *Hunter: Metalogik*).

Fakten über Prim-Dekomposition: *jede natürliche Zahl n hat eine einzigartige Prim-Dekomposition:* $\exists! p_1,...,p_k,\ n_1,...,n_k$: $n = p_1^{n1} \cdot \ldots \cdot p_k^{nk}$. Diese Prim-Dekomposition ist rekursiv (d.h. berechenbar).

Wir assoziieren mit jedem $x_i \in \mathcal{V}$: 3^i (i = 1, 2,…)

mit jedem $a_i \in \mathcal{C}$: 5^i

für n>0, mit jedem $f_i \in \mathcal{F}_n$: $7^n.11^i$

für jedes n>0, mit jedem $R_i \in \mathcal{R}_n$: $13^n.17^i$ mit ≡ 19

Wir haben 2 vermieden, sodass jede dieser Zahlen ungerade sein wird und nicht 0 enthält.

Zahlen logischer Operatoren: $\neg$ 2, $\vee$ 4, $\wedge$ 6, $\rightarrow$ 8, (12,) 14, $\forall$ 16, $\exists$ 18, ≡ 22, $\vdash$ 24.

Nach dem obigen, arithmetischen Theorem korrespondiert jedes Symbol mit genau einer Zahl, und für jede Zahl ist berechenbar, ob sie ein Symbol bezeichnet, und wenn ja, welches.

Von der Arithmetisierung der Symbole zur Arithmetisierung von Zeichenreihen: wir benutzen die *simple* Methode von Hunter für die AL: wir verwenden 0 für Platz zwischen den Symbolen, und 00 für Platz zwischen Zeichenreihen; Prämissen und Konklusionen von Sequenzen werden auch als Zeichenreihen dargestellt.

Beispiele:

$\forall x_1 F_1{}^1 x_1 \rightarrow F_1{}^1 f_1{}^1 a_1$ 1603022103080221077 05 (Zu beachten: 221 = 13.17, 77 = 7.11)

$\forall x_1 F_1{}^1 x_1 \vdash \forall x_1 F_1{}^1 x_1$: 16030221030024001603022103

$(\forall x_1 F_1{}^1 x_1 \rightarrow F_1{}^1 f_1{}^1 a_1) \vdash (\forall x_1 F_1{}^1 x_1 \rightarrow F_1{}^1 f_1{}^1 a_1)$

16030221030802210770500240016030221030802210 7705

$\forall x_1 F_1{}^1 x_1, (\forall x_1 F_1{}^1 x_1 \rightarrow F_1{}^1 f_1{}^1 a_1) \vdash F_1{}^1 f_1{}^1 a_1$

1603022103001603022103080221077050024002210 7705

So:16030221030024001603022103001603022103080221077050024001603022103 080221077050016030221030016030221030802210770500240022107705 ist die einzigartige Zahl des Beweises eines MP 1. Grades in S*:
$<\{p_1\} \vdash p_1, \{(p_1 \rightarrow p_2)\} \vdash (p_1 \rightarrow p_2), \{p_1, (p_1 \rightarrow p_2)\} \vdash p_2>$.

Anm.: eine zweite Methode beruht auf *Gödels Sequenz-Nummer-Lemma:* gegeben die Zahlen $n_1, \ldots, n_k$, gibt es eine berechenbare Funkiton seq: $|N \times \ldots \times |N \rightarrow |N$, sodass sowohl seq($n_1 \ldots, n_k$), k als auch das n_i ($1 \leq i \leq k$) rückberechenbar (zurückgewinnbar) ist. (Man erhält diese Funktion durch benutzung von Primzahlen.) Die Primzahlmethode ist mathematsich eleganter, aber sie Produziert weit größere Zahlen, als Hunters simple Methode.

$\Rightarrow$ *Abschluss des Beweises:* Für jede natürliche Zahl können wir entscheiden, welche mit einer Zeichenreihe korrespondiert. Dies gibt uns eine Wohlordnung und damit eine Nummerierung von Zeichenreihen.
Für jede $\mathcal{L}$-Zeichenreihe können wir entscheiden, ob sie eine Formel ist. Dies gibt uns eine Nummerierung für Formeln.
Für jede Zahl können wir auch entscheiden, ob sie mit einer Formelsequenz korrespondiert, oder mit einer Sequenz von Sequenzen. Daraus erhalten wir eine Nummerierung aller Sequenzen von Formeln oder Sequenzen
Letztlich können wir von jeder Sequenz von Formeln entscheiden, ob sie ein Beweis in **HL** ist, und für jede Sequenz von Sequenzen können wir entscheiden, ob sie ein Beweis in **S*** ist. Daraus gewinnen wir eine Nummerierung aller Beweise in **HL** oder in **S***.
Q.E.D.

Definition (f.M.E.): Von einer Logik $\mathbf{L} \subseteq \boldsymbol{\mathcal{L}}$ sagt man, dass sie die *finites Modell-Eigenschaft* (fME) hat gdw jede **L**-konsistente Formel A erfüllbar ist, in einem *finiten* Modell für A (wobei die Menge der finiten Modelle als rekursiv nummerierbar angenommen wird.)

Theorem (fME): (1.) Wenn eine Logik **L** fME. hat, sind ihre nicht-Theoreme r.n.
(2.) Wenn eine Logik **L** eine rekursive Axiomatisierung und fME. hat, ist **L** entscheidbar.
Übung 7.12: Beweisen Sie dieses Theorem.

Es gibt keine generellen Entscheidungsmehtoden, um die PL-Gültigkeit zu testen.
PL hat f.M.E. nicht (nicht mal die PL *ohne Identität,* $PL^{\neq}$)

Gegenbeispiel zu fME: Es gibt eine Formel, die sagt, dass R eine strikte Ordnungsrelation ist, ohne größtes Element (R = <):
$\forall x \neg Rxx \wedge \forall x \forall y(Rxy \rightarrow \neg Ryx) \wedge \forall x \forall y \forall z(Rxy \wedge Ryz \rightarrow Rxz) \wedge \forall x \exists y Rxy$
Diese Formel ist konsistent, aber sie ist nur in einem unendlichen Objektbereich erfüllbar.
Gleichermaßen ist die Formel
$[\forall x \neg Rxx \wedge \forall x \forall y(Rxy \rightarrow \neg Ryx) \wedge \forall x \forall y \forall z(Rxy \wedge Ryz \rightarrow Rxz)] \rightarrow \exists x \forall y \neg Rxy$
nur in einem unendlichen Objektbereich erfüllbar und wird von jedem endlichen Objektbereich verifiziert.

Die *monadische PL* - das ist die PL, die nur einstellige Prädikate hat, aber keine Funktionssymbole und kein Identitätssymbol - hat fME und ist daher entscheidbar.

Anm.: einstellige Funktiossymbole sind generell so ausdrucksstark wie binäre Relationssymbole plus Identität.

Heuristiken für semantische Methoden in der PL:

Um eine PL-Formel (einen PL-Schluss) zu wiederlegen, versuche man ein Gegenbeispiel zu konstruieren. Es gibt keine Garantie, eines zu finden, aber für gewöhnlich tut man dies!

Übung 7.13: Widerlegen Sie, durch Konstruktion eines Gegenbeispieles:

$\exists xFx \;\|\!\!\vdash Fa$

$\forall x\exists yRxy \rightarrow \exists y\forall xRxy$

$\forall x(Fx\vee Gx) \;\|\!\!\vdash \forall xFx \vee \forall xGx$

$\exists xFx \wedge\exists xGx \;\|\!\!\vdash \exists x(Fx\wedge Gx)$

Spezielle Methoden:

(1) Methode des finiten Universums: man transformiere PL-Formeln A in AL-Formeln A_0 über einen endlichen Objektbereich, indem man ∀ durch eine Konjunktion über alle Elemente in D ersetzt und ∃ durch eine Disjunktion. Wenn A_0 falsifiziert werden kann, dann kann es auch A; aber nicht notwendigerweise umgekehrt.

(2) Es gibt *Beth Tableaus* für die PL → (siehe Bergman); sie sind nicht entscheidbar, sondern können zu unendlichen Zweigen führen; und ihre Regeln stehen in enger Verbindung mit den Regeln der Sequenzkalküle der PL.

8. Ausblick: Weitere Metatheoreme der PL – oder: der Anfang von Logik III.

8.1 Alternative Axiomatisierungen:

Eine übliche Hilbert-Style Axiomatisierung von **S*1 - HL1:**

Axiomschemata:

(Taut)	Jedes tautologische Schema	
(UI→)	$\forall xA \rightarrow A[x/t]$	(für jedes $x\in\mathcal{V}, t\in\mathcal{T}$)
(∀→)	$\forall x(A \rightarrow B) \rightarrow (\forall xA \rightarrow \forall xB)$	(für jedes $x\in\mathcal{V}$)
(UG→)	$A \rightarrow \forall xA$ vorausgesetzt $x \notin \mathcal{V}_f(A)$	(für jedes $x\in\mathcal{V}$)
(Id)	$\forall x(x\equiv x)$	(für jedes $x\in\mathcal{V}$)
(ExtAt→)	$t_1\equiv t_2 \rightarrow (A[x/t_1] \rightarrow A[x/t_2])$	(für jedes $x\in\mathcal{V}, t_1,t_2\in\mathcal{T}$ und atomares A)

Regeln:

MP

(UGR) $A / \forall xA$ (UG-Regel)

Übung 8.1e: Beweisen Sie, dass ∀→ + UG→ + UGR gemeinsam äquivalent sind mit (UGR'): $B\rightarrow A / B\rightarrow\forall xA$, vorausgesetzt x ist nicht frei in B (im Kontext der anderen Regeln).

Def.: $\vdash_{HL1} A$ gdw es einen Beweis von A in **HL1** gibt, d.h. eine Sequenz $\langle A_1,\ldots,A_n\rangle$, sodass $A = A_n$ und jedes A_i entweder eine Instanz eines der Axiomschemata ist oder aus vorigen Gliedern A_j und möglicherweise A_k ($k, j < i$) nach einer der zwei Regeln folgt.

Warnung! Diese Axiomatisierung definiert ausschließlich **HL1** (HL1-beweisbare Formeln), aber nicht $\vdash_{HL1}$ zwischen Prämissenmenge und Konklusion.

Denn: Die Regel der universellen Generalisierung in **HL1** ist nur zulässig, aber nicht gültig!

- *Definition* (zulässige vs. gültige Regeln): Eine Regel 1. Stufe Γ/A nennt man
- gültig (bezügl. **L**) gdw *sie Wahrheit erhält:* d.h. $\forall v\,(v \models\!= \Gamma \Rightarrow v \models\!= A)$.
- zulässig (bezügl. **L**) gdw *sie Gültigkeit erhält:* $\forall v(v \models\!= \Gamma) \Rightarrow \forall v(v \models\!= A)$.

Anm.: Gültigkeit impliziert Zulässigkeit, aber nicht umgekehrt.

L ist geschlossen unter all ihren zulässigen Regeln, während $\Vdash$ nur alle gültigen Regeln enthält.
--> Zulässige Regeln können bei der Axiomatisierung einer Logik verwendet werden, aber nicht in der Axiomatisierung der (gültigen) Schlussrelation die mit der Logik korrespondiert.

Daher definiert man die Ableitungsrelation $\vdash_{HL1}$ separat, bevorzugt, wie folgt: *Definition:* $\Gamma \vdash_{HL1} A$ gdw $\vdash_{HL1} \bigwedge\Gamma_f \to A$ für irgendein finites $\Gamma_f \subseteq \Gamma$.
Alternativen - cf. Machover .

Theorem: Die $\forall$-Regel (UGR) kann im folgenden Sinne in allen Beweisen weiterentwickelt werden.
Es bezeichne UGR(Γ) den (unendlichen) Schluss von Γ nach der Regel UGR, den Axiomen$_{\mathbf{HL1}}$ (der Menge aller **HL1**-Axiome) und $\vdash_{MP}$ = Ableitung, einzig unter Verwendung von MP. Dann:
(i) $\vdash A$ gdw UGR(Axiome$_{\mathbf{HL1}}$) $\vdash_{MP} A$
(ii) $\Gamma \vdash A$ gdw $\Gamma \cup$ UGR(Axiome$_{\mathbf{HL1}}$) $\vdash_{MP} A$

Beweis: $\Leftarrow$ ist trivial. Für $\Rightarrow$ muss man zeigen
(*) UGR(Axiome$_{\mathbf{HL1}}$) $\vdash_{MP} A \quad\Rightarrow\quad$ UGR(Axiome$_{\mathbf{HL1}}$) $\vdash_{MP} \forall xA$
Dies impliziert, nach Induktion auf die Länge des Beweises von $\vdash A$, dass UGR(Axiome$_{\mathbf{HL1}}$) $\vdash A$.

Übung 8.2: (a) Beweisen Sie (*), durch Induktion auf die Länge des Beweises von UGR(Axiome$_{\mathbf{HL1}}$) $\vdash_{MP}$ A.
(b) Beweisen Sie, unter Benutzung von Theorem (ii), dass die obige Definition von $\Gamma \vdash_{\mathbf{HL1}}$ A äquivalent mit der folgenden ist (benutzt von Bell/Machover, Leblanc):
–– $\Gamma \vdash_{\mathbf{HL1}}$ A gdw es einen Beweis von A aus UGR(Axiome$_{\mathbf{HL1}}$) $\cup$ alleine mit MP gibt.
––– $\Gamma \vdash_{\mathbf{HL1}}$ A gdw es einen Beweis von A aus Axiome$_{\mathbf{HL1}}$ $\cup$ Γ gibt, wobei UGR nur auf Sätze angewandt wird, die nicht von Prämissen in Γ abhängen.

Das Theorem über die Weiterentwicklung der URG-Regel ist wichtig; es hat ein Gegenstück in der Modallogik für die Regel der Notwendigkeitszuschreibung.

Wie in der AL: Die *Korrektheit* von **HL1** wird standardmäßig bewiesen.
Starke Vollständigkeit wird durch die Ableitung essentieller **S*1**-Theoreme bewiesen.

Einige letzte, wichtige Anmerkungen:
Die Ausdrucksstärke der monadischen PL ist vergleichbar mit der AL: wenn es endlich viele monadische Prädikate $F_1,\ldots,F_n$ und Individuenkonstanten $a_1,\ldots,a_m$ gibt, dann gibt es nur endlich viele paarweise nicht-äquivalente Propositionen, die man mit der Sprache ausdrücken kann.

Ersetzung von Funktionssymbolen durch deren relationale Definition in der PL:

Die *Rechtseindeutigkeits-Bedingung* für ein (n+1)-stelliges Relationssymbol R ist die folgende Formel:
$\mathrm{Un}(R) =_{df} \forall x_1\ldots\forall x_n\exists y!Rx_1\ldots x_n y$ d.h.: $\forall x_1\ldots\forall x_n\exists y\forall z(Rx_1\ldots x_n z \leftrightarrow z{\equiv}y)$.

Für $A \in \mathcal{L}$ definieren wir A^R – das Resultat der Elimination der Funktionssymbole von A durch Relationen – wie folgt:

Wir assoziieren mit jedem n-stelligen Funktionssymbol in A genau ein (n+1)-stelliges Relationssymbol R^f.

Dann ersetzen wir in A jede atomare Formel der Form:

$Q^n t_1 \ldots t_{i-1}\, f(x_1,\ldots,x_m)\, t_{i+1} \ldots t_n$ durch

$Q^n t_1 \ldots t_{i-1}\, z\, t_{i+1} \ldots t_n \wedge R^f x_1 \ldots x_m\, z$ für z als *neue* Variable

iterativ, bis alle Funktionssymbole eliminiert worden sind. Wir nennen das Resultat A*.

Es sei:

$A^R := A^* \wedge \bigwedge\{Un(R^f) \mid f \in \mathcal{F}(A)\}$.

Das Resultat der Elimination ist nicht äquivalent, aber es ist co-gültig und co-erfüllbar:

Theorem: $\vdash A \Leftrightarrow \vdash A^R$.

Beweis: Übung:

(i) Beweisen Sie, dass (*) A erfüllbar ist gdw A^R nach dem Theorem, durch Entwicklung von $(\neg A)^R = \neg(A^R)$.

(ii) Bewiesen Sie (*) durch Induktion auf die Komplexität von A.

Inhalt von Logik IV

Weiteres zur axiomatischen Mengenlehre (Ordinal- und Kardinalzahlen)

Prädikatenlogische Theorien in Mathematik und Physik

Limitative Resultate der PL und ihre philosophischen Konsequenzen

(Löwenheim-Skolem, Tarski, Modellisomorphismen, struktureller Realismus)

Gödels Unvollständigkeitssatz

Gödel-Church Unentscheidbarkeitssatz

oder *alternativ:*

Einführung in die Modallogik