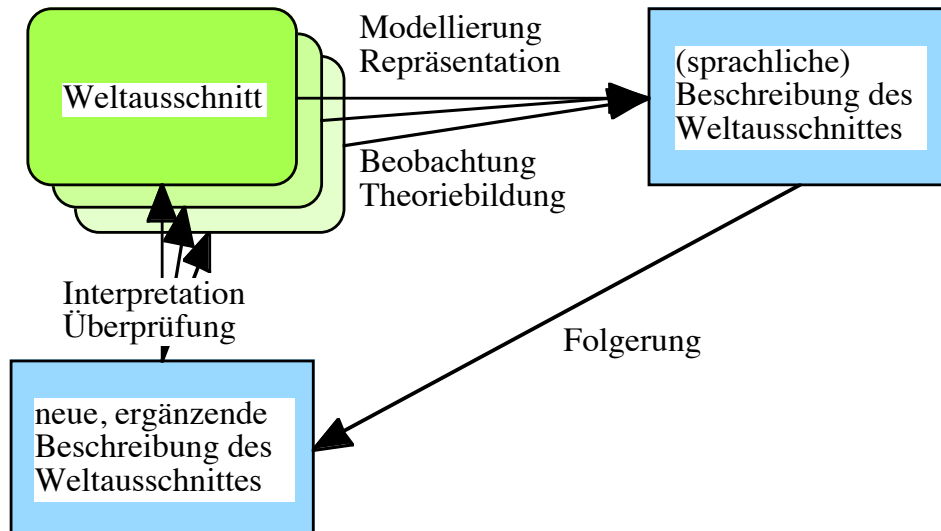


Aussagenlogik: Beweisbarkeit

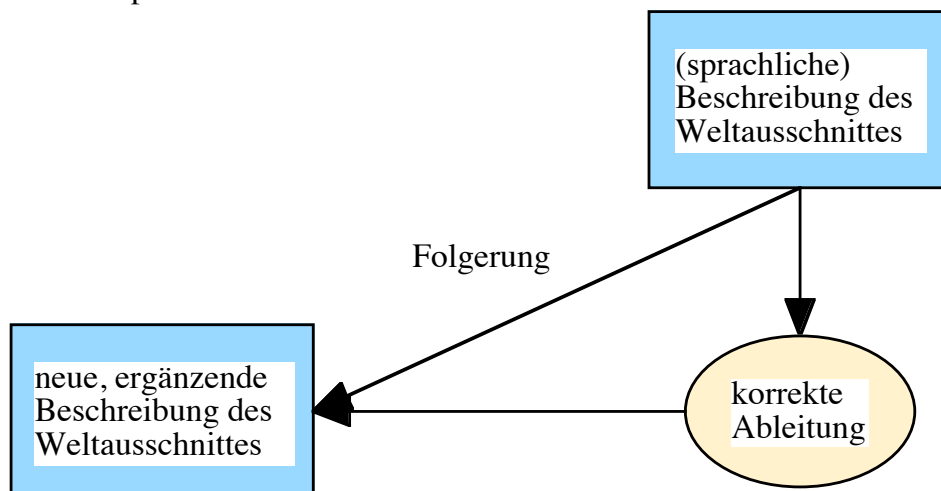
Ableitung und Widerlegung



Beweistheorie

Ableitung und Widerlegung (deduction & refutation)

- Grundidee:
Auf der Basis der syntaktischen Eigenschaften von Formeln und Formelmengen auf ihre semantischen Eigenschaften schließen, statt die Belegungen / Wahrheitswertverläufe der Formeln direkt zu prüfen.



Wenn korrekte Ableitung nichts anderes ist als Folgerung, warum brauchen wir es dann?

- Folgerung ist eine Relation zwischen Formeln, die über die Wahrheitswertverläufe definiert ist. Zur Überprüfung liegt es damit nahe, die Wahrheitstafeln zu verwenden. Dieses Verfahren ist für die Aussagenlogik auch weitgehend praktikabel.
- Für komplexere Logiken ist ein entsprechendes Vorgehen nicht mehr möglich. Z.B. ist es für prädikatenlogische Formeln im allgemeinen nicht möglich, (endliche) Tabellen aufzuschreiben, die alle möglichen Interpretationen aufführen.
- Der Ableitungsbegriff, den wir einführen werden, legt andere Berechnungsverfahren für die logischen Eigenschaften nahe. Vollständigkeit und Korrektheit zeigen, dass diese Verfahren unbesorgt anwendbar sind.
- Ableitungen kann man auch in anderen Logiken definieren und damit dann Folgerungsbeziehungen zwischen Formeln ausrechnen. Die Einführung von Ableitungsverfahren in der Aussagenlogik dient vor allem dazu, das Zusammenspiel der verschiedenen Aspekte an einem einfachen Beispiel vorzustellen. Dieses soll dann die Übertragung auf die Prädikatenlogik erleichtern.

Semantische Eigenschaften und syntaktische Muster: Beispiele

- Unabhängig von der Bedeutung von F gilt:
 - $F \wedge \neg F$ ist unerfüllbar
 - $F \vee \neg F$ ist allgemeingültig

→ Es ist unnötig, die Belegungen zu prüfen, wenn eines dieser syntaktischen Muster vorliegt.
- Entsprechend: Syntaktische Tautologieprüfung bei Klauseln:
Prüfung auf Existenz von komplementären Literalen

- Nutzung von syntaktischen Mustern mit bekannten semantischen Eigenschaften.
- Was sind syntaktische Muster (und wie erkennen wir sie)?

Uniforme (Formel-) Substitution

Definition 6.1 ((Formel-) Substitution)

Eine **(Uniforme Formel-) Substitution** ist eine rekursiv definierte Funktion $\text{sub}: \mathcal{L}_{\text{AL}} \rightarrow \mathcal{L}_{\text{AL}}$.

(s. Prinzip der strukturellen Rekursion)

- Aussagensymbole A_i werden auf Formeln $\text{sub}(A_i)$ abgebildet.

- Für Formeln $F, G \in \mathcal{L}_{\text{AL}}$ gilt:

$$\text{sub}(\neg F) = \neg \text{sub}(F)$$

$$\text{sub}((F \wedge G)) = (\text{sub}(F) \wedge \text{sub}(G))$$

$$\text{sub}((F \vee G)) = (\text{sub}(F) \vee \text{sub}(G))$$

$$\text{sub}((F \Rightarrow G)) = (\text{sub}(F) \Rightarrow \text{sub}(G))$$

$$\text{sub}((F \Leftrightarrow G)) = (\text{sub}(F) \Leftrightarrow \text{sub}(G))$$

- Ist M eine Formelmenge, dann ergibt die Substitution die Formelmenge

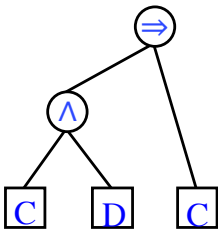
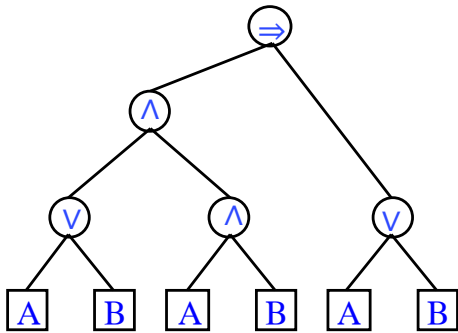
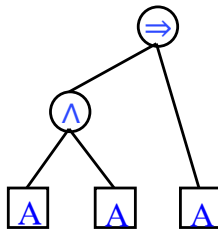
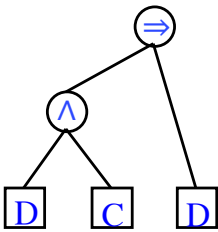
$$\text{sub}(M) = \{\text{sub}(F) \mid F \in M\}$$

→ Durch eine (Formel-)Substitution wird jede Formel F auf eine Formel $\text{sub}(F)$ abgebildet, wobei **jedes** Vorkommen eines Aussagensymbols A_i in F durch die entsprechende Formel $\text{sub}(A_i)$ ersetzt wird.

→ **Uniformität**: Jedes Aussagensymbol wird immer wieder durch die gleiche Formel ersetzt.

→ Die Substitution ist durch die Zuordnung von Formeln zu den Aussagensymbolen eindeutig bestimmt.

Beispiele für Substitutionen

	$\text{sub}_1(C) = (A \vee B)$ $\text{sub}_1(D) = (A \wedge B)$	$\text{sub}_2(C) = A$ $\text{sub}_2(D) = A$	$\text{sub}_3(C) = D$ $\text{sub}_3(D) = C$
$F =$ $(C \wedge D) \Rightarrow C$	$\text{sub}_1(F) =$ $((A \vee B) \wedge (A \wedge B)) \Rightarrow (A \vee B)$	$\text{sub}_2(F) =$ $(A \wedge A) \Rightarrow A$	$\text{sub}_3(F) =$ $(D \wedge C) \Rightarrow D$
			
$M =$ $\{(C \wedge D) \Rightarrow C,$ $(C \wedge D) \Rightarrow D\}$	$\text{sub}_1(M) =$ $\{((A \vee B) \wedge (A \wedge B)) \Rightarrow (A \vee B),$ $((A \vee B) \wedge (A \wedge B)) \Rightarrow (A \wedge B)\}$	$\text{sub}_2(M) =$ $\{(A \wedge A) \Rightarrow A\}$	$\text{sub}_3(M) =$ $\{(D \wedge C) \Rightarrow D,$ $(D \wedge C) \Rightarrow C\}$

Zum Selbststudium: Zusammenhang zwischen Ersetzung und Substitution

Definition 4.8 (Ersetzung) (Umformuliert)

Seien G' und G'' zwei Formeln und sei H' eine Formel mit der Teilformel G' und H'' eine Formel mit Teilformel G'' . Wenn der einzige Unterschied zwischen H' und H'' darin besteht, dass an einer oder mehreren Positionen, an denen in H' die Teilformel G steht in H'' die Teilformel G'' steht, dann heißt H'' *durch Ersetzung von G' durch G'' aus H' hervorgegangen*.

Definition 6.1 ((Formel-) Substitution) (Umformuliert)

Eine *(uniforme Formel-) Substitution* ist eine rekursiv definierte Funktion $\text{sub}: \mathcal{L}_{\text{AL}} \rightarrow \mathcal{L}_{\text{AL}}$.

(s. Prinzip der strukturellen Rekursion)

- Aussagensymbole A_i werden auf Formeln $\text{sub}(A_i)$ abgebildet.
- Für Formeln $F, F' \in \mathcal{L}_{\text{AL}}$ gilt:

$$\text{sub}(\neg F) = \neg \text{sub}(F)$$

$$\text{sub}((F \wedge F')) = (\text{sub}(F) \wedge \text{sub}(F'))$$

$$\text{sub}((F \vee F')) = (\text{sub}(F) \vee \text{sub}(F'))$$

$$\text{sub}((F \Rightarrow F')) = (\text{sub}(F) \Rightarrow \text{sub}(F'))$$

$$\text{sub}((F \Leftrightarrow F')) = (\text{sub}(F) \Leftrightarrow \text{sub}(F'))$$

Beobachtung

Ist H'' durch Ersetzung von G' durch G'' aus H' hervorgegangen, dann gibt es eine Formel H , ein Aussagensymbol A , das nicht in H' oder H'' vorkommt, und zwei Substitutionen sub' und sub'' , so dass gilt: $\text{sub}'(A) = G'$, $\text{sub}''(A) = G''$, für alle Aussagensymbole $B \neq A$ gilt: $\text{sub}'(B) = \text{sub}''(B) = B$ und $\text{sub}'(H) = H'$, $\text{sub}''(H) = H''$.

Substitutionen und Allgemeingültigkeit

Satz 6.2

Wenn eine Formel F allgemeingültig und sub eine Substitution ist, dann ist auch die Formel $G := \text{sub}(F)$ allgemeingültig.

Beweis

- Es sei \mathcal{A} eine Belegung,
 A_1, \dots, A_n seien die in F vorkommenden Aussagensymbole.
- Wir betrachten nun eine Belegung \mathcal{A}' , für die gilt
 $\mathcal{A}'(A_i) = \mathcal{A}(\text{sub}(A_i))$.
 - So eine Belegung gibt es, denn die Aussagensymbole sind kontingente Formeln.
- Es gilt: $\mathcal{A}'(F) = \mathcal{A}(G)$.
[zu zeigen durch strukturelle Induktion über F als Übung]
- Da F allgemeingültig ist, ist $\mathcal{A}'(F) = 1$, also auch $\mathcal{A}(G) = 1$

Vorsicht: die Umkehrung gilt nicht

- Gegenbeispiel: $(A \vee B)$ ist nicht allgemeingültig, aber $(A \vee \neg A)$ ist allgemeingültig.

Sätze 6.3

Es sei sub eine Substitution.

- Wenn eine Formel F unerfüllbar ist, dann ist auch die Formel $\text{sub}(F)$ unerfüllbar.
- Wenn die Formeln F und G äquivalent sind, dann sind auch $\text{sub}(F)$ und $\text{sub}(G)$ äquivalent.
- Wenn eine Formelmenge M unerfüllbar ist, dann ist auch die Formelmenge $\text{sub}(M)$ unerfüllbar.
- Wenn eine Formel F aus einer Formelmenge M folgt, dann folgt auch $\text{sub}(F)$ aus $\text{sub}(M)$.

Beweise: ganz analog zu 6.2 und zur Übung.

Aber zu beachten ist:

- Die Formeln F und $\text{sub}(F)$ sind im Allgemeinen nicht äquivalent !
- Vergleichen Sie Substitutionen mit den spezifischen Voraussetzungen des Ersetzbarkeitstheorems.

Inferenzregel — *Modus Ponens*

Definition 6.4 (Darstellung von Inferenzregeln)

- Es seien F_1, \dots, F_n und G Formeln.
- $R = \frac{F_1, \dots, F_n}{G}$
stellt eine **Inferenzregel** dar,
die F_i werden als **Prämissen**, G wird als **Konklusion** der Regel bezeichnet.
- Eine alternative Schreibweise: $R = F_1, \dots, F_n \therefore G$

Inferenzregeln

- sind keine Formeln der Aussagenlogik.
- spezifizieren Muster in Formelmengen
- sind als Ableitungs- bzw. Schlussfiguren aufzufassen.

Modus Ponens

Modus Ponens ist die Inferenzregel $\text{MP} = \frac{A, A \Rightarrow B}{B}$

Anwendbarkeit einer Inferenzregel

- Inferenzregeln spezifizieren Muster in Formelmengen
- Inferenzregeln sind als Ableitungs- bzw. Schlussfiguren aufzufassen.

Definition 6.5

- Es seien F_1, \dots, F_n und G Formeln und $R = \frac{F_1, \dots, F_n}{G}$ eine Inferenzregel.
- Das Muster F_1, \dots, F_n liegt in einer Formelmenge M genau dann vor, wenn es eine Substitution sub gibt, so dass $\text{sub}(\{F_1, \dots, F_n\}) \subseteq M$
 - Andere Sprechweise: Die Regel R kann auf die Formelmenge M angewendet werden.
- In diesem Fall kann die Formel $\text{sub}(G)$ aus M mit R in einem Schritt abgeleitet werden.
 - Andere Schreib- / Sprechweisen:
 - $\text{sub}(G)$ ist mit R direkt ableitbar aus M
 - $\text{sub}(G)$ ist mit R direkt ableitbar aus $\text{sub}(F_1), \dots, \text{sub}(F_n)$
 - $M \vdash_R \text{sub}(G)$ bzw. $\{\text{sub}(F_1), \dots, \text{sub}(F_n)\} \vdash_R \text{sub}(G)$

Beispiel: Ableitung mit der Inferenzregel Modus Ponens

Modus ponens

$$\frac{A, A \Rightarrow B}{B}$$

- $M_1 = \{A, A \Rightarrow B, A \Rightarrow C\}$
 $\text{sub}_1(A) = A, \text{sub}_1(B) = B$
 $\text{sub}_1(\{A, A \Rightarrow B\}) = \{A, A \Rightarrow B\} \subseteq M_1$
 $M_1 \vdash_{\text{MP}} B$
- $M_1 = \{A, A \Rightarrow B, A \Rightarrow C\}$
 $\text{sub}_2(A) = A, \text{sub}_2(B) = C$
 $\text{sub}_2(\{A, A \Rightarrow B\}) = \{A, A \Rightarrow C\} \subseteq M_1$
 $M_1 \vdash_{\text{MP}} C$
- $M_3 = \{A \wedge B, (A \wedge B) \Rightarrow \neg(C \vee D)\}$
 $\text{sub}_3(A) = A \wedge B, \text{sub}_3(B) = \neg(C \vee D)$
 $\text{sub}_3(\{A, A \Rightarrow B\}) = \{A \wedge B, (A \wedge B) \Rightarrow \neg(C \vee D)\} \subseteq M_3$
 $M_3 \vdash_{\text{MP}} \neg(C \vee D)$

Zum Selbststudium: Regeln und Ableitungen

Wie man hier sieht, gehen den Formalisten schnell die Wörter aus ...

- Regeln gibt es in kontextfreien Grammatiken, mit ihnen werden Wörter aus einem Startsymbol 'abgeleitet', man kann auch sagen 'generiert'.
- (Inferenz-)Regeln gibt es aber auch in logischen Kalkülen, mit ihnen werden Formeln aus Formelmengen 'abgeleitet', man kann auch sagen 'erschlossen'. Beweise sind spezielle Fälle solcher Ableitungen.
- Man sieht hier, wie unterschiedliche Typen von 'Regeln' zu unterschiedlichen Sequenzen von Regelanwendungen führen, die als 'Ableitungen' bezeichnet werden.
- Entsprechende Mehrdeutigkeiten gibt es aber auch in der natürlichen Sprache, man muss einfach akzeptieren, dass das so ist.

Übrigens

- Regeln in kontextfreien Grammatiken haben immer eine 'Prämisse' (ein Non-Terminalsymbol)
- Inferenz-Regeln können mehr oder weniger Prämissen haben. (Inferenzregeln ohne Prämissen sind Axiome). In jedem logischen Kalkül gibt es aber mindestens eine Regel, die zwei Prämissen hat (sehr oft ist das der Modus Ponens).

Korrektheit des Modus Ponens

- Wahrheitsverhalten bei Anwendung des Modus Ponens: $\frac{A, A \Rightarrow B}{B}$

	F	G	$(F \Rightarrow G)$
\mathcal{A}_1	0	0	1
\mathcal{A}_2	0	1	1
\mathcal{A}_3	1	0	0
\mathcal{A}_4	1	1	1

Für alle Belegungen mit $\mathcal{A}(F) = 1$ und $\mathcal{A}(F \Rightarrow G) = 1$ gilt auch $\mathcal{A}(G) = 1$.

→ Modus Ponens erhält Wahrheit.

→ Wenn die Prämissen zu MP wahr sind,
dann ist die Wahrheit der Konklusion garantiert.

- Falls \mathbf{M} eine Formelmenge und $\mathbf{M} \vdash_{\text{MP}} G$, dann $\mathbf{M} \models G$

→ Was durch Modus Ponens aus einer Menge \mathbf{M} abgeleitet werden kann,
ist auch aus \mathbf{M} folgerbar.

Korrektheit von Inferenzregeln

Definition 6.6 (Korrektheit einer Inferenzregel)

Eine Inferenzregel $R = \frac{F_1, \dots, F_n}{G}$ heißt genau dann *korrekt* (sound), falls für alle Formelmengen M und alle Formeln H gilt: wenn $M \vdash_R H$, dann $M \models H$.

→ Was mit einer korrekten Regel aus einer Formelmenge M abgeleitet werden kann, ist auch aus M folgerbar.

Sätze 6.7

- Wenn F_1, \dots, F_n allgemeingültig, R eine korrekte Regel und $\{F_1, \dots, F_n\} \vdash_R G$, dann ist G allgemeingültig.
- Eine Inferenzregel $R = \frac{F_1, \dots, F_n}{G}$ ist genau dann korrekt, wenn $\{F_1, \dots, F_n\} \models G$ gilt.

Beweise zur Übung

Korrekte Inferenzregeln: Beispiele

- Modus tollens (MT):
$$\frac{\neg B, A \Rightarrow B}{\neg A}$$
- Hypothetischer Syllogismus (HS):
$$\frac{A \Rightarrow B, B \Rightarrow C}{A \Rightarrow C}$$
- Konjunktionseinführung (KE):
$$\frac{A, B}{A \wedge B}$$
- Konjunktionslöschung (KL):
$$\frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$
- Disjunktionseinführung (DE):
$$\frac{A}{A \vee B} \qquad \frac{B}{A \vee B}$$
- Disjunktiver Syllogismus (DS):
$$\frac{\neg B, A \vee B}{A} \qquad \frac{\neg A, A \vee B}{B}$$
- Konstruktives Dilemma (KD):
$$\frac{A \Rightarrow B, C \Rightarrow D, A \vee C}{B \vee D}$$

Mehrschrittige Ableitung

Definition 6.8 ($\text{Abl}_{\mathcal{R}}(\mathbf{M})$): Menge der mit \mathcal{R} aus \mathbf{M} ableitbaren Formeln)

- Es sei \mathbf{M} eine Formelmenge und \mathcal{R} eine Menge von Inferenzregeln.
- $\text{Abl}_{\mathcal{R}}^0(\mathbf{M}) := \mathbf{M}$
- $\text{Abl}_{\mathcal{R}}^1(\mathbf{M}) := \mathbf{M} \cup \{F \in \mathcal{L}_{\text{AL}} \mid R \in \mathcal{R} \text{ und } \mathbf{M} \vdash_R F\}$
- $\text{Abl}_{\mathcal{R}}^n(\mathbf{M}) := \text{Abl}_{\mathcal{R}}^{n-1}(\mathbf{M}) \cup \{F \in \mathcal{L}_{\text{AL}} \mid R \in \mathcal{R} \text{ und } \text{Abl}_{\mathcal{R}}^{n-1}(\mathbf{M}) \vdash_R F\}$
- $\text{Abl}_{\mathcal{R}}(\mathbf{M}) := \bigcup_{n \geq 0} \text{Abl}_{\mathcal{R}}^n(\mathbf{M})$
- Ist F Element von $\text{Abl}_{\mathcal{R}}^n(\mathbf{M})$ dann ist F mit \mathcal{R} (in n Schritten) aus \mathbf{M} ableitbar.

Beobachtungen zu 6.8

- Bei mehrschrittigen Ableitungen kann jeder Schritt auf beliebige zuvor eingeführte oder abgeleitete Formeln zugreifen.
- Sind alle Inferenzregeln in \mathcal{R} korrekt, dann ist $\text{Abl}_{\mathcal{R}}(\mathbf{M}) \subseteq \text{Fol}(\mathbf{M})$.

Logik-Kalküle – Inferenzsysteme

Definition 6.9 (Kalkül)

Ein Kalkül C der Aussagenlogik wird gebildet durch:

- Eine Logik-Sprache \mathcal{L}_{AL} ,
spezifiziert durch ein Alphabet und Regeln zur Bildung von wohlgeformten Formeln,
- Eine ausgezeichnete Teilmenge von \mathcal{L}_{AL} , genannt die Axiome von C .
- Eine endliche Menge von Inferenzregeln für \mathcal{L}_{AL} .

→ C kann als Tripel $C = (\mathcal{L}_{\text{AL}}, \mathcal{Ax}, \mathcal{R})$ dargestellt werden:

- (1) Sprache \mathcal{L}_{AL} ,
- (2) Menge von Axiomen \mathcal{Ax} ,
- (3) Menge von Inferenzregeln \mathcal{R}

Ableitung in einem Kalkül

Definition 6.10

Sei C ein Kalkül der Aussagenlogik, M eine Formelmenge und G eine Formel aus \mathcal{L}_{AL} . Eine (nicht-leere) endliche Folge von Formeln F_1, \dots, F_n heißt genau dann eine aussagenlogische **Ableitung** bzgl. C von G aus M , wenn $G = F_n$ und für jedes k ($1 \leq k \leq n$) wenigstens eine der folgenden Bedingungen gilt:

1. $F_k \in M$,
2. $F_k = \text{sub}(H)$, wobei H ein Axiom aus C und sub eine Substitution ist,
3. $\{F_1, \dots, F_{k-1}\} \vdash_R F_k$, wobei R eine Inferenzregel aus C ist.

Gibt es eine Ableitung von G bzgl. C aus M , dann sagen / schreiben wir auch:

- G ist in C **ableitbar** aus M ; $M \vdash_C G$
- $\text{Abl}_C(M) := \{F \in \mathcal{L}_{AL} \mid M \vdash_C F\}$ ist die Menge aller aus M mit C ableitbaren Formeln.

Ableitung: Beispiel

$M := \{A \vee B, (A \vee B) \Rightarrow C, C \Rightarrow D, D \Rightarrow E\}$

Kalkül: $C_0 = (\mathcal{L}_{AL}, \{\}, \{\text{MP}\})$, Regel: MP: $\frac{A, A \Rightarrow B}{B}$

Nr	Formel	Begründung für Aufnahme
(1) $F_1 :=$	$A \vee B$	aus M
(2) $F_2 :=$	$(A \vee B) \Rightarrow C$	aus M
(3) $F_3 :=$	C	(1), (2) MP $\text{sub}_3(A) = (A \vee B), \text{sub}_3(B) = C$
(4) $F_4 :=$	$C \Rightarrow D$	aus M
(5) $F_5 :=$	D	(3), (4) MP $\text{sub}_5(A) = C, \text{sub}_5(B) = D$
(6) $F_6 :=$	$D \Rightarrow E$	aus M
(7) $F_7 :=$	E	(5), (6) MP $\text{sub}_7(A) = D, \text{sub}_7(B) = E$

- $M \vdash_{C_0} E$, E ist aus der Formelmenge M ableitbar.
- Bei dieser Ableitung wurde nicht auf Axiome zurückgegriffen.

Ableitbarkeit – Eigenschaften

Beobachtung 6.11

1. Wenn G ein Axiom von C ist oder $G \in M$, so gilt: $M \vdash_C G$
2. Wenn M_1 und M_2 Formelmengen sind und G eine Formel ist, so gilt für jeden Kalkül C :
Falls $M_1 \subseteq M_2$ und $M_1 \vdash_C G$, dann $M_2 \vdash_C G$. [Monotonie]
3. Wenn M_1 eine Formelmenge und G eine Formel ist, so gilt:
 $M_1 \vdash_C G$ gdw.
eine endliche Teilmenge $M_2 \subseteq M_1$ existiert mit $M_2 \vdash_C G$. [Kompaktheit]

Beweisideen

- zu 1. Länge der Ableitung ist 1, denn schon für $F_1 = G$ kann eine der Bedingungen 1. oder 2. in der Definition von Ableitung erreicht werden.
- zu 2. Wenn eine Ableitung aus M_1 möglich ist, kann die gleiche Ableitung auch gebildet werden, wenn zusätzliche Formeln (aus M_2) zur Verfügung stehen.
- zu 3. Da Ableitungen endlich sind, können auch nur endlich viele Elemente aus M_1 (und auch nur endlich viele Axiome) in der Ableitung von G berücksichtigt werden. Also muss ein endliches $M_2 \subseteq M_1$ ausreichen, um die Ableitung für G aufzubauen.

Axiome – Axiomenmengen

Axiom

αξίωμα Ein Satz, der keines Beweises bedarf.
Ein logischer Satz, den kein Vernünftiger bezweifelt. (Euklid)

Axiome für die Aussagenlogik

- Die Idee: Formeln der Aussagenlogik, „die keines Beweises bedürfen“.
- Eine Basismenge von Tautologien um weitere Tautologien abzuleiten.

Beweisbarkeit: Ableitbarkeit aus der leeren Menge (Definition 6.12)

Eine Formel G , für die gilt $\emptyset \vdash_C G$, heißt *beweisbar* in C . (in Zeichen: $\vdash_C G$)

- Beweisbare Formeln werden auch als *Theoreme* von C bezeichnet.
- Eine Ableitung, die nur Axiome und Regeln von C verwendet, heißt auch *formaler Beweis in C* .
 - Beweise sind nicht „Ableitungen aus dem Nichts“.
 - ➔ „ableitbar ausschließlich aus den Axiomen, ohne Bezug auf weitere Formeln“

Hilbert-Systeme

- Klasse aussagenlogischer Kalküle, die ausschließlich den Modus Ponens als Inferenzregel verwenden.

Unterschiede existieren in der Festlegung der Axiome.

- Modus Ponens: $\frac{A, A \Rightarrow B}{B}$
- Axiome für das System \mathcal{H}
 - $H_1 := (A \Rightarrow (B \Rightarrow A))$
 - $H_2 := ((A \Rightarrow B) \Rightarrow ((A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)))$
 - $H_3 := (A \Rightarrow (B \Rightarrow (A \wedge B)))$
 - $H_{4a} := (A \Rightarrow (A \vee B))$
 - $H_{4b} := (B \Rightarrow (A \vee B))$
 - $H_5 := ((A \Rightarrow B) \Rightarrow ((A \Rightarrow \neg B) \Rightarrow \neg A))$
 - $H_{6a} := ((A \wedge B) \Rightarrow A)$
 - $H_{6b} := ((A \wedge B) \Rightarrow B)$
 - $H_7 := ((A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C)))$
 - $H_8 := (\neg\neg A \Rightarrow A)$

Die Axiome von \mathcal{H}

Beispiel

- $(A \Rightarrow (B \Rightarrow A))$ stellt durch Substitutionen u.a. die folgenden Formeln bereit:
 - $(A \Rightarrow (B \Rightarrow A)),$
 - $(A \Rightarrow (A \Rightarrow A)),$
 - $(B \Rightarrow (A \Rightarrow B)),$
 - $(A \Rightarrow (C \Rightarrow A))$
 - $((A \vee B) \Rightarrow (C \Rightarrow (A \vee B))),$
 - $((A \wedge B) \Rightarrow (C \Rightarrow (A \wedge B))), \dots$
- Unterschiedliche Axiomenmengen des Hilbert-Stils sind u.a. durch unterschiedliche Basissätze von Junktoren ('Junktorenbasen') bedingt.

Beweisbeispiel in \mathcal{H}

- $H_1 \quad (A \Rightarrow (B \Rightarrow A))$
- $H_2 \quad ((A \Rightarrow B) \Rightarrow ((A \Rightarrow (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)))$

Satz 6.13: $\vdash_{\mathcal{H}} \mathbf{D} \Rightarrow \mathbf{D}$

Beweis

Nr.	Formaler Beweis	Begründung für die Aufnahme
(1) $F_1 :=$	$(D \Rightarrow (D \Rightarrow D)) \Rightarrow ((D \Rightarrow ((D \Rightarrow D) \Rightarrow D)) \Rightarrow (D \Rightarrow D))$	Axiom H_2 $\text{sub}_1(A) = D$ $\text{sub}_1(B) = (D \Rightarrow D)$ $\text{sub}_1(C) = D$
(2) $F_2 :=$	$(D \Rightarrow (D \Rightarrow D))$	Axiom H_1 $\text{sub}_2(A) = D$, $\text{sub}_2(B) = D$
(3) $F_3 :=$	$((D \Rightarrow ((D \Rightarrow D) \Rightarrow D)) \Rightarrow (D \Rightarrow D))$	(1), (2) MP $\text{sub}_3(A) = (D \Rightarrow (D \Rightarrow D))$ $\text{sub}_3(B) = ((D \Rightarrow ((D \Rightarrow D) \Rightarrow D)) \Rightarrow (D \Rightarrow D))$
(4) $F_4 :=$	$(D \Rightarrow ((D \Rightarrow D) \Rightarrow D))$	Axiom H_1 $\text{sub}_4(A) = D$ $\text{sub}_4(B) = (D \Rightarrow D)$
(5) $F_5 :=$	$(D \Rightarrow D)$	(3), (4) MP $\text{sub}_5(A) = (D \Rightarrow ((D \Rightarrow D) \Rightarrow D))$ $\text{sub}_5(B) = (D \Rightarrow D)$

Formale Beweise vs. ‚normale‘ Beweise

Formaler Beweis	‚normale‘ Beweise
$(D \Rightarrow (D \Rightarrow D)) \Rightarrow ((D \Rightarrow ((D \Rightarrow D) \Rightarrow D)) \Rightarrow (D \Rightarrow D))$ $(D \Rightarrow (D \Rightarrow D))$ $((D \Rightarrow ((D \Rightarrow D) \Rightarrow D)) \Rightarrow (D \Rightarrow D))$ $(D \Rightarrow ((D \Rightarrow D) \Rightarrow D))$ $(D \Rightarrow D)$ <ul style="list-style-type: none"> • weisen immer alle Details aus • sind algorithmisch prüfbar • sind für Menschen nicht verständlich • verschleiern Beweisideen 	<ul style="list-style-type: none"> • machen größere Schritte • benutzt andere Sätze und Hilfssätze • benutzen verschiedene Inferenzregeln • sind korrekt, wenn sich die einzelnen Schritte als formale Beweise rekonstruieren lassen • können sich in ihrer Detaillierung nach dem Ansprechpartner richten • sind verständlich, wenn die richtige Detaillierung gewählt wurde • können zwischen ‚Beweisidee‘ und Beweisausführung unterscheiden

Definition 6.14: Korrektheit & Vollständigkeit

Ein aussagenlogischer Kalkül C heißt genau dann

- **a-korrekt** (ableitungskorrekt), falls für alle Formelmengen M und alle Formeln G gilt: wenn $M \vdash_C G$, dann $M \models G$ (Also $\text{Abl}_C(M) \subseteq \text{Fol}(M)$)
- **b-korrekt** (beweiskorrekt), falls für alle Formeln G gilt: wenn $\vdash_C G$, dann $\models G$. (Also $\text{Abl}_C(\{\}) \subseteq \text{Taut}_{AL}$)
- **a-vollständig** (ableitungsvollständig), falls für alle Formelmengen M und alle Formeln G gilt: wenn $M \models G$, dann $M \vdash_C G$. (Also $\text{Fol}(M) \subseteq \text{Abl}_C(M)$)
- **b-vollständig** (beweisvollständig), falls für alle Formeln G gilt: wenn $\models G$, dann $\vdash_C G$. (Also $\text{Taut}_{AL} \subseteq \text{Abl}_C(\{\})$)

Beobachtung zu 6.14

- Jeder a-korrekte Kalkül ist b-korrekt und jeder a-vollständige Kalkül ist b-vollständig.
- Ein b-vollständiger Kalkül, der die Regel Modus Ponens enthält, ist a-vollständig.
- Ein b-korrekt Kalkül ist a-korrekt, wenn für ihn das Deduktionstheorem gilt.
→ Für logische Kalküle wird üblicherweise nachgewiesen:
Deduktionstheorem (→6.15), B-Korrektheit, B-Vollständigkeit, Verfügbarkeit von MP

Zum Selbststudium

Vollständigkeit und Korrektheit

- Normalerweise werden diese Begriffe einfach verwendet, ohne a- oder b-Zusatz. Gemeint ist dann meistens a-Korrektheit und a-Vollständigkeit. Wir haben die Unterscheidung hier getroffen, um den Stellenwert des Deduktionstheorems deutlicher zu machen.

Widerlegungskalküle

- Verschiedene Beweisverfahren, z.B. Resolution (kommt noch in dieser Vorlesung) und Tableau-Verfahren (Masterstudium: FGI-3) sind vorwiegend dazu geeignet, festzustellen, ob eine Formelmenge erfüllbar ist oder nicht.
- Diese Verfahren sind in der Regel nicht a- oder b-vollständig, aber wir haben ja schon gesehen, wie man Folgerbarkeits- und Tautologiefragen in Erfüllbarkeitsfragen umwandeln kann.

Ein aussagenlogischer Kalkül C heißt genau dann

- **w-korrekt** (widerlegungskorrekt), falls für alle Formelmengen M und eine Kontradiktion K gilt: wenn $M \vdash_C K$, dann ist M unerfüllbar.
- **w-vollständig** (widerlegungsvollständig), falls für alle Formelmengen M und eine Kontradiktion K gilt: wenn M unerfüllbar ist, dann $M \vdash_C K$.

Deduktionstheorem für \mathcal{H}

Satz 6.15 (Deduktionstheorem für \mathcal{H})

Seien \mathbf{M} eine Formelmenge und \mathbf{F} und \mathbf{G} Formeln mit $\mathbf{M} \cup \{\mathbf{F}\} \vdash_{\mathcal{H}} \mathbf{G}$,

dann gilt: $\mathbf{M} \vdash_{\mathcal{H}} \mathbf{F} \Rightarrow \mathbf{G}$

- Speziell für $\mathbf{M} = \emptyset$: Wenn $\{\mathbf{F}\} \vdash_{\mathcal{H}} \mathbf{G}$, dann $\vdash_{\mathcal{H}} \mathbf{F} \Rightarrow \mathbf{G}$.
- Wenn \mathbf{G} ableitbar ist aus den Annahmen \mathbf{M} und \mathbf{F} , dann ist aus \mathbf{M} ableitbar: $\mathbf{F} \Rightarrow \mathbf{G}$.
- Das Deduktionstheorem stellt die systematische Beziehung zwischen Ableitbarkeit (Relation zwischen Formeln) und Implikation (Junktor) her.

Struktur des Beweises

Sei $\mathbf{G}_1, \dots, \mathbf{G}_n$ eine Ableitung von \mathbf{G} aus $\mathbf{M} \cup \{\mathbf{F}\}$; es gilt also: $\mathbf{G}_n = \mathbf{G}$.

Beweis erfolgt durch vollständige Induktion über i , d.h. es wird für alle Schritte der Ableitung gezeigt: Wenn $\mathbf{M} \cup \{\mathbf{F}\} \vdash_{\mathcal{H}} \mathbf{G}_i$, dann $\mathbf{M} \vdash_{\mathcal{H}} \mathbf{F} \Rightarrow \mathbf{G}_i$ für $1 \leq i \leq n$.

Dafür nehmen wir die Ableitung von $\mathbf{G}_1, \dots, \mathbf{G}_n$ und formen sie zu Ableitungen für $\mathbf{F} \Rightarrow \mathbf{G}_i$ um.

Beweis des Deduktionstheorems (1)

Induktionsanfang: $i = 1$: Ein-Schritt Ableitungen aus $\mathbf{M} \cup \{\mathbf{F}\}$

- \mathbf{G}_1 ist Axiom: Wir ergänzen die Ableitung wie folgt

(1)	\mathbf{G}_1	Axiom	wie zuvor
(1.1)	$\mathbf{G}_1 \Rightarrow (\mathbf{F} \Rightarrow \mathbf{G}_1)$	Axiom \mathbf{H}_1	$\text{sub}_{1.1}(\mathbf{A}) = \mathbf{G}_1$, $\text{sub}_{1.1}(\mathbf{B}) = \mathbf{F}$
(1.2)	$\mathbf{F} \Rightarrow \mathbf{G}_1$	(1), (1.1) MP	$\text{sub}_{1.2}(\mathbf{A}) = \mathbf{G}_1$, $\text{sub}_{1.2}(\mathbf{B}) = (\mathbf{F} \Rightarrow \mathbf{G}_1)$

- $\mathbf{G}_1 \in \mathbf{M}$: Wir ergänzen die Ableitung wie folgt

(1)	\mathbf{G}_1	aus \mathbf{M}	wie zuvor
(1.1)	$\mathbf{G}_1 \Rightarrow (\mathbf{F} \Rightarrow \mathbf{G}_1)$	Axiom \mathbf{H}_1	$\text{sub}_{1.1}(\mathbf{A}) = \mathbf{G}_1$, $\text{sub}_{1.1}(\mathbf{B}) = \mathbf{F}$
(1.2)	$\mathbf{F} \Rightarrow \mathbf{G}_1$	(1), (1.1) MP	$\text{sub}_{1.2}(\mathbf{A}) = \mathbf{G}_1$, $\text{sub}_{1.2}(\mathbf{B}) = (\mathbf{F} \Rightarrow \mathbf{G}_1)$

- $\mathbf{G}_1 = \mathbf{F}$: Wir können obige 5-schrittige Ableitung für $\mathbf{D} \Rightarrow \mathbf{D}$ umformen, indem wir an Stelle von \mathbf{D} überall \mathbf{F} einsetzen.

(1.5)	$\mathbf{F} \Rightarrow \mathbf{F}$		
-------	-------------------------------------	--	--

Beweis des Deduktionstheorems (2)

Induktionsannahme

- Bedingungen des Theorems erfüllt für alle $i < m$

Induktionsschritt

- Drei Fälle können auftreten:
 - G_m ist ein Axiom \rightarrow Behandlung wie Induktionsanfang
 - $G_m \in M$ oder $G_m = F \rightarrow$ Behandlung wie Induktionsanfang
 - G_m ergibt sich durch MP aus G_i und $G_k = (G_i \Rightarrow G_m)$ ($i, k < m$)
 Nach der Induktionsannahme gibt es Ableitungen für $(F \Rightarrow G_i)$ und für $(F \Rightarrow G_k)$
- In der Ableitung also schon enthalten

(i.n)	$F \Rightarrow G_i$...
(k.n')	$F \Rightarrow (G_i \Rightarrow G_m)$...

- Ergänzung um

(m.1)	$(F \Rightarrow G_i) \Rightarrow ((F \Rightarrow (G_i \Rightarrow G_m)) \Rightarrow (F \Rightarrow G_m))$	Axiom H_2
(m.2)	$(F \Rightarrow (G_i \Rightarrow G_m)) \Rightarrow (F \Rightarrow G_m)$	(i.n) (m.1) MP
(m.3)	$F \Rightarrow G_m$	(k.n') (m.2) MP

Zum Selbststudium: Ergänzung

Hier ergänzend die Substitutionen,

- die nicht in die Tabelle passten.

(m.1)	$(F \Rightarrow G_i) \Rightarrow ((F \Rightarrow (G_i \Rightarrow G_m)) \Rightarrow (F \Rightarrow G_m))$	Axiom H_2 $\text{sub}_{m.1}(A) = F,$ $\text{sub}_{m.1}(B) = G_i,$ $\text{sub}_{m.1}(C) = G_m$
(m.2)	$(F \Rightarrow (G_i \Rightarrow G_m)) \Rightarrow (F \Rightarrow G_m)$	(i.n) (m.1) MP $\text{sub}_{m.2}(A) = (F \Rightarrow G_i),$ $\text{sub}_{m.2}(B) = (F \Rightarrow (G_i \Rightarrow G_m)) \Rightarrow (F \Rightarrow G_m)$
(m.3)	$F \Rightarrow G_m$	(k.n') (m.2) MP $\text{sub}_{m.3}(A) = (F \Rightarrow (G_i \Rightarrow G_m)),$ $\text{sub}_{m.3}(B) = F \Rightarrow G_m$

Satz 6.16: Korrektheitstheorem für \mathcal{H}

- Der Hilbertkalkül \mathcal{H} ist korrekt (a-korrekt und b-korrekt).

Ohne Beweis an dieser Stelle. Es reicht zu zeigen, dass die Axiome wirklich Tautologien sind, auf die Korrektheit des Modus Ponens zu verweisen und damit b-Korrektheit zu begründen. Das Deduktionstheorem 6.15 liefert dann a-Korrektheit.

Satz 6.17: Vollständigkeitstheorem für \mathcal{H}

- Der Hilbertkalkül \mathcal{H} ist vollständig (a-vollständig und b-vollständig).

Ohne Beweis an dieser Stelle.

→ Es gibt Kalküle für die Aussagenlogik, die vollständig und korrekt sind.

Andere Kalküle der Aussagenlogik

Weitere Deduktionssysteme

- Natürliches Schließen
 - Sequenzen-Kalkül
 - Gentzen-Kalkül
- (werden beispielhaft im Masterstudium in FGI-3 behandelt.)

Widerlegungssysteme

- Zielsetzung: Verfahren, die die syntaktische Struktur von Formeln berücksichtigen, um Mengen von Formeln als unerfüllbar nachzuweisen. (→ Inkonsistenz)
 - Tableau-Systeme (Wird im Masterstudium in FGI-3 behandelt.)
- Resolution (wird in Kap. 8 behandelt für die Aussagenlogik und in Kap. 11 für die Prädikatenlogik behandelt.)

Zur Ergänzung: Konsistenz und Inkonsistenz – Definition

Definitionen 6.18

1. Eine Menge von zwei Formeln $\{F, \neg F\}$ heißt *Kontradiktionspaar* oder *Paar komplementärer Formeln*.
2. Eine Formelmenge M heißt genau dann *inkonsistent* bzgl. eines Kalküls C ($M \vdash_C$), falls beide Elemente eines Kontradiktionspaars aus M mit C ableitbar sind, d.h. es gibt eine Formel F , so dass sowohl $M \vdash_C F$ als auch $M \vdash_C \neg F$ gilt. Anderenfalls heißt M *konsistent* bzgl. C .

Zur Ergänzung: Inkonsistenz – Unerfüllbarkeit

Satz 6.19

Wenn M inkonsistent bzgl. eines a-korrekten Kalküls ist, dann ist M unerfüllbar.

Beweis

- Wenn M inkonsistent bzgl. C ist, dann gibt es F mit: $M \vdash_C F$ und $M \vdash_C \neg F$.
- Da Ableitbarkeit mit C korrekt ist, gilt: $M \models F$ und $M \models \neg F$.
- Wäre M erfüllbar, müsste es eine Belegung geben, die sowohl F als auch $\neg F$ wahr macht, aber dies widerspricht der Definition für Belegungen (3.1).
- Also ist M unerfüllbar.

Satz 6.20

Wenn M unerfüllbar und C ein a-vollständiger Kalkül ist, dann ist M inkonsistent bzgl. C .

Beweis

- Da M unerfüllbar ist, folgt jede Formel aus M , also auch die Formeln A und $\neg A$.
- Da Ableitbarkeit mit C vollständig ist, gilt: $M \vdash_C A$ und $M \vdash_C \neg A$.

Wichtige Konzepte in diesem Foliensatz

- (Uniforme Formel-) Substitution (in der Prädikatenlogik werden wir noch einen anderen Typ von Substitution kennen lernen: Uniforme Variablen-Substitution)
- Inferenzregel, allgemein und als wichtiges Beispiel den Modus Ponens
 - Anwendbarkeit einer Inferenzregel, Ableitbarkeit mit einer Inferenzregel
 - Korrektheit einer Inferenzregel
- Kalkül
 - Axiom, Ableitung in einem Kalkül, (formaler) Beweis in einem Kalkül
 - Korrektheit und Vollständigkeit eines Kalküls
 - Konsistenz, Inkonsistenz bzgl. eines Kalküls
 - Hilbert-System als Beispiel für einen Kalkül
 - Deduktionstheorem (für den Hilbert-Kalkül)