Logisch gültige Schlußfolgerungen und Aussagen

Sokrates ist ein Mensch.
Alle Menschen sind sterblich.

Sokrates ist sterblich.

Sokrates ist sterblich.
Sokrates ist ein Mensch.

Alle Menschen sind sterblich.

Wenn jeder Arme einen reichen Vater hat, dann
gibt es einen Reichen mit einem reichen Großvater.

P und Q seien 2-stellige transitive Relationen.
$P \cup Q$ sei total und Q sei symmetrisch.

P ist total oder Q ist total.

Sprache der Prädikatenlogik 1. Stufe (PL1)

Formale Abstraktion der natürlichen,
insbesondere der mathematischen Sprache:

- Alphabet („Symbole“)
- Signatur (Symbole mit Stelligkeiten)
- Wohlgeformte Ausdrücke:
  - Terme
  - Formeln

Alphabet $\mathcal{A}$: Abzählbar unendliche Menge von Objekten („Symbolen"), partitioniert in 6 disjunkte Untermengen:

1. Unendliche Menge $\mathcal{V}$ von Variablen
2. Unendliche Menge $\mathcal{F}$ von Funktionszeichen
3. Unendliche Menge $\mathcal{P}$ von Prädikatszeichen
4. 5-elementige Menge $\mathcal{C} = \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}$ von Junktoren oder Konnektiven: $\neg$ Negationszeichen, $\wedge$ Konjunktionszeichen, $\vee$ Disjunktionszeichen, $\Rightarrow$ Konditionalzeichen, $\Leftrightarrow$ Bikonditionalzeichen.
5. 2-elementige Menge $\mathcal{Q} = \{\forall, \exists\}$ von Quantoren: $\forall$ Allquantor $\exists$ Existenzquantor.
6. 3-elementige Menge $\{(,),,\}$ von Hilfszeichen.

Signatur $\Sigma = \langle \mathcal{A}, \alpha \rangle$: $\mathcal{A}$ Alphabet und $\alpha : \mathcal{F} \cup \mathcal{P} \cup \mathcal{C} \cup \mathcal{Q} \longrightarrow \mathbb{N}_0$ (Stelligkeitsfunktion) mit:

1. Auf jedes $n \in \mathbb{N}_0$ werden unendlich viele Funktions- und Prädikatszeichen aus $\mathcal{A}$ abgebildet.
2. Negationszeichen hat Stelligkeit 1, alle anderen Junktoren und die Quantoren haben Stelligkeit 2.

(Wohlgeformte) Ausdrücke der PL1

<u>Terme</u> $\mathcal{T}$ (induktiv):

1. Alle Variablen sind <u>Terme</u>.
2. Falls f Funktionszeichen mit Stelligkeit $n \geq 0$ und $t_1, \ldots, t_n$ Terme, dann ist $f\,\hat{}\,(\hat{}\,t_1\,\hat{}\,,\hat{}\;\cdots\;\hat{}\,,\hat{}\,t_n\,\hat{}\,)$ (im folgenden kurz: $f(t_1, \cdots, t_n)$) <u>Term</u>.
   Für $a()$ schreiben wir kurz a.

<u>Formeln</u> $\mathcal{F}$ (induktiv):

1. Falls P Prädikatsszeichen mit Stelligkeit $n \geq 0$ und $t_1, \ldots, t_n$ Terme, dann ist $P(t_1, \cdots, t_n)$ <u>(atomare) Formel</u>.
   Für $P()$ schreiben wir kurz P.
2. Falls F und G Formeln, dann sind auch:

   $\neg F$, $(F \wedge G)$, $(F \vee G)$, $(F \Rightarrow G)$, $(F \Leftrightarrow G)$, und

   $\forall x F$, $\exists x F$ <u>Formeln</u>.

Semantik der Prädikatenlogik

Interpretation: Denotationelle Bedeutung von Symbolen

Interpretation $\mathcal{I} = \langle \mathcal{U}, \iota \rangle$:

- $\mathcal{U}$ Universum: Nichtleere Menge von Objekten
- ι Interpretationsfunktion:
  - $\iota(f)$ n-stellige Funktion $f' : \mathcal{U}^n \longrightarrow \mathcal{U}$ $\quad$ (f n-stellig)
  - $\iota(P)$ n-stellige Relation $P' \subseteq \mathcal{U}^n$ $\quad$ (P n-stellig)
    bzw. deren charakteristische Funktion $\Pi(P') : \mathcal{U}^n \longrightarrow \{\top, \bot\}$
    (die letztere Lesart wird im folgenden verwendet)

Variablenzuweisung: Funktion $\mathcal{A} : \mathcal{V} \longrightarrow \mathcal{U}$

... Semantik der Prädikatenlogik

Term-/Formelzuweisung: Erweiterung einer Interpretation $\langle \mathcal{U}, \iota \rangle$ und einer Variablenzuweisung $\mathcal{A}$ auf Ausdrücke

Termzuweisung: $\iota^{\mathcal{A}}(x) = \mathcal{A}(x)$

$\iota^{\mathcal{A}}(f(t_1, \ldots, t_n)) = \iota(f)(\iota^{\mathcal{A}}(t_1), \ldots, \iota^{\mathcal{A}}(t_n))$ (f n-stellig)

Formelzuweisung:

- $\iota^{\mathcal{A}}(P(t_1, \ldots, t_n)) = \iota(P)(\iota^{\mathcal{A}}(t_1), \ldots, \iota^{\mathcal{A}}(t_n))$ (P n-stellig)
- $\iota^{\mathcal{A}}(\neg F) = \top$, falls $\iota^{\mathcal{A}}(F) = \bot$, $\bot$ sonst,
- $\iota^{\mathcal{A}}(F \wedge G) = \top$, falls $\iota^{\mathcal{A}}(F) = \top$ und $\iota^{\mathcal{A}}(G) = \top$, $\bot$ sonst,
- $\iota^{\mathcal{A}}(F \vee G) = \iota^{\mathcal{A}}(\neg(\neg F \wedge \neg G))$,
- $\iota^{\mathcal{A}}(F \Rightarrow G) = \iota^{\mathcal{A}}(\neg F \vee G)$,
- $\iota^{\mathcal{A}}(F \Leftrightarrow G) = \iota^{\mathcal{A}}((F \Rightarrow G) \wedge (G \Rightarrow F))$,
- $\iota^{\mathcal{A}}(\forall x F) = \top$, falls $\iota^{\mathcal{A}_x^u}(F) = \top$ für alle $u \in \mathcal{U}$, $\bot$ sonst (wobei $\mathcal{A}_x^u(x) = u$ und sonst $\mathcal{A}_x^u = \mathcal{A}$)
- $\iota^{\mathcal{A}}(\exists x F) = \iota^{\mathcal{A}}(\neg \forall x \neg F)$.

Modellbegriff der Semantik

<u>**Modell**</u> $\mathcal{M}$ einer Formel F:
Interpretation $\langle \mathcal{U}, \iota \rangle$ mit $\iota^{\mathcal{A}}(F) = \top$ für alle Variablenzuweisungen $\mathcal{A}$

Erweiterung auf Formelmengen S: $\mathcal{M}$ Modell von S,
falls $\mathcal{M}$ Modell für alle Formeln in S.

Formel(menge) S <u>(un)erfüllbar</u>: es gibt (k)ein Modell für S.

13 Formel(menge) S <u>allgemeingültig</u>:
alle Interpretationen für S sind Modelle für S.

Logische Folgerungsbeziehung $S' \models S$: „S folgt logisch aus S'“:
Alle Modelle für S' sind Modelle für S.

$\emptyset \models S$ (kurz $\models S$) bedeutet die Allgemeingültigkeit von S.

S und S' <u>logisch äquivalent</u> (kurz $S \equiv S'$), falls $S \models S'$ and $S' \models S$.

$S \models F$ genau dann, wenn $S \cup \{\neg F\}$ unerfüllbar.

Variablensubstitutionen

(Variablen-)Substitution $\sigma : \mathcal{V} \longrightarrow \mathcal{T}$ derart, daß $\{x \mid \sigma(x) \neq x\}$ (genannt Trägermenge) endlich.

Notation: Für $\sigma(x)$ schreiben wir kurz $x\sigma$.

Angabe einer Substitution durch Trägermenge (sei $t_i = x_i\sigma$):
$\sigma = \{\langle x_1, t_1\rangle, \ldots, \langle x_n, t_n\rangle\}$ oder kürzer: $\{x_1/t_1, \ldots, x_n/t_n\}$

Erweiterung der Anwendung einer Substitutions σ auf beliebige Ausdrücke:
$E\sigma$: Resultat der simultanen Ersetzung jedes freien Vorkommnisses einer Variablen x in E durch $x\sigma$.

Aussagenlogik und Komplexitätstheorie

Aussagenlogik: Lediglich 0-stellige Prädikatszeichen und Konnektive.

Sprachklasse NP: $\mathcal{L} \in$ NP, falls ein festes Polynom p existiert und es für jedes Wort $W \in \mathcal{L}$ einen Nachweis seiner Elementschaft gibt mit der Komplexität $< p(|W|)$ ($|W|$ Komplexität von W).

Präzisierte Definition: (S.A. Cook 1971) Klasse aller Sprachen, die von einem nichtdeterministischen Algorithmus (Turingmaschine) akzeptiert werden in polynomieller Zeit bzgl. der Größe des Inputs.

Sprachklasse P: deterministischer Algorithmus

Eine Sprache $\mathcal{L}$ ist vollständig für eine Sprachklasse K (kurz: K-vollständig), falls es für alle Sprachen in K eine polynomielle Transformation nach $\mathcal{L}$ gibt.

…Aussagenlogik und Komplexitätstheorie

Satz: (Cook 1971) Die Menge aller erfüllbaren aussagenlogischen Formeln ist NP-vollständig. Oder in anderer Sprechweise:
Das Erfüllbarkeitsproblem der Aussagenlogik ist NP-vollständig.

Andere Sprachen/Probleme in NP: Sortiertheit, Graphisomorphismus, Nichtprimzahl, Lineare Programmierung, …

Andere NP-vollständige Sprachen/Probleme:
Klauselsubsumtion, Subgraphisomorphismus, Jobverteilung auf Multiprozessor, Rucksackproblem, Rundreise („Traveling Salesman“), Zahlmengenpartition, …

Literatur zur NP-Vollständigkeit: M.R. Garey und D.S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, New York, 1978.

. . . Aussagenlogik und Komplexitätstheorie

Komplement coK einer Sprachklasse K:

Klasse der Komplementsprachen der Sprachen in K.

Unerfüllbarkeitsproblem und Gültigkeitsproblem der Aussagenlogik sind coNP-vollständig.

Offene Fragen der Komplexitätstheorie:

- P $=$ NP?
- NP $=$ coNP?

Ein Paradoxon der Komplexitätstheorie

NP $\subseteq$ coNP genau dann, wenn coNP $\subseteq$ NP.

Vollständige Junktorenmengen

Menge von Wahrheitsfunktionen $\mathcal{C}$ ist vollständig, falls jede Wahrheitsfunktion $w : \{\top, \bot\}^n \longrightarrow \{\top, \bot\}$ durch $\mathcal{C}$ ausdrückbar.

Vollständige Junktorenmengen sind z.B. $\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \Rightarrow\}$.

Es gibt Junktoren, die allein vollständig sind, z.B. $\mid$ (Sheffer) und $\downarrow$:

$\iota(F \mid G) = \top$, falls $\iota(F) = \bot$ oder $\iota(G) = \bot$, sonst $\bot$.

$\iota(F \downarrow G) = \top$, falls $\iota(F) = \bot$ und $\iota(G) = \bot$, sonst $\bot$.

Literatur: W. Kneale und M. Kneale, The Development of Logic, Clarendon Press, Oxford, 1988^{10}.

Frege/Hilbert Kalküle (Aussagenlogik)

Logikkalkül = Nichtdeterministischer Algorithmus für Gültigkeit (bzw. Unerfüllbarkeit)

Axiomatische Kalküle: Axiome und Inferenzregeln

Beispiel: Kalkül von Lukasiewicz für $\{\neg, \Rightarrow\}$

Axiomenschemata:

$$(A_1) \qquad (\Phi \Rightarrow \Psi) \Rightarrow ((\Psi \Rightarrow \mathrm{X}) \Rightarrow (\Phi \Rightarrow \mathrm{X}))$$

$$(A_2) \qquad (\neg\Phi \Rightarrow \Phi) \Rightarrow \Phi$$

$$(A_3) \qquad \Phi \Rightarrow (\neg\Phi \Rightarrow \Psi)$$

Inferenzregel (Modus Ponens):

$$\frac{\Phi \qquad \Phi \Rightarrow \Psi}{\Psi}$$

Beispielherleitung im Hilbert-Kalkül

Herleitung der Formel $p \Rightarrow p$ im Kalkül von Lukasiewicz:

(1)	$(p \Rightarrow (\neg p \Rightarrow p)) \Rightarrow (((\neg p \Rightarrow p) \Rightarrow p) \Rightarrow (p \Rightarrow p))$	(A_1)
(2)	$p \Rightarrow (\neg p \Rightarrow p)$	(A_3)
(3)	$((\neg p \Rightarrow p) \Rightarrow p) \Rightarrow (p \Rightarrow p)$	(MP 2,1)
(4)	$(\neg p \Rightarrow p) \Rightarrow p$	(A_2)
(5)	$p \Rightarrow p$	(MP 4,3)

Herleitungen in Kalkülen

<u>Herleitung</u> einer Formel F_n im Kalkül K: $\vdash_K F_n$
Folge $F_1, \ldots, F_n$ von Formeln mit: für alle F_k $(1 \leq k \leq n)$
gibt es eine Anwendung einer Inferenzregel (eines Axiomes)

$$\frac{F_{k_1} \cdots F_{k_i}}{F_k} \quad \text{aus } K$$

wobei alle $F_{k_1}, \ldots F_{k_i}$ in der Folge und die Indizes $k_1, \ldots, k_i < k$.

<u>Korrektheit</u> eines Kalküls K: falls $\vdash_K F$, dann $\models F$.

<u>Vollständigkeit</u> eines Kalküls K für eine Sprache $\mathcal{L}$:
für alle $F \in \mathcal{L}$: falls $\models F$, dann $\vdash_K F$.

Satz: Der Kalkül von Lukasiewicz ist korrekt und vollständig
für die Aussagenlogik über den Junktoren $\neg$ und $\Rightarrow$.

Sequenzenkalkül (Aussagenlogik)

„Natürliche“ Kalküle (Gentzen, 1934):

Natürliche Deduktion, **Sequenzenkalkül**

Sequenz: $$\underbrace{F_1, \ldots, F_m}_{\text{Antezedens}} \to \underbrace{G_1, \ldots, G_n}_{\text{Sukzedens}}$$

$\widehat{=}$ $$(F_1 \wedge \cdots \wedge F_m) \Rightarrow (G_1 \vee \cdots \vee G_n)$$

$\widehat{=}$ unter den Annahmen $F_1, \ldots, F_m$ gilt eine der Formeln G_i

Logische Regeln des Sequenzenkalküls

Regelname	Antezedens	Sukzedens
[Axiom]	$\dfrac{}{D \to D}$	
[¬-Einführung]	$\dfrac{\Gamma \to \Theta, A}{\neg A, \Gamma \to \Theta}$	$\dfrac{A, \Gamma \to \Theta}{\Gamma \to \Theta, \neg A}$
[∨-Einführung]	$\dfrac{A, \Gamma \to \Theta \qquad B, \Gamma \to \Theta}{A \vee B, \Gamma \to \Theta}$	$\dfrac{\Gamma \to \Theta, A}{\Gamma \to \Theta, A \vee B}$ $\dfrac{\Gamma \to \Theta, B}{\Gamma \to \Theta, A \vee B}$
[∧-Einführung]	$\dfrac{A, \Gamma \to \Theta}{A \wedge B, \Gamma \to \Theta}$ $\dfrac{B, \Gamma \to \Theta}{A \wedge B, \Gamma \to \Theta}$	$\dfrac{\Gamma \to \Theta, A \qquad \Gamma \to \Theta, B}{\Gamma \to \Theta, A \wedge B}$
[⇒-Einführung]	$\dfrac{\Gamma \to \Theta, A \qquad B, \Delta \to \Lambda}{A \Rightarrow B, \Gamma, \Delta \to \Theta, \Lambda}$	$\dfrac{A, \Gamma \to \Theta, B}{\Gamma \to \Theta, A \Rightarrow B}$

Strukturelle Regeln des Sequenzenkalküls

Regelname	Antezedenz	Sukzedens
[Verdünnung]	$\dfrac{\Gamma \rightarrow \Theta}{\mathsf{D}, \Gamma \rightarrow \Theta}$	$\dfrac{\Gamma \rightarrow \Theta}{\Gamma \rightarrow \Theta, \mathsf{D}}$
[Zusammenziehung]	$\dfrac{\mathsf{D}, \mathsf{D}, \Gamma \rightarrow \Theta}{\mathsf{D}, \Gamma \rightarrow \Theta}$	$\dfrac{\Gamma \rightarrow \Theta, \mathsf{D}, \mathsf{D}}{\Gamma \rightarrow \Theta, \mathsf{D}}$
[Vertauschung]	$\dfrac{\Gamma, \mathsf{D}, \mathsf{E}, \Delta \rightarrow \Theta}{\Gamma, \mathsf{E}, \mathsf{D}, \Delta \rightarrow \Theta}$	$\dfrac{\Gamma \rightarrow \Theta, \mathsf{E}, \mathsf{D}, \Lambda}{\Gamma \rightarrow \Theta, \mathsf{D}, \mathsf{E}, \Lambda}$

[Schnitt]

$$\frac{\Gamma \rightarrow \Theta, \mathsf{D} \qquad\qquad \mathsf{D}, \Delta \rightarrow \Lambda}{\Gamma, \Delta \rightarrow \Theta, \Lambda}$$

Beispielherleitungen im Sequenzenkalkül

$$\dfrac{A \to A}{\to A \Rightarrow A}$$

$$\dfrac{\dfrac{\dfrac{A \to A}{\to A, \neg A}}{\neg\neg A \to A}}{\to \neg\neg A \Rightarrow A}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \to A}{\to A, \neg A}}{\to \neg A, A} \qquad \dfrac{}{B \to B}}{A \Rightarrow B \to \neg A, B}}{A \Rightarrow B \to \neg A, \neg A \vee B}}{A \Rightarrow B \to \neg A \vee B, \neg A}}{A \Rightarrow B \to \neg A \vee B, \neg A \vee B}}{A \Rightarrow B \to \neg A \vee B}}{\to (A \Rightarrow B) \Rightarrow (\neg A \vee B)}$$

Eigenschaften des Sequenzenkalküls

Herleitbarkeit von Formeln F im Sequenzenkalkül: $\vdash_{\mathcal{S}} \rightarrow F$

Herleitungen als Folgen von Sequenzen (analog zu oben) oder als Herleitungsbäume

Schnittfreier Sequenzenkalkül: ohne Schnittregel

Satz: Der (schnittfreie) aussagenlogische Sequenzenkalkül ist korrekt und vollständig ($\vdash_{\mathcal{S}} \rightarrow F$ gdw $\models F$) für die Aussagenlogik über den Junktoren $\neg$, $\wedge$, $\vee$ und $\Rightarrow$.

Aber: Schnittelimination kann zu exponentiellem Anwachsen von Herleitungen führen.

... Eigenschaften des Sequenzenkalküls

Intuitionistische (konstruktive) Herleitung: Nur Sequenzen mit höchstens einer Formel im Sukzedens.

Unterformeleigenschaft:
Gegeben schnittfreie Sequenzen-Herleitung $S_1, \ldots, S_n$:
Alle Formeln in den Sequenzen $S_1, \ldots, S_{n-1}$ sind
Unterformeln der Endsequenz S_n.

Beweissuche im schnittfreien Sequenzenkalkül:
Dekompositiv von der Endsequenz aus

Komprimierung der Kalkülschritte:
Von Listen zu Mengen