Logik und Berechenbarkeit

Vorlesung von Sophie Frisch

Vorlesungsmitschrift verfasst von Maria Eichlseder im WS 2008/09. Version 29. April 2009.
Fehlerfunde bitte melden an `maria.eichlseder@student.tugraz.at`.

Inhaltsverzeichnis

Kapitel 1

Aussagenlogik (Sentential Logic)

1.1 Sprache der Aussagenlogik

Alphabet mit abzählbar vielen aussagenlogischen Variablen, Junktoren und Klammern,

$$\mathcal{B} = \{A_i \mid i \in \mathbb{Z}\} \cup \{\neg, \vee, \wedge, \rightarrow, \leftrightarrow, |\} \cup \{(,)\}$$

Definiere daraus die Sprache

$$\mathcal{B}^* = \{\text{Wörter mit Buchstaben aus } \mathcal{B}\}$$

Dabei ist ein Wort ein String endlicher Länge, das leere Wort ε ist zugelassen.

$\mathcal{A}$, die Sprache der Aussagenlogik, ist definiert als Teilmenge von $\mathcal{B}^*$ induktiv durch

1. $\forall\, i:\ A_i \in \mathcal{A}$
2. $A, B \in \mathcal{A} \ \Rightarrow\ (\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A|B) \in \mathcal{A}$

Bedeutung dieser induktiven Definition: Allgemeine Teilmenge T einer Menge S induktiv definieren heißt Angabe einer Liste von Relationen, wobei T definiert ist als der Durchschnitt aller Teilmengen von S, die bezüglich dieser Relationen abgeschlossen sind. Wenn $R \subseteq S \times \ldots \times S = S^n$ n-stellige Relation auf S ist, dann heißt $M \subseteq S$ abgeschlossen bezüglich R, wenn $\forall\, m_1, \ldots, m_n \in S$ mit $m_1, \ldots, m_{n-1} \in M$ und $(m_1, \ldots, m_{n-1}, m_n) \in R$ gilt: $m_n \in M$.

Am Beispiel der aussagenlogischen Sprache $\mathcal{A}$ ist $S = \mathcal{B}^*$, und $\mathcal{A}$ ist definiert als Durchschnitt aller Teilmengen von $\mathcal{B}^*$, die abgeschlossen bezüglich folgender Relationen sind:

1. $R_a \subseteq \mathcal{B}^*$: $w \in R_a :\Leftrightarrow w \in \{A_i \mid i \in \mathbb{N}\}$. Abgeschlossenheit bezüglich einer einstelligen Relation heißt einfach, dass jene Elemente, die die Relation erfüllen, in $\mathcal{A}$ sind. $(m_1, \ldots, m_{n-1} \in \mathcal{A}, (m_1, \ldots, m_n) \in R \ \Rightarrow\ m_n \in R$, im Fall $n = 1$ gibt es keine $m_1, \ldots, m_{n-1}$, daher $m_1, \ldots, m_{n-1} \in \mathcal{A}$ "leer erfüllt")
2. $R_\neg = \{(B, (\neg B)) \mid B \in \mathcal{B}^*\}$, $R_\wedge = \{(A, B, (A \wedge B)) \mid A, B \in \mathcal{B}^*\}$ etc.

Umgangssprachliche Abkürzungen für aussagenlogische Formeln:

- Äußerste Klammer weglassen: $\neg A$ steht für $(\neg A)$, $A \vee B$ für $(A \vee B)$ etc
- Bindungsstärke: $\neg$ bindet stärker als alle anderen Junktoren, dh. $\neg A \vee B$ steht für $((\neg A) \vee B)$ (und eben nicht $(\neg(A \vee B))$). $\wedge, \vee$ binden stärker als $\rightarrow, \leftrightarrow$, dh. $A \wedge B \rightarrow C$ steht für $((A \wedge B) \rightarrow C)$.

Das sind ausschließlich umgangssprachliche Abkürzungen, keine Formeln $\in \mathcal{A}$, wenn man Formeln als formale Ausdrücke behandelt vorher die weggelassenen Klammern eintragen.

Andere Art, die Sprache der Aussagenlogik zu definieren: Postfix- und Prefix-Notation. Hier Postfix-Notation (Vorteil: keine Klammern, Nachteil: nicht optimal human readable).

Definition 1.1: $\mathcal{A}_P$ ist definiert als Teilmenge von $\mathcal{B}^*$, $\mathcal{B} = \{A_i \mid i \in \mathbb{N}\} \cup \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, |\}$ durch

1. $\forall\, i \in \mathbb{N}:\ A_i \in \mathcal{A}_P$
2. $A, B \in \mathcal{A}_P \ \Rightarrow\ A\neg, AB\wedge, AB\vee, AB\rightarrow, AB\leftrightarrow, AB| \in \mathcal{A}_P$

Anmerkung (Strukturelle Induktion)*:* Wenn eine Menge M induktiv definiert ist, dann kann man Aussagen für jedes $m \in M$ beweisen, indem man eine Induktion entlang der induktiven Struktur (in der Definition von M) führt, dh. man zeigt:

1. Für alle Elemente, die die einstelligen Relationen in der Definition von M erfüllen: diese Elemente erfüllen die Aussage.
2. Für alle n-stelligen ($n > 1$) Relationen in der Definition von M: wenn $m_1, \ldots, m_{n-1}$ jeweils die Aussage erfüllen und $(m_1, \ldots, m_{n-1}, m_n) \in R$, dann erfüllt m_n die Aussage.

Andere Formulierung: damit alle $m \in M$ die Aussage X erfüllen, genügt es, zu zeigen: $\forall R$ Relation, die in der induktiven Definition von M vorkommen: wenn $m_1, \ldots, m_{n-1}$ X erfüllen und $(m_1, \ldots, m_{n-1}, m_n) \in R$, dann erfüllt auch m_n die Aussage X. (Punkt 1 betreffend der einstelligen Relationen wird bei dieser Formulierung von Induktion auch erledigt, da für einstellige R die Aussage, $m_1, \ldots, m_{n-1}$ erfüllen X, "leer erfüllt" ist und man Aussage X für jene m mit $m \in R$ ohne Vorbedingung zeigen muss).

Beweis (Beweis, dass diese Induktion funktioniert)*:* Sei $M \subseteq S$ induktiv definiert, N Menge der $s \in S$, für die die Aussage X gilt. Angenommen, dass $\forall R$ in der Definition von M gilt "$(m_1, \ldots, m_n) \in R$ und $m_1, \ldots, m_{n-1} \in N$ dann auch $m_n \in N$". Zu zeigen ist dann $M \subseteq N$. Das ist klar, da $N \subseteq S$ und N bezüglich allen Relationen in der Definition von M abgeschlossen ist,

$$M = \bigcap_{L \text{ abgeschlossen}} L$$

N kommt unter den Mengen L, als deren Durchschnitt M definiert ist, vor, also $N \supseteq M = \bigcap L$
□

Übung: In jeder Formel $\in \mathcal{A}$ kommen gleich viele "(" wie ")" vor, in jedem echten nichttrivialen Anfangsabschnitt mehr "(".

Definition 1.2 (Anfangsabschnitt)**:** Der Anfangsabschnitt eines Wertes $b_1 b_2 \ldots b_n$ ist ein Ausdruck der Gestalt $b_1 b_2 \ldots b_k$ für $k \leq n$. Der Abschnitt ist nichttrivial, wenn $k > 0$, dh. der Abschnitt ist nicht ε. Der Abschnitt ist echt, falls $k < n$, dh. der Abschnitt ist nicht das ganze Wort.

Korollar 1.1: Kein echter Anfangsabschnitt einer aussagenlogischen Formel $\in \mathcal{A}$ (Version mit Klammern) ist selbst eine Formel der Aussagenlogik.

Proposition 1.2: Jede Formel $\in \mathcal{A}$ erfüllt die "eindeutige Lesbarkeit" in Bezug auf obige induktive Definition von $\mathcal{A}$, dh. für jede aussagenlogische Formel F gilt genau einer der Fälle

1. $F = A_i$ für ein $i \in \mathbb{N}$
2. $F = (\neg A)$ für ein $A \in \mathcal{A}$
3. $F = (A \star B)$ für $A, B \in \mathcal{A}$ und $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow, |\}$

und im Fall 1 ist i, im Fall 2 ist A, im Fall 3 sind A, B und $\star$ eindeutig bestimmt.

Beweis: (Beweis der eindeutigen Lesbarkeit von Formeln $\in \mathcal{A}$ in Bezug auf die induktive Struktur in der Definition). Zu zeigen: Für jede Formel $B \in \mathcal{A}$ gilt genau einer der drei Fälle:

1. $B = A_i$ für ein $i \in \mathbb{N}$ (aussagenlogische Variable)
2. $B = (\neg C)$ für eine Formel $C \in \mathcal{A}$
3. $B = (C \star D)$ für Formeln $C, D \in \mathcal{A}$ und Junktor $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow, |\}$

und in Fall 1 ist i eindeutig bestimmt, in Fall 2 ist C eindeutig, in Fall 3 C, D und $\star$.

Jede Formel $\in \mathcal{A}$ ist von dieser Gestalt (überlegen).

Fall 1 und 2, 3 schließen sich gegenseitig aus. Verwenden dazu Lemma: kein echter, nichttrivialer Anfangsabschnitt einer Formel $\in \mathcal{A}$ ist selbst Formel $\in \mathcal{A}$ (weil: jede Formel $\in \mathcal{A}$ hat gleich viele rechte wie linke Klammern; jeder echte Anfangsabschnitt hat echt mehr linke Klammern). Daraus folgt: im Fall 3 sind $C, D, \star$ eindeutig bestimmt, denn angenommen $B = (C \star D) = (E \circ F)$ mit $C, D, E, F \in \mathcal{A}$, $\star, \circ$ Junktoren. $\star$ sei k-ter Buchstabe, $\circ$ ℓ-ter Buchstabe. Wenn $k = \ell$, dann $\star = \circ$, $C = E$, $D = F$. Wenn $k < \ell$, dann ist C echter Anfangsabschnitt von E, geht nicht wegen Anzahl der Klammern.

Im Fall 2 ist C sowieso eindeutig.

Fälle 2, 3 schließen sich aus, da keine Formel $\in \mathcal{A}$ mit $\neg$ anfängt. □

1.2 Wahrheitsfunktionen für Formeln

Proposition 1.3: Sei $M \subseteq S$ induktiv definiert und erfülle eindeutige Lesbarkeit. Dann kann man eine Funktion $f : M \rightarrow N$ (N beliebige Menge) definieren, indem man

1. für alle $m \in M$, die eine einstellige Relation in der Definition von M erfüllen, einen Wert $f(m) \in N$ angibt und
2. Für jede n-stellige Relation, $n > 1$, in der induktiven Definition von M eine Vorschrift angibt, wie man für $m_1, \ldots, m_n \in S$ mit $(m_1, \ldots, m_n) \in R$ aus bekannten $f(m_1), \ldots, f(m_{n-1})$ den Wert $f(m_n)$ berechnet.

Beispiel: Wahrheitsfunktionen für Formeln der Aussagenlogik aus Belegungen der aussagenlogischen Variablen berechnen.

Definition 1.3: Eine Belegung ist eine Funktion $b : \{A_i \mid i \in I\} \rightarrow \{0, 1\}$, wobei $I \subseteq \mathbb{N}$. Eine Belegung ist vollständig, wenn $I = \mathbb{N}$.

Den Junktoren werden folgende Funktionen zugeordnet:

$$\Phi_\neg : \{0,1\} \rightarrow \{0,1\}, \qquad \Phi_\neg(x) = \begin{cases} 1 & x = 0 \\ 0 & x = 1 \end{cases}$$

$$\Phi_\wedge : \{0,1\} \times \{0,1\} \rightarrow \{0,1\}, \qquad \Phi_\wedge(x,y) = \begin{cases} 1 & x = y = 1 \\ 0 & \text{sonst} \end{cases}$$

$$\Phi_\vee : \{0,1\} \times \{0,1\} \rightarrow \{0,1\}, \qquad \Phi_\vee(x,y) = \begin{cases} 0 & x = y = 0 \\ 1 & \text{sonst} \end{cases}$$

$$\Phi_\rightarrow : \{0,1\} \times \{0,1\} \rightarrow \{0,1\}, \qquad \Phi_\rightarrow(x,y) = \begin{cases} 0 & x = 1, y = 0 \\ 1 & \text{sonst} \end{cases}$$

$$\Phi_\leftrightarrow : \{0,1\} \times \{0,1\} \to \{0,1\}, \qquad \Phi_\leftrightarrow(x,y) = \begin{cases} 1 & x = y \\ 0 & \text{sonst} \end{cases}$$

$$\Phi_| : \{0,1\} \times \{0,1\} \to \{0,1\}, \qquad \Phi_|(x,y) = \begin{cases} 0 & x = y = 1 \\ 1 & \text{sonst} \end{cases}$$

Vollständige Belegung b zu Funktion $\overline{b} : \mathcal{A} \to \{0,1\}$ fortsetzen durch induktive Definition,

1. Funktionswerte für aussagenlogische Variablen sind durch b gegeben, für $i \in \mathbb{N}$ ist $\overline{b}(A_i) = b(A_i)$.
2. für $F = (\neg A)$ mit $A \in \mathcal{A}$ sei $\overline{b}(F) = \Phi_\neg(\overline{b}(A))$ und für $\star \in \{\wedge, \vee, \to, \leftrightarrow, |\}$ und $F = (A \star B)$ ist $\overline{b}(F) = \Phi_\star(\overline{b}(A), \overline{b}(B))$.

Die früher bewiesene eindeutige Lesbarkeit ausnützend, haben wir für jede Funktion $b : \{A_i \mid i \in \mathbb{N}\} \to \{0,1\}$ eine Fortsetzung $\overline{b} : \mathcal{A} \to \{0,1\}$ definiert. Dadurch definiert jede Formel $A \in \mathcal{A}$ eine Funktion $f_A : \mathcal{B} \to \{0,1\}$, wobei $\mathcal{B}$ die Menge aller Belegungen der Variablen A_i mit Wahrheitswerten, dh. $\mathcal{B} = \{b \mid b : \{A_i \mid i \in \mathbb{N}\} \to \{0,1\}\}$, nämlich $f_A(b) = \overline{b}(A)$. Man sieht leicht, dass $\overline{b}(A)$ nur von $b(A_1), \ldots, b(A_n)$ abhängt, wenn in A keine Variablen außer $A_1, \ldots, A_n$ vorkommen. Daher definiert $A \in \mathcal{A}$, in der außer $A_1, \ldots, A_n$ keine Variablen vorkommen, eine Funktion $f_A : \{b : \{A_1, \ldots, A_n\} \to \{0,1\}\} \to \{0,1\}$. Alle vollständigen Belegungen c, die auf $A_1, \ldots, A_n$ mit b übereinstimmen, haben denselben Wert bei A: $b(A_i) = c(A_i)$ für $i = 1, \ldots, n$, dann ist $\overline{b}(A) = \overline{c}(A)$ und wir definieren für $\tilde{b} : \{A_1, \ldots, A_n\} \to \{0,1\}$, $\tilde{\overline{b}}(A) = \overline{b}(A)$, b beliebige vollständige Belegung mit $b(A_i) = \tilde{b}(A_i)$, $i = 1, \ldots, n$.

Definition 1.4: $A, B \in \mathcal{A}$ heißen äquivalent ($A \Leftrightarrow B$), wenn $f_A = f_B$, dh. wenn für jede Belegung b gilt $\overline{b}(A) = \overline{b}(B)$.

Beispiel: Es ist $(A_1 \to A_2) \Leftrightarrow ((\neg A_1) \vee A_2)$.

A_1	A_2	$(A_1 \to A_2)$	$((\neg A_1) \vee A_2)$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Ebenfalls ist $A = ((A_1 \to A_2) \wedge (A_3 \vee (\neg A_3))) \Leftrightarrow (A_1 \to A_2) = B$. Betrachte f_A, f_B auf einer Obermenge der in A, B vorkommenden Variablen.

Definition 1.5 (Tautologie, Kontradiktion, Erfüllbarkeit)**:** Eine Formel $A \in \mathcal{A}$ heißt Tautologie, wenn $f_A(b) = 1$ für jede Belegung $b : \{A_i \mid i \in \mathbb{N}\} \to \{0,1\}$. A heißt Kontradiktion (unerfüllbar), wenn $f_A(b) = 0$ für alle Belegungen b. A heißt erfüllbar, wenn A keine Kontradiktion ist.

Beispiel (Tautologien)*:*

- Tertium non datur: $(A \vee (\neg A))$, $A \in \mathcal{A}$
- $(\neg(A \wedge (\neg A)))$
- Kontraposition: $((A \to B) \leftrightarrow ((\neg B) \to (\neg A)))$

Proposition 1.4: $A, B \in \mathcal{A}$, dann ist $(A \leftrightarrow B)$ Tautologie genau dann, wenn $A \Leftrightarrow B$.

Beweis: Angenommen $A \leftrightarrow B$ Tautologie, dh. $\forall b : \overline{b}(A \leftrightarrow B) = 1$, dh. $\forall b : \Phi_\leftrightarrow(\overline{b}(A), \overline{b}(B)) = 1$ wegen der Definition von $\Phi_\leftrightarrow$, nämlich

$$\Phi_\leftrightarrow(x,y) = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$$

äquivalent: $\forall b : \overline{b}(A) = \overline{b}(B)$, dh. $A \Leftrightarrow B$. □

Einige Äquivalenzen:

- Assoziativität von $\wedge$: $((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$, analog für $\vee$
- Kommutativität von $\wedge$: $(A \wedge B) \Leftrightarrow (B \wedge A)$, analog für $\vee$
- De Morgan: $(\neg(A \wedge B) \Leftrightarrow ((\neg A) \vee (\neg B))$, analog $(\neg(A \vee B)) \Leftrightarrow ((\neg A) \wedge (\neg B))$

Wegen der Assoziativität von $\vee$ und $\wedge$ sind alle Formeln $\in \mathcal{A}$, die eine Konjunktion von $B_1, \ldots, B_n$ in dieser Reihenfolge sind, mit beliebiger Klammerung äquivalent: schreiben $B_1 \wedge B_2 \wedge \cdots \wedge B_n$ als Abkürzung für $(((B_1 \wedge B_2) \wedge B_3) \ldots)$.

1.3 Normalformen

Definition 1.6 (Literal, Klausel, Normalform)**:** Ein Literal ist eine Formel der Gestalt A_i oder $(\neg A_i)$ (A_i Variable).

Eine Klausel ist eine Formel der Gestalt $B_1 \vee B_2 \vee \ldots \vee B_n$ für ein $n \in \mathbb{N}$, wobei jedes B_i ein Literal ist. Analog ist eine duale Klausel von der Gestalt $B_1 \wedge B_2 \wedge \ldots \wedge B_n$.

Eine duale n-Klausel ist eine Klausel der Gestalt $B_1 \wedge \ldots \wedge B_n$, wobei für $i = 1, \ldots, n$ B_i entweder A_i oder $(\neg A_i)$ ist. Analog ist eine n-Klausel von der Gestalt $B_1 \vee B_2 \vee \ldots \vee B_n$.

Eine Formel ist in disjunktiver Normalform, wenn sie von der Gestalt $C_1 \vee C_2 \vee \ldots \vee C_k$ mit C_i eine duale Klausel ist. Sie ist in disjunktiver n-Form, wenn jedes C_i eine duale n-Klausel ist und $C_i \neq C_j$ für $i \neq j$. Analog ist eine konjunktive Normalform (n-Form) von der Gestalt $C_1 \wedge C_2 \wedge \ldots \wedge C_k$ mit C_i Klausel (n-Klausel).

Beispiel: Disjunktive 2-Form: $(A_1 \wedge (\neg A_2)) \vee ((\neg A_1) \wedge (\neg A_2))$, disjunktive Normalform: $A_1 \vee (A_2 \wedge A_3) \vee ((\neg A_1) \wedge A_3)$

Anmerkung: Jede Formel, in der außer $A_1, \ldots, A_n$ keine weiteren Variablen vorkommen, ist äquivalent zu einer disjunktiven Normalform. Wenn sie erfüllbar ist (dh. keine Kontradiktion), dann ist sie äquivalent zu einer disjunktiven n-Form. Diese disjunktive n-Form ist eindeutig bis auf Reihenfolge der dualen Klauseln.

Ebenso ist jede Formel äquivalent zu einer konjunktiven Normalform, und wenn es keine Tautologie ist, dann zu einer konjunktiven n-Form.

Bildung der Formen aus Min- bzw. Maxtermen (Wahrheitstabelle).

Definition 1.7 (Subformel einer Formel $B \in \mathcal{A}$)**:** Für $B = A_i$ ist nur A_i selbst eine Subformel von B. Für $B = (\neg C)$ ist die Menge der Subformeln von C gegeben durch $\{B\} \cup \{\text{Subformeln von } C\}$. Für $B = (C \star D)$ ist die Menge der Subformeln $\{B\} \cup \{\text{Subformeln von } C\} \cup \{\text{Subformeln von } D\}$.

Proposition 1.5: Wenn man in $A \in \mathcal{A}$ eine Subformel C durch eine äquivalente Formel C' (dh. $C \Leftrightarrow C'$) ersetzt erhält man eine zu A äquivalente Formel.

Beweis: Induktion nach der Struktur von A:

- Fall $A = A_i$: einzige Subformel A_i durch C' mit $C' \Leftrightarrow A_i$ ersetzen: Man erhält C', wobei $C' \Leftrightarrow A_i = A$ nach Voraussetzung.

- Fall $A = (\neg C)$: Subformel A ersetzen durch C' mit $C' \Leftrightarrow A$ erhält $C' \Leftrightarrow A$ ✓. Subformel C_1 von C ersetzen durch $C' \Leftrightarrow C_1$: nach Induktionsvoraussetzung erhält man $A' = (\neg D')$ mit $D \Leftrightarrow C$. Dann gilt für jede Belegung b

  $$\overline{b}(A') = \Phi_\neg(\overline{b}(D)) = \Phi_\neg(\overline{b}(C)) = \overline{b}(A)$$

  weil $D \Leftrightarrow C$ definiert ist durch $\forall b : \overline{b}(C) = \overline{b}(D)$.

- Fall $A = (C \star D)$: ganz A ersetzen wie in obigen Fällen. Ersetzen Subformel C_1 von C durch C_2 mit $C_1 \Leftrightarrow C_2$. Nach Induktionsvoraussetzung ist das Ergebnis des Ersetzens von C_1 durch C_2 in C eine zu C äquivalente Formel E. Zu zeigen ist: Wenn A' das Ergebnis der Ersetzung von C_1 durch C_2 in A ist, dann ist $A' \Leftrightarrow A$, für alle Belegungen b:

  $$\overline{b}(A') = \Phi_\star(\overline{b}(E), \overline{b}(D)) = \Phi_\star(\overline{b}(C), \overline{b}(D)) = \overline{b}(A)$$ □

Proposition 1.6: Sei A Tautologie, $B_1, \ldots, B_n \in \mathcal{A}$. Dann ist $A[A_1/B_1, \ldots, A_n/B_n]$ Tautologie.

Anmerkung (Notation)*:* $A[A_1/B_1, \ldots, A_n/B_n]$ bezeichnet das Ergebnis des Einsetzens von B_i in jedes Vorkommnis von A_i (einmalig und gleichzeitig, nicht rekursiv).

Beweis (Beweisskizze zur Proposition)*:* Sei $f_{A'}$ die Wahrheitsfunktion von $A[A_1/B_1, \ldots, A_n/B_n]$ eine Funktion in den Variablen $A_1, \ldots, A_m$ mit $m \geq n$, und m so groß, dass in $B_1, \ldots, B_n$ keine Variablen außer $A_1, \ldots, A_m$ vorkommen,

$$f_{A'}(A_1, \ldots, A_m) = f_A(f_{B_1}(A_1, \ldots, A_m), f_{B_2}(A_1, \ldots, A_m), \ldots, f_{B_n}(A_1, \ldots, A_m), A_{n+1}, \ldots, A_m)$$

Die Funktion ist konstant 1, da f_A konstant 1 ist. □

Anmerkung (Vollständigkeit von Teilsprachen von $\mathcal{A}$)*:* Sei $\mathcal{B} = \mathcal{A}_I$ die Teilmenge von $\mathcal{A}$ bestehend aus jenen Formeln, in denen keine Junktoren außer jenen aus $I \subseteq \{\wedge, \vee, \rightarrow, \leftrightarrow, |, \neg\}$ vorkommen. $\mathcal{B}$ heißt vollständig, wenn $\forall A \in \mathcal{A}\ \exists B \in \mathcal{B}$ mit $B \Leftrightarrow A$. Wir wissen aus der Existenz von konjunktiven (bzw. disjunktiven) Normalformen, dass $A_{\{\neg,\wedge,\vee\}}$ vollständig ist.

Übung: $\mathcal{A}_{\{\neg,\wedge\}}$ und $\mathcal{A}_{\{\neg,\vee\}}$ sind vollständig, $\mathcal{A}_{\{\wedge,\vee,\rightarrow,\leftrightarrow\}}$ hingegen nicht.

Definition 1.8: $A \Rightarrow B$, B ist Folgerung von A (für $A, B \in \mathcal{A}$) ist definiert durch: Für alle Belegungen b mit $\overline{b}(A) = 1$ gilt $\overline{b}(B) = 1$.

Übung: Aus der KNF von A lassen sich leicht die KNF von allen Folgerungen von A bestimmen, analog aus der DNF.

Kapitel 2

Topologie und Kompaktheitssatz

Definition 2.1: Eine Menge von Formeln $\mathcal{B} \subseteq \mathcal{A}$ heißt erfüllbar, wenn $\exists b$ Belegung mit $\forall B \in \mathcal{B} : \bar{b}(B) = 1$. $\mathcal{B}$ heißt unerfüllbar, wenn $\forall b \, \exists B \in \mathcal{B} : \bar{b}(B) \neq 1$.

Satz 2.1 (Kompaktheitssatz)**:** Sei $\mathcal{B} \subseteq \mathcal{A}$. Wenn $\mathcal{B}$ unerfüllbar ist, dann existiert eine endliche Teilmenge $\{B_1, \ldots, B_n\} \subseteq \mathcal{B}$, die unerfüllbar ist. Äquivalent: Wenn jede endliche Teilmenge von $\mathcal{B}$ erfüllbar ist, dann ist auch $\mathcal{B}$ erfüllbar.

Anmerkung: Dieser Satz gilt auch, wenn man in die Definition von $\mathcal{A}$ statt einer abzählbar unendlichen Menge von Variablen $\{A_i \mid i \in \mathbb{N}\}$ eine überabzählbare Menge von Variablen $\{A_i \mid i \in I\}$, I beliebig groß, verwendet.

2.1 Topologie

Definition 2.2 (Topologie)**:** Sei X eine Menge. Eine Topologie von X ist ein $\tau \subseteq \mathcal{P}(X)$, so dass gilt:

1. $\emptyset, X \in \tau$
2. $\forall i \in I : U_i \in \tau$ (I beliebige Indexmenge), dann gilt $\bigcup_{i \in I} U_i \in \tau$
3. $U, W \in \tau \Rightarrow U \cap W \in \tau$

Die Elemente von τ nennt man "offene" Teilmengen von X. (X, τ) heißt topologischer Raum.

Beispiel: (X, d) metrischer Raum hat durch d definierte Topologie:

$$U \in \tau \Leftrightarrow \forall u \in U \, \exists \varepsilon > 0 : B_\varepsilon(u) \subseteq U$$

Definition 2.3: (X, τ) topologischer Raum. $A \subseteq X$ heißt abgeschlossen, wenn $X \setminus A$ offen ist, dh. $(X \setminus A) \in \tau$.

Anmerkung: Sei (X, τ) topologischer Raum. Sei α die Menge der abgeschlossenen Mengen,

$$\alpha = \{A \subseteq X \mid (X \setminus A) \in \tau\}$$

Dann gilt

1. $\emptyset, X \in \alpha$
2. $\forall i \in I : A_i \in \alpha \Rightarrow \bigcap_{i \in I} A_i \in \alpha$

3. $A, B \in \alpha \Rightarrow A \cup B \in \alpha$

Man kann durch Angabe von $\alpha \subseteq \mathcal{P}(X)$ mit 1, 2, 3 eine Topologie τ auf X definieren durch

$$\tau = \{U \subseteq X \mid (X \setminus U) \in \alpha\}$$

Definition 2.4: Sei (X, τ) topologischer Raum. $\mathcal{B} \subseteq \tau$ heißt Basis der Topologie τ, wenn

$$\forall U \in \tau \; \exists \{B_i \mid i \in I\} \subseteq \mathcal{B} : U = \bigcup_{i \in I} B_i$$

Beispiel: In $\mathbb{R}^n$ ist eine (abzählbare) Basis der durch die Euklidische Metrik d gegebenen Topologie

$$\mathcal{B} = \{B_{1/r}(x) \mid r \in \mathbb{N}, x \in \mathbb{Q}^n\}$$

Anmerkung: Sei X Menge, $\mathcal{B} \subseteq \mathcal{P}(X)$, so dass

1. $\emptyset, X \in \mathcal{B}$
2. $U, W \in \mathcal{B} \Rightarrow U \cap W \in \mathcal{B}$

Dann ist auf X eine Topologie definiert durch

$$U \in \tau \Leftrightarrow \{B_i \mid i \in I\} \subseteq \mathcal{B}, \quad U = \bigcup_{i \in I} B_i$$

und $\mathcal{B}$ ist eine Basis dieser Topologie τ.

Definition 2.5 (Produkttopologie)**:** Seien für $i \in I$ (I beliebige Indexmenge) X_i topologische Räume. Dann ist auf dem kartesischen Produkt $\prod_{i \in I} X_i$ die Produkttopologie definiert durch Angabe einer Basis $\mathcal{B}$, nämlich $B \in \mathcal{B}$ genau dann, wenn $\exists i_1, \ldots, i_n \in I$ und $U_{i_1}, \ldots, U_{i_n}$ mit U_{i_j} offen $\subseteq X_{i_j}$ ($U_{i_j} \in \tau_{i_j}$), so dass $b = (b_i)_{i \in I} \in B$ genau dann, wenn für $j = 1, \ldots, n$, $b_{i_j} \in U_{i_j}$,

$$B = X_1 \times U_2 \times X_3 \times U_4 \times \ldots \times X_i$$

B ist definiert durch: für endlich viele Koordinaten muss $b_i \in U_i$ sein, alle anderen Koordinaten ohne Einschränkung.

Definition 2.6 (Karthesisches Produkt)**:** Karthesisches Produkt, zB Produkt von endlich vielen Mengen,

$$X_1 \times X_2 \times \ldots \times X_n = \prod_{i=1}^{n} X_i = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i\}$$

Für eine Menge von X_i, indiziert mit $i \in I$, I beliebige Indexmenge, ist

$$\prod_{i \in I} X_i = \{(x_i)_{i \in I} \mid x_i \in X_i\}$$

die Menge der "Auswahlfunktionen"

$$f : I \to \bigcup_{i \in I} X_i$$

Funktion mit $f(i) \in X_i$ für alle $i \in I$.

Kürzen eine Auswahlfunktion f durch die Liste ihrer Werte ab: $(x_i)_{i\in I}$ steht für f mit $f(i) = x_i \in X_i$.

In $\prod X_i$ kann man "Quader" definieren durch

$$\prod_{i\in I} Y_i \subseteq \prod_{i\in I} X_i$$

wenn für jedes i eine Teilmenge $Y_i \subseteq X_i$ gegeben ist, dann sei

$$\prod_{i\in I} Y_i = \{(x_i)_{i\in I} \mid x_i \in Y_i \forall i\}$$

2.2 Kompaktheit

Definition 2.7 (Kompaktheit)**:** $S \subseteq X$, (X, τ) topologischer Raum. S heißt kompakt :$\Leftrightarrow$ Aus

$$S \subseteq \bigcup_{i\in I} O_i$$

mit O_i offen für alle i folgt: $\exists i_1, \ldots, i_n \in I$, so dass

$$S \subseteq O_{i_1} \cup O_{i_2} \cup \ldots \cup O_{i_n}$$

Dh. jede offene Überdeckung von S hat eine endliche Teilüberdeckung.

Beispiel: Jede endliche Teilmenge eines beliebigen topologischen Raums ist kompakt.

Beispiel: $S \subseteq \mathbb{R}^n$ (euklidische Metrik) ist genau dann kompakt, wenn S beschränkt ($\exists B_r(0)$ mit $S \subseteq B_r(0)$) und abgeschlossen ist.

Anmerkung: S ist kompakt $\Leftrightarrow$ Aus

$$S \cap \bigcap_{i\in I} A_i = \emptyset$$

mit A_i abgeschlossen für alle i folgt $\exists i_1, \ldots, i_n \in I$, so dass

$$S \cap (A_{i_1} \cap \ldots \cap A_{i_n}) = \emptyset$$

Entspricht Anwendung des Komplements auf obige Definition.

Satz 2.2 (Satz von Tychonoff)**:** Seien X_i für $i \in I$ beliebig viele kompakte topologische Räume, dann ist auch

$$\prod_{i\in I} X_i$$

mit Produkttopologie kompakt.

Anmerkung (Produkttopologie)*:* Die offenen Mengen sind genau die Vereinigungen von "offenen Basismengen". Eine offene Basismenge ist eine Menge der Form (für eine endliche Menge $\{i_1, \ldots, i_n\} \subseteq I$)

$$O = O_{i_1} \times O_{i_2} \times \ldots \times O_{i_n} \times \prod_{i\in I\setminus\{i_1,\ldots,i_n\}} X_i$$

für O_{i_k} offen $\subseteq X_{i_k}$.

Anmerkung: Gegensatz dazu ist Boxtopologie. Offene Basismengen

$$\prod_{i \in I} O_i = \{(x_i)_{i \in I} \mid \forall i : x_i \in O_i\}$$

mit O_i offen $\subseteq X_i$. Damit würde Tychonoff nicht funktionieren.

Anwendung des Satzes von Tychonoff auf Aussagenlogik:

Für $A \subseteq \mathcal{A}$ sei

$$\Delta(A) = \{b : \{A_i \mid i \in \mathbb{N}\} \to \{0,1\} \mid \overline{b}(A) = 1\} \subseteq \prod_{i \in \mathbb{N}} \{0,1\}$$

Menge der Belegungen (Funktionen $\{A_i \mid i \in \mathbb{N}\} \to \{0,1\}$ als Produktraum)

$$\{0,1\}^{\mathbb{N}} = \prod_{i \in \mathbb{N}} \{0,1\}$$

auffassen durch

$$b \mapsto (b(A_i))_{i \in \mathbb{N}}$$

Es gilt $A \Leftrightarrow B$ (nach Definition genau dann, wenn $\forall b : \overline{b}(A) = \overline{b}(B)$) genau dann, wenn

$$\Delta(A) = \Delta(B)$$

Das ergibt eine Äquivalenzrelation. Betrachten Menge der Äquivalenzklassen von Formeln in $\mathcal{A}$. Jeder Klasse $\overline{A}$ kann man zuordnen $\Delta(\overline{A}) = \Delta(A)$, ist wohldefiniert, denn: Sei $B \in \overline{A}$, dh. $B \Leftrightarrow A$, dann $\Delta(B) = \Delta(A)$.

Eine Formel A ist erfüllbar genau dann, wenn $\Delta(A) \neq \emptyset$. Eine Menge von Formeln $\mathcal{C} \subseteq \mathcal{A}$ heißt erfüllbar, wenn $\exists b$ Belegung, so dass $\forall C \in \mathcal{C} : \overline{b}(C) = 1$. Das ist äquivalent zu

$$\bigcap_{c \in \mathcal{C}} \Delta(C) \neq \emptyset$$

Satz 2.3 (Kompaktheitssatz der Aussagenlogik)**:** $\mathcal{C} \subseteq \mathcal{A}$ ist erfüllbar genau dann, wenn jede endliche Teilmenge $\mathcal{C}' = \{C_1, \ldots, C_k\} \subseteq \mathcal{C}$ erfüllbar ist.

Variante, äquivalent: Wenn $\mathcal{C} \subseteq \mathcal{A}$ unerfüllbar ist, dann $\exists \mathcal{C}'$ endlich, $\mathcal{C}' \subseteq \mathcal{C}$, mit $\mathcal{C}'$ unerfüllbar. Wenn also

$$\bigcap_{C \in \mathcal{C}} \Delta(C) = \emptyset$$

dann existieren $C_1, \ldots, C_n \in \mathcal{C}$, so dass

$$\Delta(C_1) \cap \ldots \cap \Delta(C_n) = \emptyset$$

Beweis: Das folgt aus dem Satz von Tychonoff, angewendet auf

$$\prod_{i \in \mathbb{N}} \{0,1\}$$

mit Produkttopologie. □

Anmerkung (Diskrete Topologie)*:* Sei X beliebige Menge, dann ist die diskrete Topologie auf X definiert durch:

$$\tau = \mathcal{P}(X)$$

Dh. jede Teilmenge von X ist offen.

Anmerkung: Sei X endliche Menge, also topologischer Raum betrachtet, ohne dass die Topologie eigens definiert oder erwähnt ist, dann ist immer die diskrete Topologie gemeint.

Anmerkung: Die Produkttopologie auf $\prod_{i\in\mathbb{N}}\{0,1\}$ hat als offene Basismengen genau die Mengen der Form

$$\{(x_i)_{i\in\mathbb{N}} \mid x_{i_1} = \varepsilon_{i_1}, x_{i_2} = \varepsilon_{i_2}, \ldots, x_{i_n} = \varepsilon_{i_n}\}, \quad \varepsilon_{i_k} \in \{0,1\}$$

Diese offenen Basismengen sind gleichzeitig abgeschlossen, da das Komplement eine Vereinigung offener Basismengen ist, also offen.

Es gilt: Für jede Formel $A \in \mathcal{A}$ ist $\Delta(A)$ abgeschlossen, da als Vereinigung von endlich vielen offen-abgeschlossenen Basismengen darstellbar. Wenn in A keine Variablen außer $A_1, \ldots, A_n$ vorkommen, dann hängt $\overline{b}(A)$ nur von

$$b\big|_{\{A_1,\ldots,A_n\}} : \{A_1, \ldots, A_n\} \to \{0,1\}$$

ab. Seien $b_1, \ldots, b_k$ jene Belegungen von $A_1, \ldots, A_n$ mit $\overline{b}(A) = 1$, dann ist

$$\Delta(A) = \bigcup_{i=1}^{k} \{(x_m)_{m\in\mathbb{N}} \mid x_1 = b_i(A_1), x_2 = b_i(A_2), \ldots, x_n = b_i(A_n)\}$$

$\Delta(A)$ ist abgeschlossen als Vereinigung endlich vieler abgeschlossener Mengen (k Stück, $k \leq 2^n$, n die Anzahl in A vorkommender Variablen, k die Anzahl der Belegungen von $\{A_1, \ldots, A_n\}$, die A erfüllen).

So lässt sich aus dem Kompaktheitssatz von Tychonoff folgern: Sei $\mathcal{C} \subseteq \mathcal{A}$; wenn $\mathcal{C}$ unerfüllbar, dann

$$\bigcap_{C\in\mathcal{C}} \Delta(C) = \emptyset$$

Da $\prod\{0,1\}$ kompakt ist und jedes $\Delta(C)$ abgeschlossen, gibt es endlich viele $C_1, \ldots, C_\ell \in \mathcal{C}$ mit

$$\Delta(C_1) \cap \ldots \cap \Delta(C_\ell) = \emptyset$$

dh. $\{C_1, \ldots, C_\ell\}$ unerfüllbar.

Kapitel 3

Boolesche Algebra

3.1 Boolesche Algebren

Definition 3.1 (Boolesche Algebra)**:** Ein Ring mit 1 $(R, +, \cdot)$ heißt Boolesche Algebra, wenn jedes Element idempotent ist, dh. $\forall r \in R : r^2 = r$.

Beispiel: Betrachte

$$\prod_{s \in S} \{0, 1\}$$

mit koordinatenweise Addition und Multiplikation, wobei in jeder einzelnen Koordinate Addition und Multiplikation von ganzen Zahlen modulo 2 ausgeführt werden.

$+$	0	1
0	0	1
1	1	0

,

$\cdot$	0	1
0	0	0
1	0	1

Anmerkung: Wiederholung: Ein Ring $(R, +, \cdot)$ ist eine Menge $R \neq \emptyset$ mit zweiwertigen Operationen $+ : R \times R \to R$, $\cdot : R \times R \to R$, wobei $(R, +)$ kommutative Gruppe ist, dh.

1. Assoziativität: $r + (s + t) = (r + s) + t$
2. Nullelement $e = 0$: $\exists e \in R : \forall r \in R : e + r = r + e = r$
3. Additives Inverses $s = -r$: $\forall r \in R : \exists s \in R : r + s = s + r = 0$
4. Kommutativität: $r + s = s + r$

und $(R, \cdot)$ ist Halbgruppe, dh.

5. $r \cdot (s \cdot t) = (r \cdot s) \cdot t$

und die beiden Operationen erfüllen Distributivität,

6. $r \cdot (s + t) = r \cdot s + r \cdot t$ sowie $(s + t) \cdot r = s \cdot r + t \cdot r$

Bei einem Ring mit 1 gilt zusätzlich

7a. Multiplikatives Nullelement $v = 1$: $\exists v \in R : \forall r \in R : v \cdot r = r \cdot v = r$, dieses Element ist eindeutig.

Ein Ring heißt kommutativ, wenn zusätzlich

7b. $r \cdot s = s \cdot r$

Zur Notation: $\cdot$ bindet stärker als $+$.

Lemma 3.1: $(R, +, \cdot)$ sei Boolesche Algebra, dann ist R kommutativ und $\forall r \in R : r = -r$

Beweis:

$$r + s = (r + s)^2 = r^2 + rs + sr + s^2 = r + rs + sr + s = (r + s) + (rs + sr)$$

Rechts und links $(r + s)$ kürzen (dh. $-(r + s)$ addieren), dann folgt

$$0 = rs + sr \;\Rightarrow\; rs = -sr$$

Das gilt für alle $r, s \in R$, insbesondere für $s = 1$, daher

$$\forall r \in R : r \cdot 1 = -1 \cdot r \;\Rightarrow\; r = -r$$

Außerdem gilt $rs = -sr = sr$, dh. Kommutativität. □

Definition 3.2: Sei $(R, +, \cdot)$ Boolesche Algebra. Definiere Relation $\leq$ auf R durch

$$r \leq s :\Leftrightarrow r \cdot s = r$$

(Analog zu $\subseteq$, $\cdot$ entspricht $\cap$)

Anmerkung: Das ist eine Ordnungsrelation:

1. Reflexivität: zu zeigen $\forall r \in R : r \cdot r = r$, stimmt
2. Transitivität: zu zeigen $r \leq s, s \leq t \;\Rightarrow\; r \leq t$. Haben $r \cdot s = r$, $s \cdot t = s$, es folgt $r \cdot t = r \cdot s \cdot t = r \cdot s = r$, also $r \leq t$.
3. Antisymmetrie: zu zeigen $r \leq s \wedge s \leq r \Rightarrow r = s$. $r \cdot s = r$ und $s \cdot r = s$, mit Kommutativität des Rings folgt $r = r \cdot s = s \cdot r = s$, also $r = s$.

Anmerkung: Bezüglich $\leq$ haben je zwei Elemente $r, s \in R$ ein "größtes gemeinsames Kleineres" Element $\inf(r, s)$ und ein "kleinstes gemeinsames Größeres", $\sup(r, s)$.

3.2 Verbände aus Booleschen Algebren

Definition 3.3: Gegeben eine Menge mit Ordnungsrelation $(X, \leq)$. Wir sagen $i = \inf(a, b)$ genau dann, wenn

1. $i \leq a$, $i \leq b$
2. $\forall x \in X$ mit $x \leq a$, $x \leq b$ gilt $x \leq i$.

Analog ist $s = \sup(a, b)$ genau dann, wenn

1. $a \leq s$, $b \leq s$
2. $\forall x \in X$ mit $a \leq x$, $b \leq x$ gilt $s \leq x$.

$\sup(a, b)$ und $\inf(a, b)$ müssen nicht existieren, aber wenn, dann sind sie jeweils eindeutig.

Anmerkung: In der Booleschen Algebra ist für $r, s \in R$

$$\inf(r, s) = r \cdot s, \quad \sup(r, s) = r + s + r \cdot s$$

Überprüfung Infimum:

$$r \cdot (r \cdot s) = r^2 \cdot s = r \cdot s \;\Rightarrow\; r \cdot s \leq r$$

Analog $r \cdot s \leq s$. Sei $x \leq r, x \leq s$, ist zu zeigen $x \leq r \cdot s$:

$$x \cdot r = x, \quad x \cdot s = x \;\Rightarrow\; x \cdot (r \cdot s) = (x \cdot r) \cdot s = x \cdot s = x \;\Rightarrow\; x \leq r \cdot s$$

Überprüfung Supremum:

$$r \cdot (r + s + r \cdot s) = r^2 + r \cdot s + r^2 \cdot s = r \;\Rightarrow\; r \leq r + s + r \cdot s$$

Analog $s \leq r + s + r \cdot s$. Sei $r \leq x$, $s \leq x$, dh. $r \cdot x = r$, $s \cdot x = s$:

$$(r + s + r \cdot s) \cdot x = r \cdot x + s \cdot x + r \cdot s \cdot x = r + s + r \cdot s \;\Rightarrow\; r + s + r \cdot s \leq x$$

Definition 3.4 (Verband)**:** Eine Menge X mit Ordnungsrelation $\leq$ heißt Verband (lattice), wenn zu je zwei Elementen $x, y \in X$ ein $\inf(x, y)$ und ein $\sup(x, y)$ in X existieren.

Anmerkung: Man schreibt dann $x \wedge y$ ("meet") für $\inf(x, y)$ und $x \vee y$ ("join") für $\sup(x, y)$. Es gelten dann für $\wedge, \vee$

V1. Kommutativität, $x \wedge y = y \wedge x$, $x \vee y = y \vee x$

V2. Assoziativität, $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, analog für $\vee$

V3. $x \wedge x = x$, $x \vee x = x$

V4. $(x \wedge y) \vee y = y$, $(x \vee y) \wedge y) = y$

Beweis: Zu V1: sup, inf sind in x, y symmetrisch definiert, daher klar.

Zu V2: Hilfsdefinition

Definition 3.5: Gegeben $(X, \leq)$, $Y \subseteq X$, dann sei

- $i = \inf Y :\Leftrightarrow \forall y \in Y$: $i \leq y$ und $\forall y \in Y$: $x \leq y \;\Rightarrow\; x \leq i$.
- $s = \sup Y :\Leftrightarrow \forall y \in Y$: $y \leq s$ und wenn für $x \in X$ gilt $\forall y \in Y$: $y \leq x$, dann $s \leq x$.

$\sup Y$, $\inf Y$ gibt es nicht für jede Menge $Y \subseteq X$, aber wenn, dann eindeutig.

Zeige jetzt: in Verband $(X, \leq)$ ist sowohl $\inf(x, y, z) = x \wedge (y \wedge z)$ als auch $\inf(x, y, z) = (x \wedge y) \wedge z$, also folgt Gleichheit. Supremum analog. Mit Induktion gilt in jedem Verband $(X, \leq)$: Es gibt zu jeder endlichen Menge $\{x_1, \ldots, x_n\} \subseteq X$ Supremum und Infimum. Jede Klammerung von $x_1 \wedge x_2 \wedge \ldots \wedge x_n$ ist Infimum, jede Klammerung von $x_1 \vee x_2 \vee \ldots \vee x_n$ erfüllt die Bedingung für Supremum.

Anmerkung: Ein Verband, in dem $\forall Y \subseteq X$ $\sup Y$ und $\inf Y$ existieren, heißt vollständiger Verband.

Zu V3: Klar.

Zu V4: Übung. □

Anmerkung: Umgekehrt bekommt man aus jeder Menge X mit zweistelligen Operationen $\wedge, \vee$, die V1 bis V4 erfüllen, einen Verband, indem man definiert $x \leq y :\Leftrightarrow x \wedge y = x$ (äquivalent: $x \vee y = y$, Übung).

Beweis: Überprüfung, dass es sich beim so gewonnenen $(X, \leq)$ um einen Verband handelt: Je zwei Elemente haben ein Infimum, nämlich $\inf(x, y) = x \wedge y$, und ein Supremum, nämlich $\sup(x, y) = x \vee y$. Aus V1 - V2 lässt sich ableiten:

$$(x \wedge y) \wedge y = x \wedge (y \wedge y) = x \wedge y \Rightarrow (x \wedge y) \leq y$$
$$(x \wedge y) \wedge x = (y \wedge x) \wedge x = y \wedge (x \wedge x) = y \wedge x \Rightarrow (x \wedge y) \leq x$$

Angenommen $z \leq x, z \leq y$, zeige $z \leq x \wedge y$:

$$z \wedge y = z, z \wedge x = z \Rightarrow z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z \Rightarrow z \leq x \wedge y$$

Analog folgt $\sup(x, y) = x \vee y$. □

Anmerkung: Man nennt auch eine Menge $(X, \wedge, \vee)$, die die Axiome V1 bis V4 erfüllen, Verband.

Aus Verband $(X, \leq)$ den Verband $(X, \wedge, \vee)$ konstruieren mittels $x \wedge y := \inf(x, y)$, $x \vee y := \sup(x, y)$, aus zweiterem ersteres mittels $x \leq y :\Leftrightarrow x \wedge y = x$.

Wenn man von $(X, \leq)$ auf $(X, \wedge, \vee)$ übergeht und aus $\wedge, \vee$ wieder $\leq$ definiert, bekommt man die ursprüngliche Relation $\leq$ zurück. Es gilt nämlich in $(X, \leq)$: $x \leq y \Leftrightarrow \inf(x, y) = x$ (bzw. auch $x \leq y \Leftrightarrow \sup(x, y) = y$).

Übung: Von $(X, \wedge, \vee)$ zur $(X, \leq)$ übergeben durch $x \leq y :\Leftrightarrow x \wedge y = x$ und dann aus $\leq$ (für das Supremum und Infimum je zweier Elemente existieren) $\wedge, \vee$ konstruiert durch $x \wedge y = \inf(x, y)$, $x \vee y = \sup(x, y)$, dann sind die neuen $\wedge, \vee$ dieselben wie die, von denen man ausgegangen ist.

Eigenschaften des aus einer Booleschen Algebra gewonnenen Verbandes:

In dem aus einer Booleschen Algebra $(R, +, \cdot)$ gewonnenen Verband gibt es ein größtes Element $\sup R$, nämlich 1, und ein kleinstes Element $\inf R$, nämlich 0.

Da $x \leq y :\Leftrightarrow x \cdot y = x$ gilt $\forall x \in R : x \cdot 1 = x$, also $\forall x \in R : x \leq 1$. Außerdem gilt in jedem Ring $(R, +, \cdot)$: $\forall r \in R : 0 \cdot r = r \cdot 0 = 0$ (Aus den Ringaxiomen folgt $0 + 0 = 0$, also $\forall r \in R$:

$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$$

Durch Subtraktion von $r \cdot 0$ auf beiden Seiten folgt $0 = r \cdot 0$. Analog $0 \cdot r = 0$). Insbesondere in der Booleschen Algebra: $\forall x \in R$: $0 \cdot x = 0$, also $0 \leq x$. Sprechweise: 0 ist neutrales Element bezüglich $+$ $(0 + x = x + 0 = x)$ und adsorbierendes Element bezüglich $\cdot$ $(0 \cdot x = x \cdot 0 = 0)$. Hingegen ist 1 neutrales Element bezüglich $\cdot$ $(1 \cdot x = x \cdot 1 = x)$ und adsorbierendes Element bezüglich $+$ $(1 + x = x + 1 = 1)$.

Definition 3.6 (Komplement, komplementärer Verband)**:** In einem Verband $(X, \leq)$ mit kleinstem Element 0 und größtem Element 1 heißt y Komplement von x, wenn $x \wedge y = 0$ und $x \vee y = 1$, dh. $\inf(x, y) = 0$ und $\sup(x, y) = 1$. Ein Verband, in dem zu jedem $x \in X$ ein Komplement existiert, heißt komplementärer Verband.

Proposition 3.2: Der von einer Booleschen Algebra kommende Verband ist komplementärer Verband

Beweis: $1 + x$ ist Komplement zu x:

$$(1 + x) \cdot x = x + x^2 = x + x = 0 \Rightarrow (1 + x) \wedge x = 0, \quad \sup(1 + x, x) = 0$$

$$(1 + x) + x + (1 + x) \cdot x = 1 + x + x + 0 = 1 \Rightarrow (1 + x) \vee x = 1, \quad \inf(1 + x, x) = 1 \qquad \square$$

Definition 3.7 (Distributiver Verband)**:** Ein Verband $(X, \wedge, \vee)$ heißt distributiv, wenn $\forall a, b, c \in X$:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Anmerkung: In einem Verband gilt

$$\forall a, b, c : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \Leftrightarrow \forall a, b, c : a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Satz 3.3: Der aus einer Booleschen Algebra konstruierte Verband ist distributiv.

Beweis: Zu zeigen ist:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

also zu zeigen

$$x(y + z + yz) = (xy) + (xz) + (xy)(xz)$$

$$x(y + z + yz) = xy + xz + xyz = xy + xz + xyxz$$ □

Übung: Ein Verband erfüllt $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ genau dann, wenn er $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ erfüllt.

Wir haben also gezeigt: der aus einer Booleschen Algebra ($(R, +, \cdot)$ Ring mit 1, in dem gilt $\forall r \in R : r^2 = r$) konstruierte Verband (mit $\leq$ definiert durch $x \leq y :\Leftrightarrow xy = x$ bzw. $x \wedge y := \inf(x, y)$, $x \vee y := \sup(x, y)$ bezüglich dieser $\leq$-Relation) ist ein distributiver, komplementärer Verband.

Satz 3.4: In jedem distributiven komplementären Verband ($(V, \wedge, \vee)$, so dass V1 bis V4 erfüllt sind und V ein größtes Element 1 und ein kleinstes Element 0 hat und $\forall x \in V \exists x^c \in V$ mit $x \wedge x^c = 0$, $x \vee x^c = 1$) gilt:

1. $\forall x \in V : x^c$ ist eindeutig bestimmt
2. de Morgan: $(x \wedge y)^c = x^c \vee y^c$ und $(x \vee y)^c = x^c \wedge y^c$

Beweis:

1. angenommen, y_1, y_2 erfüllen beide die Bedingungen von x^c, dann

   $$y_1 = y_1 \wedge 1 = y_1 \wedge (x \vee y_2) = (y_1 \wedge x) \vee (y_1 \wedge y_2) = 0 \vee (y_1 \wedge y_2) = y_1 \wedge y_2$$

   also $y_1 \leq y_2$. Durch Vertauschung der Rollen erhält man analog $y_2 \leq y_1$. Insgesamt folgt $y_1 = y_2$.

2. Wir zeigen: $x^c \vee y^c$ erfüllt die Bedingungen für das Komplement von $x \wedge y$:

   $$(x^c \vee y^c) \wedge (x \wedge y) = (x^c \wedge x \wedge y) \vee (y^c \wedge x \wedge y) = 0 \vee 0 = 0$$

   $$(x^c \vee y^c) \vee (x \wedge y) = (x^c \vee y^c \vee x) \wedge (x^c \vee y^c \vee y) = (1 \vee y^c) \wedge (x^c \vee 1) = 1 \wedge 1 = 1$$

   Andere Richtung als Übung. □

3.3 Boolesche Algebren aus Verbänden

Jetzt gehen wir von einem distributiven komplementären Verband $(V, \wedge, \vee)$ aus und konstruieren daraus eine Boolesche Algebra $(V, +, \cdot)$ durch

$$x \cdot y := x \wedge y, \qquad x + y := (x \wedge y^c) \vee (x^c \wedge y)$$

Anmerkung: Es gilt $x + y = (x \vee y) \wedge (x \wedge y)^c$, da nämlich

$$\begin{aligned}(x \wedge y^c) \vee (x^c \wedge y) &= (x \vee x^c) \wedge (x \vee y) \wedge (y^c \vee x^c) \wedge (y^c \vee y) = 1 \wedge (x \vee y) \wedge (y^c \vee x^c) \wedge 1 \\ &= (x \vee y) \wedge (y^c \vee x^c) = (x \vee y) \wedge (x \wedge y)^c\end{aligned}$$

- Jedes Element $x \in V$ ist idempotent: $x = x \cdot x$ heißt $x = x \wedge x$ (ein Verbandsaxiom).
- Assozitivität von $\cdot$ ist Assoziativität von $\wedge$, also ebenfalls ein Verbandsaxiom.
- Neutrales Element bezüglich $\cdot$ ist das größte Element 1 des komplementären Verbandes: $1 \wedge x = x \wedge 1 = x$.
- Neutrales Element bezüglich $+$ ist das kleinste Element 0 des komplementären Verbandes: $0 + x = x + 0 = (x \wedge 0^c) \vee (x^c \wedge 0) = (x \wedge 1) \vee (x^c \wedge 0) = x \vee 0 = x$
- Kommutativität von $+$ folgt aus Kommutativität von $\vee$.
- Inverses Element von x bezüglich $+$, dh. $-x$, existiert und es gilt $-x = x$, da: $x + x = (x \wedge x^c) \vee (x^c \wedge x) = 0 \vee 0 = 0$.
- Assoziativität von $+$:

  $$\begin{aligned}x + (y + z) &= (x \wedge (y + z)^c) \vee (x^c \wedge (y + z)) \\ &= (x \wedge ((y \wedge z^c)^c \wedge (y^c \wedge z)^c)) \vee (x^c \wedge ((y \wedge z^c) \vee (y^c \wedge z))) \\ &= (x \wedge (y^c \vee z) \wedge (y \vee z^c)) \vee (x^c \wedge ((y \wedge z^c) \vee (y^c \wedge z))) \\ &= ((x \wedge y^c) \vee (x \wedge z)) \wedge (y \vee z^c)) \vee ((x^c \wedge y \wedge z^c) \vee (x^c \wedge y^c \wedge z)) \\ &= ((x \wedge y^c) \wedge (y \vee z^c)) \vee ((x \wedge z) \wedge (y \vee z^c)) \vee (x^c \wedge y \wedge z^c) \vee (x^c \wedge y^c \wedge z) \\ &= (x \wedge y^c \wedge z^c) \vee (x \wedge z \wedge y) \vee (x^c \wedge y \wedge z^c) \vee (x^c \wedge y^c \wedge z)\end{aligned}$$

  Dieser Ausdruck ist wegen Kommutativität von $\wedge, \vee$ symmetrisch in x, z, also $x+(y+z) = z + (y + x)$. Mit Kommutativität von $+$ folgt $x + (y + z) = (x + y) + z$. Überprüfen: $x(y + z) = xy + xz$, $(y + z)x = yx + zx$ mit Distributivitätsgesetzen von $\wedge, \vee$ und de Morgan.
- Distributivität: noch zu zeigen.

Anmerkung: Wenn man aus einer Booleschen Algebra einen distributiven komplementären Verband konstruiert und aus diesem wieder eine Boolesche Algebra, bekommt man die ursprüngliche Boolesche Algebra zurück; analog, wenn man vom distributiven komplementären Verband ausgeht.

3.4 Unteralgebren, Algebrahomomorphismen, Satz von Stone

Definition 3.8 (Unteralgebra)**:** Eine Unteralgebra einer Booleschen Algebra $(R, +, \cdot)$ ist eine Teilmenge $S \subseteq R$, die bezüglich $+, -, \cdot$ abgeschlossen ist und 1 enthält, das heißt $S \subseteq R : \forall a, b \in S : a + b$, $a - b$, $a \cdot s \in S$ und $1 \in S$.

Anmerkung: Eine Unteralgebra einer Booleschen Algebra ist bezüglich Einschränkungen von $+, \cdot$ auf $+ : S \times S \to S$, $\cdot : S \times S \to S$ wieder eine Boolesche Algebra (da bezüglich $+, -, \cdot$ abgeschlossen). Eine bezüglich $+, -, \cdot$ abgeschlossene Teilmenge muss nicht 1 enthalten.

Beispiel: $Y \subseteq X$: $\mathcal{P}(Y) \subseteq \mathcal{P}(X)$ ist abgeschlossen bezüglich $\cap, \cup$, also bezüglich $\cap, \Delta$ (sind $\cdot, +$); aber $\mathcal{P}(Y)$ enthält nicht $1_{\mathcal{P}(X)} = X$.

Satz 3.5 (Satz von Stone)**:** Jede Boolesche Algebra ist isomorph zu einer Unteralgebra einer Booleschen Algebra der Form $(\mathcal{P}(A), \cap, \cup)$.

Dabei ist ein Isomorphismus Boolescher Algebren ein Ringisomorphismus mit $f(1) = 1$, dh, eine Funktion $f : A \to B$ bijektiv mit

- $f(a_1 + a_2) = f(a_1) + f(a_2)$
- $f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2)$
- $f(1) = 1$

Nämlich genauer: eine Boolesche Algebra A ist isomorph zur Unteralgebra der offen-abgeschlossenen Teilmengen des Stoneschen Raums $\mathcal{S}(A)$, der wiederum eine Unteralgebra von $(\mathcal{P}(A), \cap, \cup)$ ist.

$\mathcal{P}(A)$ kann aufgefasst werden als

$$\prod_{a \in A} \{0, 1\}$$

(Jede Teilmenge von A mit ihrer charaketeristischen Funktion χ_S identifizieren)

$$\chi_s : A \to \{0, 1\}, \qquad \chi_S(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$$

$\prod\{0, 1\}$ wiederum kann man auffassen als Menge aller Funktion $f : A \to \{0, 1\}$ mit elementweiser Addition und Multiplikation.

$$\begin{aligned} \mathcal{S}(A) &= \{f : A \to \{0, 1\} \mid f \text{ Ringhomomorphismus}\} \\ &= \{f : A \to \{0, 1\} \mid f(a + b) = f(a) + f(b), \quad f(a \cdot b) = f(a) \cdot f(b), \quad f(1) = 1\} \end{aligned}$$

Gegeben eine Boolesche Algebra $(A, +, \cdot)$ (bzw. $(A, \wedge, \vee)$). Dann ist A isomorph zu der Sub-Algebra der offen-abgeschlossenen Mengen des Stone-Raums $S(A)$ von A.

Definition 3.9: Seien $(A, +, \cdot)$, $(B, +, \cdot)$ Boolesche Algebren. $f : A \to B$ heißt Homomorphismus Boolescher Algebren, wenn

1. $f(1) = 1$
2. $f(a + c) = f(a) + f(c)$
3. $f(a \cdot c) = f(a) \cdot f(c)$

Ein bijektiver Homomorphismus heißt Isomorphismus.

Definition 3.10 (Stone-Raum)**:** Sei $(A, +, \cdot)$ Boolesche Algebra und

$$S(A) = \hom(A, \{0, 1\})$$

die Menge der Homomorphismen $f : A \to \{0, 1\}$ mit Addition und Multiplikation

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

$S(A)$ heißt Stone-Raum.

Dieser Raum $S(A)$ hat die Topologie geerbt von der Produkttopologie von

$$\prod_{a \in A} \{0,1\}$$

Dh. eine Menge $T \subseteq S(A)$ heißt offen, wenn sie Durchschnitt einer offenen Menge im Produkt $\prod\{0,1\}$ mit $S(A)$ ist, dh. es gibt O offen, $O \subseteq \prod\{0,1\}$ mit $O \cap S(A) = S$.

In $\prod\{0,1\}$ sind die offenen Mengen genau die Vereinigungen beliebig vieler offener Basismengen, wobei die offenen Basismengen genau die Mengen der Form für gewisse endlich viele $a_1, \ldots, a_n \in A$, $\varepsilon_1, \ldots, \varepsilon_n \in \{0,1\}$:

$$O = \left\{ (x_a)_{a \in A} \in \prod_{a \in A} \{0,1\} \;\middle|\; x_{a_1} = \varepsilon_1, x_{a_2} = \varepsilon_2, \ldots, x_{a_n} = \varepsilon_n \right\}$$

In dieser Topologie sind die offenen Basismengen gleichzeitig abgeschlossen (und das sind schon alle offen-abgeschlossenen Mengen $\subseteq S(A)$). Die offen-abgeschlossenen Mengen von $S(A)$ bilden eine Sub-Algebra (nach Axiomen der Topologie ist die Menge der offen-abgeschlossenen Mengen bezüglich $\cap, \cup$ (von endlich vielen) abgeschlossen).

Ein Isomorphismus $\varphi : A \to$ Sub-Algebren der offen-abgeschlossenen Teilmengen von $S(A)$ ist gegeben durch

$$\varphi(a) = \{f \in S(A) \mid f(a) = 1\}$$

Das ist offensichtlich eine offene Basismenge von $S(A)$. Man bekommt alle offenen Basismengen (dh. φ surjektiv), sei nämlich

$$O = \{f \in S(A) \mid f(a_1) = \ldots = f(a_n) = 1\}$$

dann ist

$$O = \{f \mid f(c) = 1\}, \quad c = (a_1 \wedge a_2 \wedge \ldots \wedge a_n) \wedge (b_1^c \wedge b_2^c \wedge \ldots \wedge b_k^c)$$

Kapitel 4

Prädikatenlogik (First Order Logic)

4.1 Terme

Das Alphabet $\mathcal{B}$ einer Sprache erster Ordnung besteht aus

1. $\mathcal{V} = \{v_i \mid i \in \mathbb{N}\}$ abzählbar unendlich viele Variablen
2. $\{(,), \wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$ (oder Klammern und eine Menge J von Junktoren, so dass $\mathcal{A}_J$ (Aussagenlogik mit Junktoren in J) vollständig ist)
3. $\{\forall, \exists\}$ Quantoren (theoretisch würde auch einer genügen)
4. $\forall n \in \mathbb{N}$ F_n eine höchstens abzählbar unendliche Menge von Funktionssymbolen
5. $\forall n \in \mathbb{N}$ R_n eine höchstens abzählbar unendliche Menge von Relationssymbolen
6. In einer Sprache mit "=" muss in R_2 das Symbol "=" vorkommen.
7. $\mathcal{C}$ eine Menge von Konstanten (Symbolen), kann diese aber auch als $\mathcal{C} = F_0$, dh. als Menge der nullstelligen Funktionssymbole einführen.

Das Alphabet $\mathcal{B}$ ist disjunkte Vereinigung der genannten Mengen.

Definieren zuerst Subformeln, die in einem Modell "Elemente" bezeichnen sollen, nämlich Terme.

Definition 4.1: Die Menge der Terme der Sprache $\mathcal{L}$, $T(\mathcal{L})$, ist definiert als die kleinste Teilmenge von $\mathcal{B}^*$ (Worte mit Buchstaben in $\mathcal{B}$, $\mathcal{B}$ das Alphabet von $\mathcal{L}$), die

1. alle Variablen und Konstanten von $\mathcal{L}$ enthält
2. abgeschlossen ist bezüglich der Relationen

   $$(t_1, t_2, \ldots, t_k, f t_1 t_2 \cdots t_k)$$

   für $f \in F_k$. Abgeschlossenheit einer Menge $M \subseteq \mathcal{B}^*$ bezüglich dieser Relation heißt: $\forall n \in \mathbb{N}, \forall f \in F_n : t_1, \ldots, t_n \in M \Rightarrow f t_1 t_2 \cdots t_n \in M$.

Die kleinste Menge, die $\mathcal{V}, \mathcal{C}$ enthält und bezüglich dieser Relationen abgeschlossen ist, ist wieder formal definiert als Durchschnitt aller $M \subseteq \mathcal{B}^*$ mit obigen zwei Eigenschaften.

Die Terme der Sprache erfüllen eindeutige Lesbarkeit, dh. $t \in T(\mathcal{L})$, dann gilt genau einer der Fälle

1. $t \in \mathcal{V}$
2. $t \in \mathcal{C}$
3. $\exists n \in \mathbb{N}, \exists f \in F_n, \exists t_1, \ldots, t_n \in T(\mathcal{L})$ mit $t = f t_1 \cdots t_n$

und im Fall 3 sind $n, f, t_1, \ldots, t_n$ eindeutig bestimmt. Da

$$\mathcal{V} \cap \mathcal{C} \cap \left(\bigcup_{n \in \mathbb{N}} F_n \right) = \emptyset, \quad n \neq m \Rightarrow F_n \cap F_m = \emptyset$$

schließen 1, 2, 3 sich gegenseitig aus und im Fall 3 sind f und n eindeutig bestimmt. Die einzige Möglichkeit zur Mehrdeutigkeit wäre

$$f t_1 \cdots t_n = f s_1 \cdots s_n$$

mit Termen s_i, t_i. Sei k minimal mit $t_k \neq s_k$, dann ist t_k ein echter Anfangsabschnitt von s_k (oder umgekehrt).

Lemma 4.1: Kein echter Anfangsabschnitt eines Terms ist selbst ein Term.

Beweis: Führe ganzzahlige Gewichte $w(x)$ für Symbole x ein:

$$w(x) = \begin{cases} 1 & x \in \mathcal{V} \cup \mathcal{C} \\ 1 - n & x \in F_n \end{cases}$$

und definieren das Gewicht eines Wortes $b_1 \cdots b_m$ mit b_i Buchstabe $\in \mathcal{V} \cup \mathcal{C} \cup \bigcup F_n$ als

$$w(b_1 \cdots b_m) = \sum_{i=1}^{m} w(b_i)$$

Dann gilt für alle $t \in T(\mathcal{L})$: $w(t) = 1$ und für jeden echten Anfangsabschnitt a eines Terms ist $w(a) < 1$.

Wir zeigen $w(t) = 1$ für Terme t mittels Induktion: Behauptung ist erfüllt für $t \in \mathcal{V} \cup \mathcal{C}$. Im Fall $t = f t_1 \cdots t_n$, $f \in F_n$, $t_1, \ldots, t_n$ Terme ist laut Induktionsvoraussetzung $w(t_i) = 1$ für alle i, insgesamt erhält man

$$w(t) = w(f) + w(t_1) + \ldots + w(t_n) = 1$$

Für echte Anfangsabschnitte eines Terms t wird ebenfalls eine Induktion geführt. Im Fall $t \in \mathcal{V} \cup \mathcal{C}$ gibt es keine echten Anfangsabschnitte, Aussage erfüllt. Im Fall $t = f t_1 \cdots t_n$ unterscheide je nach Form des Anfangsabschnitts a: Falls $a = f$, $w(a) = 1 - n \leq 0 < 1$. Falls $a = f t_1 \cdots t_k s_{k+1}$ mit s_{k+1} echter Anfangsabschnitt von t_{k+1} oder $k + 1 < n$ und $s_{k+1} = t_{k+1}$, dann ist

$$\begin{aligned} w(a) &= (1 - n) + w(t_1) + \ldots + w(t_k) + w(s_{k+1}) \\ &= 1 - n + k + w(s_{k+1}) < 1 \end{aligned}$$

da entweder $w(s_{k+1}) < 1$ oder $w(s_{k+1}) = 1$ und $k + 1 < n$, also insgesamt kleiner 1. □

Durch die eindeutige Lesbarkeit von Termen ist für jeden Term auch eine "Höhe" definiert, und zwar Höhe $h(t) = 0$ für $t \in \mathcal{V} \cup \mathcal{C}$ und für $t = f t_1 \cdots t_n$ Höhe $h(t) := \max\{h(t_1), \ldots, h(t_n)\} + 1$. Das entspricht der Anzahl der Schritte, die man braucht, um diesen Term schrittweise aus vorhandenen k Termen und einem davorgestellten k-stelligen Funktionensymbol zu konstruieren.

Umgangssprachlich schreibt man für Terme in Präfixnotation $fagb$ auch $f(a, g(b))$ für f zweistelliges, g einstelliges Funktionssymbol, a, b Konstanten bzw. $(a + b)$ für $+ab$ etc.

4.2 Sprache erster Ordnung, Struktur einer Sprache

Definition 4.2 (Sprache $\mathcal{L}$)**:** Induktive Definition der Formeln der Sprache $\mathcal{L}$:

1. Eine atomare Formel ist $Rt_1t_2\dots t_n$, wobei R ein n-stelliges Relationssymbol ist und $t_1,\dots,t_n$ Terme.
2. Wenn A, B Formeln sind, dann auch $(\neg A)$, $(A \wedge B)$, $(A \vee B)$ und so weiter.
3. Wenn A Formel ist und $v_i \in \mathcal{V}$ (Variable), dann sind auch $\exists v_i A$ und $\forall v_i A$ Formeln.

Die Sprache $\mathcal{L}$ ist die kleinste Menge von Wörtern, die die atomaren Formeln enthält und bezüglich der Konstruktionen 2, 3 abgeschlossen ist (dh. der Durchschnitt aller solcher Mengen).

Struktur zu einer Sprache $\mathcal{L}$: $\mathcal{M} = (M$, Relationen, Funktionen, Konstanten), wobei M nichtleere Menge und eine Zuordnung zu jeder Konstante $c \in \mathcal{L}$ ein Element $\overline{c} \in M$ zu jedem n-stelligen Funktionssymbol f von $\mathcal{L}$ eine Funktion $\overline{f} : M^n \to M$ zu jedem n-stelligen Relationssymbol R von $\mathcal{L}$ eine n-stellige Relation $\overline{R} \subseteq M^n$ existiert.

Wenn $\mathcal{L}$ Sprache mit "=" ist, dann soll diesem Symbol die Gleichheitsrelation (Diagonale von M^2) zugeordnet werden, beispielsweise $(\mathbb{N}, \leq, +, \cdot)$, $(\mathbb{R}, \leq, +, \cdot)$, $(\mathbb{Z}, \leq, +, \cdot)$ sind Strukturen für eine Sprache $\mathcal{L}$ mit einem zweistelligen Relationssymbol und zwei zweistelligen Funktionssymbolen.

Freie und gebundene Variablen in Formeln von $\mathcal{L}$

Beispiel:

$$\exists x((x \leq y) \wedge \forall z(z \cdot x = x))$$

Hier sind x, z gebunden, y frei.

Beispiel:

$$\forall x(\neg(y < y) \wedge \forall y(y = y))$$

Hier ist x gebunden; y ist vor $\forall$ frei, danach gebunden.

Beispiel:

$$\exists y(\forall x(x \leq y))$$

Diese Aussage enthält keine freien Variablen, dh. sie ist eine "geschlossene" Formel, interpretierbar als Aussage über eine Struktur.

Beispiel: $\forall x(x \leq y)$ ist als Aussage über ein bestimmtes Element einer Struktur interpretierbar, je nachdem, was man für y einsetzt.

Definition 4.3 (Freie, gebundene Vorkommen)**:** Die freien Vorkommen der Variable v in einer Formel $F \in \mathcal{L}$ sind:

1. Wenn F atomar ist, sind alle Vorkommen von v in F frei.
2. Wenn $F = (\neg G)$ oder $F = (G \star H)$, $\star$ Junktor, dann sind die freien Vorkommen von v in F genau die freien Vorkommen von v in G bzw. G und H.
3. Wenn $F = \forall w A$ oder $F = \exists w A$ und w eine andere Variable als v ist, dann sind die freien Vorkommen von v in F genau diejenigen in A.

4. Wenn $F = \forall v A$ oder $F = \exists v A$, dann ist kein Vorkommen von v in F frei.

"Nicht frei" ist synonym zu "gebunden".

Eine Variable kann in einer Formel sowohl freie als auch gebundene Vorkommen haben. Die freien Variablen einer Formel sind diejenigen Variablen, die in F mindestens ein freies Vorkommen haben.

Man schreibt $F = F[v_1, \ldots, v_k]$, wenn keine andere Variablen als $v_1, \ldots, v_k$ in F frei sind.

Analog für Terme $t = t[v_1, \ldots, v_k]$ heißt, in t kommen höchstens die Variablen $v_1, \ldots, v_k$ und keine weiteren vor. Ein geschlossener Term ist ein Term ohne Variable (nur in Sprachen mit Konstanten möglich).

Eine geschlossene Formel ist ein Formel ohne freie Variable.

Jedes gebundene Vorkommen einer Variable in einer Formel ist von genau einem Quantor gebunden (Bindungsbereich des Quantors).

Definition 4.4 (Bindungsbereich eines Quantors)**:** Sei $Q \in \{\forall, \exists\}$. Der Bindungsbereich von Q in QvF sind genau alle freien Vorkommen von v in F sowie das v, das unmittelbar auf Q folgt.

Der Bindungsbereich aller Quantoren in F der Form $(\neg G)$, $(G \star H)$ ist genau der Bindungsbereich des Quantors in der Subformel G bzw. H, in der er vorkommt. (Atomare Formeln haben keine Quantoren).

Anmerkung: Wir haben hier die eindeutige Lesbarkeit von Formeln in $\mathcal{L}$, einer Sprache erster Ordnung, verwendet.

4.3 Interpretation von Formeln, Modelle

Gegeben eine Sprache $\mathcal{L}$ und $\mathcal{M}$ dazupassende Struktur, dann interpretiert man Variablen als Elemente von M (der Grundmenge von $\mathcal{M}$) und man kann dadurch jedem Term ein Element von M zuordnen.

Definition 4.5: Sei t Term, $t = t[v_1, \ldots, v_n]$. Unter der Interpretation von v_i als $m_i \in M$ für gewisse $m_1, \ldots, m_n \in M$ interpretiert man t wie folgt:

1. t eine Konstante c, interpretiert als $\overline{c} \in M$ (die Zuordnung von Konstantensymbolen in $\mathcal{L}$ zu Elementen von M ist mit der Struktur gegeben).
2. t eine Variable v_i $(1 \leq i \leq n)$, interpretiere als m_i.
3. $t = f t_1 \ldots t_n$, interpretiere als $\overline{f}(\overline{t}_1, \ldots, \overline{t}_n)$, wobei $\overline{t}_i$ die Interpretation von t_i und $\overline{f} : M^n \to M$ die in der Struktur dem Symbol f zugeordnete Funktion ist.

Man schreibt $\overline{t}^{(\mathcal{M}, v_1 \to m_1, \ldots, v_n \to m_n)}$ oder $\overline{t}^{\mathcal{M}}$ bzw. $\overline{t}$ für die Interpretation von t in $\mathcal{M}$ (abhängig von einer Interpretation der in t vorkommenden Variablen als Elemente von M, $v_1 \to m_1, \ldots, v_n \to m_n$.

Interpretiere im Folgenden Formeln als Aussage über die Struktur (im Fall einer geschlossenen Formel) bzw. als Aussagen über Elemente der Grundmenge der Struktur (im Fall einer Formel mit freien Variablen) und definiere, wann $\mathcal{M}$ eine Aussage erfüllt.

Definition 4.6: Sei $\mathcal{L}$ Sprache, $\mathcal{M}$ die zugehörige Struktur. Gegeben eine Interpretation der Variablen $v_1, \ldots, v_n$ als Elemente $m_1, \ldots, m_n$ (dh. $v_1 \to m_1, \ldots, v_n \to m_n$), dann interpretiere Formeln, die außer $v_1, \ldots, v_n$ keine freien Variabalen enthalten, wie folgt:

1. Wenn F atomare Formel, $F = Rt_1 \ldots t_k$: $\mathcal{M}(v_1 \to m_1, \ldots, v_n \to m_n) \vDash F$ genau dann, wenn $(\bar{t}_1, \ldots, \bar{t}_k) \in \overline{R}$. Die Struktur $\mathcal{M}$ unter der Interpretation von v_i als m_i, $i = 1, \ldots, n$, erfüllt $F = Rt_1 \ldots t_k$ genau dann, wenn die Interpretation $\bar{t}_1, \ldots, \bar{t}_k$ der Terme t_i in Relation $\overline{R}$ stehen ($\overline{R}$ für die dem Symbol R von $\mathcal{L}$ zugeordnete Relation).

2. Wenn $F = (\neg G)$, dann $\mathcal{M}(v_i \to m_i, i = 1, \ldots, n) \vDash F$ genau dann, wenn $\mathcal{M}(v_i \to m_i) \nvDash G$. $\nvDash$ heißt "erfüllt nicht", Verneinung von $\vDash$. Wenn $F = (G \wedge H)$, dann $\mathcal{M}(v_i \to m_i) \vDash F$ genau dann, wenn $\mathcal{M}(v_i \to m_i) \vDash G$ und $\mathcal{M}(v_i \to m_i) \vDash H$. Weitere Junktoren analog.

3. Falls $F = \forall x G$, x eine Variable $\notin \{v_1, \ldots, v_n\}$. $\mathcal{M}(\ldots) \vDash F$ genau dann, wenn für alle $a \in M$ gilt $\vDash (x \to a, v_1 \to m_1, \ldots, v_n \to v_m) \vDash G$. Falls $F = \exists x G$, $x \notin \{v_1, \ldots, v_n\}$, dann gilt $\mathcal{M}(\ldots) \vDash F$ genau dann, wenn ein $a \in M$ existiert, so dass $\mathcal{M}(x \to a, v_1 \to m_1, \ldots, v_n \to m_n) \vDash G$. Wenn $F = \forall v_i G$, dann $\mathcal{M}(\ldots) \vDash F$ genau dann, wenn für alle $a \in M$ gilt $\mathcal{M}(v_j \to m_j (j \neq i, 1 \leq j \leq n), v_i \to a) \vDash G$. und falls $F = \exists v_i G$, dann $\mathcal{M}(\ldots) \vDash F$ genau dann, wenn es ein $a \in M$ gibt, so dass $\mathcal{M}(v_i \to a, v_j \to m_j (i \neq j, 1 \leq j \leq n)) \vDash G$.

Wir haben definiert, wann eine Formel $F \in \mathcal{L}$ (Sprache $\mathcal{L}$) in einer Interpretation von $\mathcal{L}$, $\mathcal{M}(x_i \to a_i \mid i = 1, \ldots, n)$ ($\mathcal{M}$ eine $\mathcal{L}$-Struktur, $\{x_1, \ldots, x_n\}$ umfasst alle in F freien Variablen) gilt, geschrieben $\mathcal{M}(x_i \to a_i) \vDash F$. Abgekürzte Schreibweise $\mathcal{M} \vDash F[a_1, \ldots, a_n]$, falls klar ist, dass $F = F[x_1, \ldots, x_n]$ (Obermenge $\mathcal{M} \vDash F$ der in F frei vorkommenden Variablen und deren Reihenfolge ist fix $x_1, \ldots, x_n$).

Definition 4.7: Eine Formel F, in der keine Variable frei vorkommt, heißt geschlossen.

Aus der Definition folgt auch die Definition von $\mathcal{M} \vDash F$ für $\mathcal{M}$ $\mathcal{L}$-Struktur, $F \in \mathcal{L}$ geschlossen (braucht keine Variablen interpretieren, $\emptyset$ ist Obermenge der in F frei vorkommenden Variablen).

Wenn $\mathcal{M} \vDash F$ sagt man, $\mathcal{M}$ ist Modell von F, bzw. für Menge von geschlossenen Formeln $\Phi \subseteq \mathcal{L}$ sagt man, $\mathcal{M}$ ist Modell von Φ ($\mathcal{M} \vDash \Phi$), wenn $\forall F \in \Phi : \mathcal{M} \vDash F$.

Definition 4.8: Seien $F, G \in \mathcal{L}$. Man sagt, G ist logische / semantische Folgerung von F, wenn für jede $\mathcal{L}$-Struktur $\mathcal{M}$ mit $\mathcal{M} \vDash F$ auch $\mathcal{M} \vDash G$ gilt. F, G heißen logisch äquivalent, wenn F logische Folgerung von G ist und umgekehrt.

Man schreibt $F \vDash G$ für G logische Folgerung von F, und $F \dashv\vDash G$ für logische Äquivalenz von F, G.

Eine Formel $F \in \mathcal{L}$ heißt allgemeingültig, wenn für jede $\mathcal{L}$-Struktur $\mathcal{M}$ gilt $\mathcal{M} \vDash F$ und $F \in \mathcal{L}$ heißt erfüllbar, wenn eine Struktur existiert mit $\mathcal{M} \vDash F$.

Lemma 4.2: $F \vDash G$ genau dann, wenn $\vDash (F \to G)$.

Beweis: Folgt aus der Definition von $\vDash$:

"$\Rightarrow$" Sei $F \vDash G$, dh. jedes $\mathcal{M}$ mit $\mathcal{M} \vDash F$ erfüllt $\mathcal{M} \vDash G$. Jedes $\mathcal{M}$ erfüllt entweder F oder es erfüllt F nicht. Im ersten Fall erfüllt $\mathcal{M}$ auch G, also $\mathcal{M} \vDash (F \to G)$. Im zweiten Fall, dh. $\mathcal{M} \nvDash F$, dann $\mathcal{M} \vDash (F \to G)$ nach Definition.

"$\Leftarrow$" Wenn $\vDash (F \to G)$, dann gilt für jedes $\mathcal{M}$ nach Definition von $\vDash$, dass $\mathcal{M} \nvDash F$ oder $\mathcal{M} \vDash G$. Also für jene $\mathcal{M}$ mit $\mathcal{M} \vDash F$ folgt $\mathcal{M} \vDash G$. $\square$

Analog: $F \models\!\models G$ genau dann, wenn $\models (F \leftrightarrow G)$.

Für Formel F mit freien Variablen $\mathcal{M} \models F$ definieren: $\mathcal{M} \models F$ genau dann, wenn $\mathcal{M} \models \overline{F}$, wobei $\overline{F}$ der universelle Abschluss von F ist. Wenn $x_1, \ldots, x_n$ die freien Variablen von F sind, dann $\overline{F} := \forall x_1 \forall x_2 \ldots \forall x_n F$. Reihenfolge der x_i bis auf logische Äquivalenz egal. Dh. wenn $\{x_1, \ldots, x_n\}$ die freien Variablen von F sind, dann ist für jede Permutation π von $1, \ldots, n$ $\forall x_{\pi(1)} \forall x_{\pi(2)} \ldots \forall x_{\pi(n)} F$ logisch äquivalent zu $\forall x_1 \forall x_2 \ldots \forall x_n F$.

Ähnlich wie in der Aussagenlogik: wenn man nur modulo $\models\!\models$ rechnet, kann man zB. Junktoren eliminieren, da zB. $F \to G \models\!\models (\neg F \vee G)$ etc. Auch Klammern können wegen Assoziativität von $\vee$, $\wedge$ weggelassen werden. Ebenfalls kann man bis auf logische Äquivalenz $\forall$ durch Formel mit $\exists$, $\neg$ umschreiben, da $\forall x F \models\!\models \neg \exists x \neg F$.

Anmerkung: Bei Formeln F, G mit freien Variablen aufpassen: $\models (\overline{F} \leftrightarrow \overline{G})$ bzw. $\overline{F} \models\!\models \overline{G}$ reicht nicht, damit $F \models\!\models G$.

Kapitel 5

Sequenzenkalkül

5.1 Sequenzen

Nach Ebbinghaus, Flum, Thomas.

Gegeben eine Sprache $\mathcal{L}$, Menge S von Paaren (Γ, φ) mit $\Gamma \subseteq \mathcal{L}$, $\varphi \in \mathcal{L}$. Schreibe ein Paar als $\Gamma\varphi$. Men nennt $\Gamma\varphi$ eine Sequenz. S ist induktiv definiert als kleinste Menge von Sequenzen, die abgeschlossen ist bezüglich folgender Ableitungsregeln (wenn die Sequenz oberhalb eines Strichs in S, dann auch die Sequenz unterhalb):

1. ("Element") Wenn $\varphi \in \Gamma$,

$$\frac{}{\Gamma \quad \varphi}$$

2. ("Teilmenge") Wenn $\Gamma' \supseteq \Gamma$

$$\frac{\Gamma \quad \varphi}{\Gamma' \quad \varphi}$$

3. ("Oder vorne")

$$\frac{\begin{array}{lll}\Gamma & \varphi & \chi \\ \Gamma & \psi & \chi\end{array}}{\Gamma \quad (\varphi \vee \psi) \quad \chi}$$

4. ("Oder hinten")

$$\frac{\Gamma \quad \varphi}{\Gamma \quad (\varphi \vee \psi)} \qquad \text{und} \qquad \frac{\Gamma \quad \varphi}{\Gamma \quad (\psi \vee \varphi)}$$

5. ("Fallunterscheidung")

$$\frac{\begin{array}{lll}\Gamma & \psi & \varphi \\ \Gamma & \neg\psi & \varphi\end{array}}{\Gamma \qquad \varphi}$$

6. (“Indirekter Beweis”)

$$\frac{\begin{array}{lll}\Gamma & \neg\varphi & \psi \\ \Gamma & \neg\varphi & \neg\psi\end{array}}{\begin{array}{ll}\Gamma & \varphi\end{array}}$$

7. (“Gleichheit”) Für t Term

$$\frac{}{t = t}$$

8. (“Gleiches Einsetzen”)

$$\frac{\begin{array}{lll}\Gamma & & \varphi\left(\frac{t}{x}\right)\end{array}}{\begin{array}{lll}\Gamma & t = t' & \varphi\left(\frac{t'}{x}\right)\end{array}}$$

9. (“Existenzquantor vorne”) wenn y nicht frei in Γ, $\exists x\varphi$, ψ

$$\frac{\begin{array}{lll}\Gamma & \varphi\left(\frac{y}{x}\right) & \psi\end{array}}{\begin{array}{lll}\Gamma & \exists x\varphi & \psi\end{array}}$$

10. (“Existenzquantor hinten”)

$$\frac{\begin{array}{ll}\Gamma & \varphi\left(\frac{t}{x}\right)\end{array}}{\begin{array}{ll}\Gamma & \exists x\varphi\end{array}}$$

Definition 5.1 (Einsetzen in eine Formel)**:** Sei $\varphi \in \mathcal{L}$, t ein Term von $\mathcal{L}$, dann soll $\varphi(\frac{t}{x})$ (bzw. alternativ $\varphi(t/x)$) die Formel aus $\mathcal{L}$ bezeichnen, die man durch simultanes Einsetzen von t für alle freien Vorkommen von x in φ erhält, analog $\varphi(t_1/x_1, t_2/x_2, \ldots, t_n/x_n)$ bezeichnet simultanes Einsetzen von t_i für alle freien Vorkommen von x_i.

Formale Definition induktiv nach der Struktur von φ.

Zum Sequenzenkalkül: wir nennen eine Sequenz $\Gamma\varphi$ korrekt, wenn $\Gamma \vDash \varphi$ (φ ist logische bzw. semantische Folgerung von Γ), dh. wenn für jede Struktur $\mathcal{M}$ mit $\mathcal{M} \vDash \Gamma$ auch $\mathcal{M} \vDash \varphi$ gilt.

Für Ableitungsregeln zeigen: wenn alle Sequenzen oberhalb des Strichs korrekt sind, dann auch jene unterhalb des Strichs. Daraus folgt: alle Sequenzen in S sind korrekt. Für $\Gamma\varphi \in S$ schreibt man $\vdash_S \Gamma\varphi$ bzw. $\Gamma \vdash_S \varphi$. Wegen Korrektheit gilt: Wenn $\Gamma \vdash_S \varphi$, dann $\Gamma \vDash \varphi$.

Beispiel (Ableitung von Sequenzen bzw. Formeln in S)*:*

Anmerkung: Sequenz $\emptyset\varphi$ wird als φ geschrieben.

Ableitung: $(\varphi \vee \neg\varphi)$ (“tertium non datur”) für beliebiges $\varphi \in \mathcal{L}$.

$$\frac{\begin{array}{lll}\varphi & \varphi & \text{Element} \\ \varphi & (\varphi \vee \neg\varphi) & \text{Oder hinten} \\ \neg\varphi & (\varphi \vee \neg\varphi) & \text{Oder hinten}\end{array}}{\begin{array}{ll}& (\varphi \vee \neg\varphi) \quad \text{Fallunterscheidung}\end{array}}$$

Schreibweise: Man schreibt endliche Menge Γ einfach als Folge ihrer Elemente, schreibt Folgerungen ohne Strich unter die schon abgeleiteten Sequenzen, nur vor der letzten Sequenz Strich.

Man kann auch zusätzliche Regeln ableiten, zB. Kettenschluss:

$$\begin{array}{lll} \Gamma & & \varphi \\ \Gamma & \varphi & \psi \\ \hline \Gamma & & \psi \end{array}$$

Dh. wenn $\Gamma\varphi \in S$ und $\Gamma\varphi\psi \in S$, dann auch ψ.

Beweise vorher zusätzlich "Ex Falso Quodlibet",

$$\begin{array}{ll} \Gamma & \psi \\ \Gamma & \neg\psi \\ \hline \Gamma & \varphi \end{array}$$

Mittels

$$\begin{array}{lll} \Gamma & \psi & \text{Voraussetzung} \\ \Gamma & \neg\psi & \text{Voraussetzung} \\ \Gamma & \neg\varphi \quad \psi & \text{Teilmenge} \\ \Gamma & \neg\varphi \quad \neg\psi & \text{Teilmenge} \\ \hline \Gamma & \varphi & \text{indirekter Beweis} \end{array}$$

Daher $\Gamma\varphi \in S$.

$$\begin{array}{lll} \Gamma & \varphi & \text{Voraussetzung} \\ \Gamma & \varphi \quad \psi & \text{Voraussetzung} \\ \Gamma & \neg\varphi \quad \varphi & \text{Teilmenge für } \Gamma' = \Gamma \cup \{\neg\varphi\} \\ \Gamma & \neg\varphi \quad \neg\varphi & \text{Element} \\ \Gamma & \neg\varphi \quad \psi & \text{Ex falso quodlibet} \\ \hline \Gamma & \psi & \text{Fallunterscheidung (2), (5)} \end{array}$$

5.2 Vollständigkeitssatz

Satz von Gödel formuliert, Beweis (hier nur skizziert) nach Henkin.

Wiederholung der Notation:

Semantik: $\mathcal{L}$ ist eine fixe Sprache erster Ordnung, eine Struktur $\mathcal{M}$ für $\mathcal{L}$ besteht aus einer Grundmenge M und für jedes n-stellige Funktionensymbol $f \in \mathcal{L}$ einer Funktion $\overline{f} : M^n \to M$ und für jedes n-stellige Relationssymbol $R \in \mathcal{L}$ einer Relation $\overline{R} \subseteq M^n$. $\mathcal{M}$ von $\mathcal{L}$ heißt Modell einer Menge von Formeln $\Phi \subseteq \mathcal{L}$, wenn $\mathcal{M}$ alle $\varphi \in \Phi$ erfüllt. Man schreibt dann $\mathcal{M} \vDash \Phi$. Wenn Φ eine Menge von Formeln $\subseteq \mathcal{L}$ ist, φ eine Formel $\in \mathcal{L}$, dann schreibt man $\Phi \vDash \varphi$ für: $\forall\mathcal{M}$ Modell mit $\mathcal{M} \vDash \Phi$ gilt auch $\mathcal{M} \vDash \varphi$.

Syntax: Wir haben das Sequenzenkalkül S und formale Ableitungen von Sequenzen in S definiert und zwar so, dass wenn $\Gamma\varphi$ in S ableitbar ist (Γ eine endliche Folge von Formeln $\in \mathcal{L}$, $\varphi \in \mathcal{L}$), dann $\Gamma \vDash \varphi$. Man schreibt $\vdash \Gamma\varphi$ für $\Gamma\varphi$ in S ableitbar. Für eine beliebige Menge von Formeln $\Phi \subseteq \mathcal{L}$, $\varphi \in \mathcal{L}$, schreiben wir $\Phi \vdash \varphi$, wenn es ein endliches $\Phi' \subseteq \Phi$ gibt mit $\vdash \Phi'\varphi$. Für endliche Mengen von Formeln ist $\vdash \Phi\varphi$ äquivalent zu $\Phi \vdash \varphi$.

Korrektheit des Kalküls: Es gilt: Wenn $\Phi \vdash \varphi$, dann $\Phi \vDash \varphi$.

Satz 5.1 (Vollständigkeitssatz V1)**:** $\Phi \vDash \varphi$ genau dann, wenn $\Phi \vdash \varphi$.

(Anmerkung: "$\Leftarrow$" ist genau die Korrektheit des Kalküls, "$\Rightarrow$" ist die eigentliche Vollständigkeitsaussage)

Satz 5.2 (Vollständigkeitssatz V2)**:** Jede konsistente (widerspruchsfreie) Theorie hat ein Modell.

Eine Theorie ist dabei eine Menge (geschlossener) Formeln; Konsistenz bedeutet, dass keine Widersprüche ableitbar sind, dh. dass es keine Formel φ gibt, so dass sowohl φ als auch die Verneinung $\neg\varphi$ abgeleitet werden kann.

Beispiel: $\Phi = \{(\varphi \vee \psi), (\varphi \vee \neg\psi), \neg\varphi\}$ ist nicht konsistent, da $\Phi \vdash \psi$ und $\Phi \vdash \neg\psi$.

Beweis (Beweis von V2 $\Rightarrow$ V1)*:* Angenommen, V2 gilt, und sei Φ eine Menge von Formeln, φ Formel, so dass $\Phi \models \varphi$, $\Phi \not\models \varphi$. Wegen $\Phi \models \varphi$ hat $\Phi \cup \{\neg\varphi\}$ kein Modell. $\Phi \cup \{\neg\varphi\}$ konsistent. Angenommen, es wäre nicht konsistent, dann $\Phi \cup \{\neg\varphi\} \vdash \varphi$ und $\Phi \cup \{\varphi\} \vdash \varphi$. Nach der Fallunterscheidungs-Regel im Kalkül gilt also $\Phi \vdash \varphi$, Widerspruch zur Voraussetzung. $\square$

Beweis (Beweisskizze für V2)*:* Gegeben $\Phi \subseteq \mathcal{L}$. Wir konstruieren daraus eine Struktur (Terminterpretation bezüglich Φ) $\mathcal{I}_\Phi$.

Grundmenge $\mathcal{T}_\Phi$: Äquivalenzklassen von Termen $\in \mathcal{L}$ bzgl. Äquivalenzrelation $\sim$, definiert als

$$t_1 \sim t_2 :\Leftrightarrow \Phi \vdash t_1 = t_2$$

Bezeichne mit $\bar{t}$ die Äquivalenzklasse von t bezüglich $\sim$.

Einem n-stelligen Funktionssymbol $f \in \mathcal{L}$ ordnen wir die Funktion $\overline{f} : \mathcal{T}_\Phi^n \to \mathcal{T}_\Phi$ zu durch

$$\overline{f}\bar{t}_1 \cdots \bar{t}_n := \overline{ft_1 \cdots t_n}$$

(Wohldefiniertheit: wenn $t_1 \sim t_1', \ldots, t_n \sim t_n'$, dann $ft_1 \cdots t_n \sim ft_1' \cdots t_n'$)

Für ein n-stelliges Relationssymbol R definiere n-stellige Relation $\overline{R} \subseteq \mathcal{T}_\Phi^n$ durch:

$$\overline{R}\bar{t}_1 \cdots \bar{t}_n \quad (\text{dh. } (\bar{t}_1, \ldots, \bar{t}_n) \in \overline{R}) \quad :\Leftrightarrow \quad \Phi \vdash Rt_1 \cdots t_n$$

(Wohldefiniertheit: wenn $t_1 \sim t_1', \ldots, t_n \sim t_n'$, dann $\Phi \vdash Rt_1 \cdots t_n \Leftrightarrow \Phi \vdash Rt_1' \cdots t_n'$)

Definition 5.2: Eine Theorie Φ heißt vollständig (negationstreu), wenn $\forall\varphi \in \mathcal{L}$ gilt ($\Phi \vdash \varphi$ oder $\Phi \vdash \neg\varphi$).

Anmerkung: Diese Vollständigkeit ist nicht dieselbe wie im Vollständigkeitssatz!

Definition 5.3: Eine Theorie Φ heißt Henkin-Theorie, wenn gilt: Für jede Formel $\in \mathcal{L}$ der Gestalt $\exists x\varphi$ existiert ein Term t, so dass $\Phi \vdash (\exists x\varphi \to \varphi(t/x))$, dh. zu jeder Existenz-Aussage in Φ gibt es einen "Zeugen" (ein Beispiel).

Satz 5.3 (Satz von Henkin)**:** Für jede konsistente, vollständige Henkin-Theorie Φ gilt: $\mathcal{I}_\Phi \models \Phi$, also insbesondere: jede konsistente, vollständige Henkin-Theorie hat ein Modell.

Anmerkung: Aus der Definition von $\mathcal{I}_\Phi$ folgt für eine beliebige konsistente Theorie Φ für beliebige atomare Formeln φ, dass $\Phi \vdash \varphi \Leftrightarrow \mathcal{I}_\Phi \models \varphi$.

Vollständigkeit von Φ liefert die Analogie von $\Phi \vdash \varphi$ oder $\Phi \vdash \neg\varphi$ zu $\mathcal{I}_\Phi \models \varphi$ oder $\mathcal{I}_\Phi \models \neg\varphi$ und erlaubt es, die Äquivalenz $\Phi \vdash \varphi \Leftrightarrow \mathcal{I}_\Phi \models \varphi$ fortzusetzen auf Formeln der Gestalt $\varphi \vee \psi$, $\neg\varphi$, $\varphi \wedge \psi$ etc.

Schließlich Fortsetzbarkeit der Äquivalenz auf Formeln der Gestalt $\exists x\varphi$ durch Henkin-Eigenschaft.

Nachdem der Satz von Henkin bewiesen ist, folgt V2 durch Einbettung einer beliebigen konsistenten Theorie in eine konsistente vollständige Henkin-Theorie. $\square$

Kapitel 6

Berechenbarkeit

6.1 Turingmaschinen, rekursive Funktionen

Eine Turingmaschine besteht aus einem "Band" mit abzählbar unendlich vielen Feldern, in denen jeweils 0 oder 1 steht. Die Maschine steht mit einem Lese-/Schreibkopf auf einem Feld, und es gilt gerade eine von endlich vielen Regeln $r_1, \ldots, r_n$ der Maschine; die Regel i besagt, wenn die Maschine auf einem Feld mit 1 steht, entweder: statt 1 schreibe 0, oder wieder 1, und dann nach rechts gehen oder nach links gehen und zur Regel j übergehen, oder die Regel i ist undefiniert; analog für 0. Zu Beginn der Berechnung steht auf dem Band der Input, und es gilt Regel 1; die Maschine läuft, bis sie zu einer undefinierten Regel kommt, dann hält sie. Es kann sein, dass die Maschine nie hält.

Definition 6.1 (Turingmaschine)**:** Eine Turing-Maschine mit n Regeln ist definiert als Funktion

$$f : \operatorname{dom} f \subseteq \{1, \ldots, n\} \times \{0, 1\} \to \{1, \ldots, n\} \times \{0, 1\} \times \{R, L\}$$

Definition 6.2 (partiell rekursiv)**:** Eine Funktion

$$F : \operatorname{dom} F \subseteq \mathbb{N}_0 \to \mathbb{N}_0$$

heißt partiell rekursiv, wenn eine Turing-Maschine existiert, die F berechnet, dh. eine Turingmaschine, die, wenn sie auf einem Band, das einen Block von $n+1$ konsekutiven 1 enthält, sonst 0, auf dem Feld mit dem 1 ganz links unter Gültigkeit der Regel 1 gestartet wird und

1. genau dann niemals hält, wenn $n \notin \operatorname{dom} F$
2. wenn $n \in \operatorname{dom} F$, hält mit Output $F(n)$, dh. auf dem Band steht ein Block von $F(n) + 1$ konsekutiven 1, sonst 0, und die Maschine steht auf dem 1 ganz links, während eine Regel, die bei 1 nicht definiert ist, gilt.

Analog heißt

$$F : \operatorname{dom} F \subseteq \mathbb{N}_0^k \to \mathbb{N}_0$$

partiell rekursiv, wenn eine Turingmaschine existiert, wenn eine Turingmaschine existiert, die für alle $(m_1, \ldots, m_k) \in \operatorname{dom} F$ mit dem Input

$$0 \overset{R_1}{\to} \underbrace{11\ldots1}_{m_1+1} 0 \underbrace{11\ldots1}_{m_2+1} 0 \ldots 0 \underbrace{11\ldots1}_{m_k+1} 00\ldots$$

den folgenden Output liefert

$$0 \overset{R_j}{\to} \underbrace{11\ldots1}_{F(m_1,\ldots,m_k)+1}$$

wobei die Maschine bei $(j,1)$ undefiniert ist, und für alle $(m_1,\ldots,m_k) \in \mathbb{N}_0^k \setminus \operatorname{dom} F$ mit Input $(m_1,\ldots,m_k)$ wie oben nicht hält.

Für $(m_1,\ldots,m_k) \in \operatorname{dom} F$ schreibt man $F(m_1,\ldots,m_k)\downarrow$, für $(m_1,\ldots,m_k) \notin \operatorname{dom} F$ entsprechend $F(m_1,\ldots,m_k)\uparrow$.

Eine partiell rekursive Funktion $F : \operatorname{dom} F \subseteq \mathbb{N}_0^k \to \mathbb{N}_0$ heißt total rekursiv, wenn $\operatorname{dom} F = \mathbb{N}_0^k$.

Notation: $\operatorname{dom} F$ ist der Definitionsbereich ("domain") der Funktion F.

Beispiel: Versuch einer Additions-Turingmaschine: es soll abgebildet werden

$$\ldots0 \overset{R_1}{\to} \underbrace{11\ldots1}_{n+1}0\underbrace{11\ldots1}_{m+1}0\ldots \quad \text{auf} \quad \ldots0 \overset{\text{undef}}{\to} \underbrace{11\ldots1}_{n+m+1}0\ldots$$

Regeln (in der Form (Regel, Feldinhalt) $\mapsto$ (Regel, Inhalt, Richtung)):

$(1,1) \mapsto (1,1,R)$
$(1,0) \mapsto (2,1,R)$
$(2,1) \mapsto (2,1,R)$
$(2,0) \mapsto (3,0,L)$
$(3,1) \mapsto (4,0,L)$
$(4,1) \mapsto (5,0,L)$
$(5,1) \mapsto (5,1,L)$
$(5,0) \mapsto (6,0,R)$

Nach unserer Definition der Turingmaschine hat diese hier 6 Regeln,

$$f : \operatorname{dom} f \subseteq \{1,\ldots,6\} \times \{0,1\} \to \{1,\ldots,6\} \times \{0,1\} \times \{R,L\}$$

also

$$\operatorname{dom} f = \{(1,1),(1,0),(2,1),(2,0),(3,1),(4,1),(5,1),(5,0)\}$$

Beispiel einer totalen ($F : \mathbb{N}_0^k \to \mathbb{N}_0$) Funktion, die nicht rekursiv ist: Sei für $n,k \in \mathbb{N}_0$ $b(n,k) = c \in \mathbb{N}_0$ maximal, so dass c als Wert $F(k)$ einer durch eine Turing-Maschine mit $\leq n$ Regeln berechneten Funktion auftritt. Da es nur endlich viele Turingmaschinen mit $\leq n$ Regeln gibt, können diese auch nur endlich viele verschiedene Outputs bei Input k liefern. Sei $G(n) := b(n,n)+1$ dann ist, wenn F durch eine Turingmaschine mit m Regeln berechnet wird, $F(m) \leq b(m,m) < G(m)$, also $G \neq F$. Daher ist G keine rekursive Funktion.

Übung: ebenso die "Busy Beaver"-Funktion nicht rekursiv, $b(m)$ ist die maximale Länge eines Blocks von 1 (sonst 0), der als Output einer Turingmaschine mit $\leq m$ Regeln (die schlussendlich hält), gestartet auf leerem (nur 0) Band, auftritt.

Sei A beliebiges abzählbar unendliches Alphabet, und A^* die Menge der endlichen Wörter mit Buchstaben $\in A$. Man kann $\varphi : A^* \hookrightarrow \mathbb{N}_0$ injektiv A^* in $\mathbb{N}_0$ abbilden (Wörter in A^*

eindeutig durch natürliche Zahlen codieren). Man kann durch Turingmaschine auch Funktionen $F : \operatorname{dom} F \subseteq (A^*)^k \to A^*$ berechnen, indem man die Funktion F^* mit $F^*(\varphi(w_1), \ldots, \varphi(w_k)) := \varphi(F(w_1, \ldots, w_k))$ betrachtet.

Beispielsweise könnte man, eindeutige Primfaktorzerlegung in $\mathbb{Z}$ ausnützend, $\varphi : A^* \to \mathbb{N}_0$ mit $A = \{a_1, a_2, \ldots\}$ so definieren:

$$\varphi(a_{k_1} a_{k_2} a_{k_3} \ldots a_{k_n}) = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdots p_n^{k_n} = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$$

wobei p_i die i-te Primzahl bezeichnet. So kann man auch Turingmaschinen als Wörter über dem Alphabet $\mathbb{N}_0 \cup \{(,), R, L, \mapsto\}$ auffassen und als natürliche Zahlen codieren.

Halteproblem für Turingmaschinen: betrachte die Funktion $H : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, so dass

$$H(n,k) = \begin{cases} 1 & \text{wenn Turingmaschine } n \text{ bei Input } k \text{ schließlich hält} \\ 0 & \text{wenn Turingmaschine } n \text{ bei Input } k \text{ nicht hält} \end{cases}$$

$$H_0(n) = \begin{cases} 1 & \text{wenn Turingmaschine } n \text{ bei Input leeres Band hält} \\ 0 & \text{wenn Turingmaschine } n \text{ bei Input leeres Band nicht hält} \end{cases}$$

Das ist nicht rekursiv; wir zeigen zuerst, dass die Funktion $G : \mathbb{N}_0 \to \mathbb{N}_0$ gegeben durch $G(n)$ ist die maximale Anzahl von Schritten, die eine Turingmaschine mit $\leq n$ Regeln, die schließlich hält, bei Input eines leeren Bandes zurücklegen kann, ist nicht rekursiv (sonst wäre die Busy Beaver-Funktion rekursiv). Wenn H rekursiv wäre, dann auch G; man müsste nur diejenigen Maschinen, die stehenbleiben werden ablaufen lassen und Ergebnisse vergleichen.

6.2 Formalisierungen von Berechenbarkeit

Satz 6.1 (Churchsche These (Church's thesis))**:** Die durch Turingmaschinen berechenbaren Funktionen entsprechen genau den Funktionen, für die ein "Algorithmus" existiert, der sie berechnet.

Da die Formulierung nicht exakt ist, sondern intuitiv-umgangssprachlich, ist sie nicht beweisbar (also auch kein Satz).

Plausibel wird Church's Thesis durch die Tatsache, dass alle bisherigen Versuche, "Berechenbarkeit" zu formalisieren, dieselbe Klasse von Funktionen geliefert haben, beispielsweise

- Turingmaschinen
- Registermaschinen: Register R_i, $i \in \mathbb{N}$, in denen jeweils eine Zahl aus $\mathbb{N}_0$ stehen kann (zu Beginn in r_1 der Input, sonst 0), und endlich viele mit $1, \ldots, n$ nummerierte Instruktionen I_k; jedes I_k ist dabei von einer der folgenden Formen:
  - $R_j := 0$
  - $R_j := R_j + 1$
  - $R_j := R_i$
  - if $R_j = R_i$ then goto I_m else goto I_ℓ

  (oder so ähnlich).

- Klasse der rekursiven Funktionen tatsächlich rekursiv definieren: Zuerst eine Teilmenge "primitiv rekursive Funktionen"; Initiale Funktionen: $f : \mathbb{N}_0^k \to \mathbb{N}_0$ von der Form
  - $f(k) = c$ konstante Funktion
  - $f(k) = k + 1$ Nachfolger
  - $f(k_1, \ldots, k_n) = k_i$ (für ein i mit $1 \leq i \leq n$) Projektion auf i-te Koordinate

  Zusammensetzung von Funktionen (Komposition) für $g : \mathbb{N}_0^m \to \mathbb{N}_0$, $h_i : \mathbb{N}_0^n \to \mathbb{N}_0$, $i = 1, \ldots, m$ sei die Zusammensetzung $f : \mathbb{N}_0^n \to \mathbb{N}_0$ definiert als:

  $$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

  Primitive Rekursion: $g : \mathbb{N}_0^n \to \mathbb{N}_0$, $h : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$ definieren ein $f : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$ wie folgt:

  $$f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n), \qquad f(k+1, x_1, \ldots, x_n) = h(k, x_1, \ldots, x_n, f(k, x_1, \ldots, x_n))$$

  Die kleinste Klasse von Funktionen, die die initialen Funktionen enthält und bezüglich Zusammensetzung und primitiver Rekursion abgeschlossen ist (Durchschnitt aller solcher Mengen von Funktionen), heißt Klasse der primitiv rekursiven Funktionen.

Beispiel: Beispiel für rekursive, nicht primitiv rekursive Funktionen (nach Ackermann):

$$A_0(x) = x + 1, \qquad A_{n+1}(0) = A_n(1), \quad A_{n+1}(x + 1) = A_n(A_{n+1}(x))$$

$A(n, x) = A_n(x)$, $A : \mathbb{N}_0^2 \to \mathbb{N}$ nicht primitiv rekursiv (aber rekursiv nach Church). Für alle $f : \mathbb{N}_0^2 \to \mathbb{N}$ primitiv rekursiv existiert n, so dass für alle a, b gilt

$$f(a, b) < A_n(\max(a, b))$$

Unbeschränkte Suche: gegeben $f : \mathbb{N}_0^{k+1} \to \mathbb{N}_0$. Definiere $g : \mathbb{N}_0^k \to \mathbb{N}_0$ durch

$$g(x_1, \ldots, x_k) = y \Leftrightarrow f(x_1, \ldots, x_k, y) = 0 \quad \text{und} \quad \forall z < y : f(x_1, \ldots, x_k, z) \text{ definiert und } \neq 0$$

$$g(x_1, \ldots, x_n) = \begin{cases} \min\{y \mid f(x_1, \ldots, x_k, y) = 0, \quad f(x_1, \ldots, x_k, z) \downarrow \text{, falls } z < y\} \\ \text{undefiniert, falls } \nexists y f(x_1, \ldots, x_k, y) = 0 \text{ oder } \exists y f(x_1, \ldots, x_k, y) \uparrow \\ \qquad \text{und } f(x_1, \ldots, x_k, z) \neq 0 \text{ für } z < y \end{cases}$$

Partiell rekursive Funktionen: die kleinste Menge von Funktionen, die die initialen Funktionen enthält und bezüglich Zusammenhang, primitiver Rekursion und unbeschränkter Suche abgeschlossen ist.

(Definition von Zusammensetzung, primitiver Rekursion adaptieren auf partielle Funktionen: f definiert genau dann, wenn alle Funktionen auf der rechten Seite definiert sind.)

f berechenbar: $x_1, \ldots, x_n$ fix: berechnen $g(x_1, \ldots, x_n)$: für $y = 0, 1, 2, \ldots$ $f(x_1, \ldots, x_n, y)$ berechnen: entweder man kommt (erstmals) zu einer Nullstelle, einem y mit $f(x_1, \ldots, x_n, y) = 0$, setze $g(x_1, \ldots, x_n) = y$, oder Berechnung läuft ewig (entweder keine Nullstelle, oder man gerät an ein y, so dass Berechnung von $f(x_1, \ldots, x_n, y)$ ewig läuft - dann g undefiniert.

6.3 Rekursive und Diophantische Mengen

Definition 6.3: Eine Teilmenge $S \subseteq \mathbb{N}_0$ heißt rekursiv, wenn ihre charakteristische Funktion $\chi_x : \mathbb{N}_0 \to \{0, 1\}$ definiert durch

$$\chi_S(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$$

rekursiv ist. $S \subseteq N_0$ heißt rekursiv aufzählbar, wenn es ein partiell rekursives f gibt, $f : \operatorname{dom} f \subseteq \mathbb{N}_0 \to \mathbb{N}_0$, so dass $S = \operatorname{Im} f = f(\mathbb{N}_0)$ (auch r.e. recursively enumerable, e.e. effectively enumerable).

Anmerkung: Eine rekursiv aufzählbare Menge $\neq \emptyset$ ist auch durch eine total rekursive Funktion aufzählbar: f partiell rekursiv mit $f(\mathbb{N}) = S$; konstruiere daraus total rekursives g. Berechnung von g:

- 1. Schritt: 1. Schritt der Berechnung von $f(0)$
- 2. Schritt: 2. Schritt der Berechnung von $f(0)$, erster Schritt der Berechnung von $f(1)$
- ...
- n-ter Schritt: n-ter Schritt der Berechnung von $f(0)$, ..., 1. Schritt der Berechnung von $f(n)$

Sobald erstmals die Berechnung eines $f(k)$ abbricht und einen Wert liefert, $g(0) := f(k)$, ab diesem Schritt $g(n)$ setzen auf den beim aktuellen Schritt aufgetauchten Wert von f, sonst auf $g(n-1)$

Satz 6.2: S rekursiv $\Leftrightarrow$ S und $\mathbb{N}_0 \subseteq S$ beide rekursiv aufzählbar.

Beweis: Übung (Egal, welche Definition von Berechenbarkeit man zugrunde legt: intuitiv klar). □

Beispiel: Rekursiv aufzählbare Menge, nicht rekursiv: Nummern jener Turingmaschinen, die bei 0 halten.

Definition 6.4: $S \subseteq \mathbb{N}^k$ heißt Diophantisch, wenn es ein Polynom $p \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_m]$ gibt, so dass $(a_1, \ldots, a_k) \in S \Leftrightarrow p(a_1, \ldots, a_k, y_1, \ldots, y_m)$ eine Nullstelle in $\mathbb{Z}^m$ hat.

Satz 6.3: Die Diophantischen Mengen sind genau die rekursiv aufzählbaren Mengen.

Beweis: Durch Matiyasievich et al. (Robinson, ...). □

Anmerkung: Folgerung: Hilberts 10. Problem, die Frage, ob es einen Algorithmus zur Entscheidung, ob ein Polynom in mehreren Variablen mit Koeffizienten in $\mathbb{Z}$, $p \in \mathbb{Z}[y_1, \ldots, y_n]$ eine Nullstelle in $\mathbb{Z}^m$ hat, gibt, hat die Antwort nein.

Ob man Nullstellen in $\mathbb{Z}^m$ oder $\mathbb{N}_0^m$ betrachtet, ist egal: $f \in \mathbb{Z}[y_1, \ldots, y_m]$ hat Nullstelle in $\mathbb{N}_0^m$ genau dann, wenn

$$g = f(y_{11}^2 + y_{12}^2 + y_{13}^2 + y_{14}^2, \ldots, y_{m1}^2 + y_{m2}^2 + y_{m3}^2 + y_{m4}^2)$$

eine Nullstelle in $\mathbb{Z}^{4m}$ hat, und $f \in \mathbb{Z}[y_1, \ldots, y_m]$ hat Nullstelle in $\mathbb{Z}^m$ genau dann, wenn

$$g = f(y_{11} - y_{12}, y_{21} - y_{22}, \ldots, y_{m1} - y_{m2})$$

eine Nullstelle in $\mathbb{N}_0^{2m}$ hat.

Die Unlösbarkeit von Hilberts 10. Problem folgt aus dem Satz "r.e. $\Leftrightarrow$ Diophantisch" so: Man wähle $S \subseteq \mathbb{N}_0$, S r.e., nicht rekursiv, dann $\exists p \in \mathbb{Z}[x, y_1, \ldots, y_m]$, so dass $p(s, y_1, \ldots, y_m)$ Nullstelle in $\mathbb{Z}^m$ hat genau wenn $s \in S$. Hätte man einen Entscheidungsalgorithmus für die Existenz ganzzahliger Nullstellen von $p(s, y_1, \ldots, y_m)$, dann wäre S rekursiv.

Anmerkung: Folgerung: $S \subseteq \mathbb{N}_0$ ist r.e. genau dann, wenn $\exists f \in \mathbb{Z}[x_1, \ldots, x_m]$, so dass $S = \mathbb{N}_0 \cap f(\mathbb{Z}^m)$. Sei S r.e., $Q \in \mathbb{Z}[x, y_1, \ldots, y_m]$, so dass $Q(s, y_1, \ldots, y_m)$ Nullstelle hat genau dann, wenn $s \in S$,

$$p(x, y_1, \ldots, y_m) = (x + 1) \cdot (1 - Q(x, y_1, \ldots, y_m)^2) - 1$$

Für x einsetzen $\in \mathbb{N}_0$, für $y_1, \ldots, y_m$ in $\mathbb{Z}$ einsetzen. s tritt als Wert von $p(\mathbb{N}_0 \times \mathbb{Z}^n) \cap \mathbb{N}_0$ auf genau dann, wenn $s \in S$. Für x einsetzen $x_1^2 + x_2^2 + x_3^2 + x_4^2$, dann ist p ein Polynom mit den erwünschten Eigenschaften.