Theoretische Informatik II

Contents

1 Aussagenlogik

Einheit 1 und 2 aus Vorlesung Nr.1

1.1 Syntax der Aussagenlogik

- Atomare Formeln ($A_i, i = 1, 2, 3$) sind Formeln.
  Atomare Formeln sind einfache Aussagen wie "Der Himmel ist Blau"
- Falls F und G Formeln sind, dann sind auch $(F \wedge G)$, $(F \vee G)$, $(F \Rightarrow G)$ und $(F \Leftrightarrow G)$ Formeln.
- Wenn F eine Formel ist, dann ist auch $\neg F$ eine Formel

1.2 Abkürzungen

- Namen ohne Index: $A, B, C, ...$ für $A_1, A_2, A_3, ...$
  In dem Fall $A = A_1; B = A_2; C = A_3; ...$
- Implikation $F_1 \to F_2$ steht für $(\neg F_1 \vee F_2)$
- Äquivalenz $F_1 \leftrightarrow F_2$ steht für $((F_1 \wedge F_2) \vee (\neg F_1 \wedge \neg F_2))$
- n-Faches Oder
  $$\bigvee_{i=1}^{n} F_i$$
  steht für $(...((F_1 \vee F_2) \vee F_3)... \vee F_n)$
- n-Faches Und
  $$\bigwedge_{i=1}^{n} F_i$$
  steht für $(...((F_1 \wedge F_2) \wedge F_3)... \wedge F_n)$

Beispiel:

$$\begin{aligned} B \leftrightarrow (C \to E) &= ((B \wedge A) \vee (\neg B \wedge \neg A)) \text{ [1]} \\ &= ((B \wedge (C \to E)) \vee (\neg B \wedge \neg(C \to E))) \text{ [2]} \\ &= ((B \wedge (\neg C \vee E)) \vee (\neg B \wedge \neg(\neg C \vee E))) \text{ [3]} \\ &= ((A_2 \wedge (\neg A_3 \vee A_5)) \vee (\neg A_2 \wedge \neg(\neg A_3 \vee A_5))) \text{ [4]} \end{aligned}$$

[1] Äquivalenzformel angewendet und $A = C \to E$
[2] A mit $C \to E$ ersetzt
[3] Implikationsformel angewendet
[4] Namen ohne Index angewendet aber andersherum

1.3 Semantik der Aussagenlogik

Sei D eine Teilmenge von Formeln $\{A_1, A_2, ...\}$.
Eine Abbildung $\mathcal{A} : D \to \{0, 1\}$ heißt **Belegung**.

Die Elemente in $\{0, 1\}$ heißen die **Wahrheitswerte**. Man schreibt 0 statt falsch und 1 statt wahr.

Durch eine Belegung erhält jede atomare Formel einen Wert.

- **Induktionsanfang:**
  Der Wert einer atomaren Formel A_i ist genau dann definiert, wenn $A_i \in D$ gilt, und er ist dann $\mathcal{A}(A_i)$.
- **Induktionsschritt:**
  Wir nehmen an, dass $\mathcal{A}(F)$ und $\mathcal{A}(G)$ definiert sind.
  - $\mathcal{A}(F \wedge G)$ sei das Minimum von $\mathcal{A}(F)$ und $\mathcal{A}(G)$
    $\mathcal{A}(F \wedge G) = 1 \leftrightarrow \mathcal{A}(F) = 1 \wedge \mathcal{A}(G) = 1$
  - $\mathcal{A}(F \vee G)$ sei das Maximum von $\mathcal{A}(F)$ und $\mathcal{A}(G)$
    $\mathcal{A}(F \wedge G) = 1 \leftrightarrow \mathcal{A}(F) = 1 \vee \mathcal{A}(G) = 1$
  - $\mathcal{A}(\neg F)$ sei definiert durch $\mathcal{A}(\neg F) = 1 - \mathcal{A}(F)$ $\mathcal{A}(\neg F) \leftrightarrow \mathcal{A}(F) = 0$

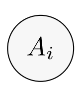
1.4 Verknüpfungstabellen

$\mathcal{A}(F)$	$\mathcal{A}(G)$	$\mathcal{A}(F \to G)$
0	0	1
0	1	1
1	0	0
1	1	1

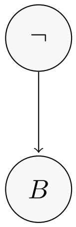
$\mathcal{A}(F)$	$\mathcal{A}(G)$	$\mathcal{A}(F \leftrightarrow G)$
0	0	1
0	1	0
1	0	0
1	1	1

1.5 Baumstruktur für Formeln

1. Für atomare Formeln wird ein Knoten, in den als Label die atomare Formel eingetragen:

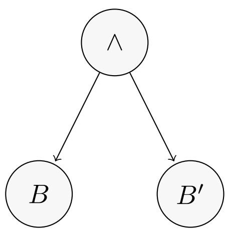


2. Für $\neg F$ wird ein Knoten, in den als Label die Verknüpfung eingetragen ist, darunter ein Baum B für F:

   In dem Fall ist B der Baum für F.
   Man kann das so allgemeinern, weil z.B kann F auch $A_1 \leftrightarrow A_2$ sein.

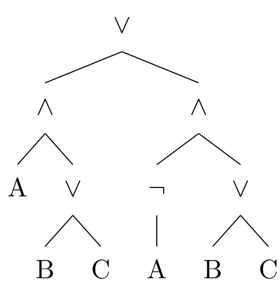
3. Für $F \wedge G$ wird ein Knoten, in den als Label $\wedge$ eingetragen ist, darunter Bäume für F und G:

   Analog zu Punkt 2. ist B ein Baum für F und B' ein Baum für G.

   Das gleiche gilt auch für $\vee$.

   Beispiel von einer Baumstruktur:
   Formel: $((A \wedge (B \vee C)) \vee (\neg A \wedge (B \vee C)))$

   Man wertet den Syntaxbaum von unten nach oben ab.

1.6 Modelle, Gültigkeit, Erfüllbarkeit und Tautologie

Sei F eine Formel und sei $\mathcal{A} : M \rightarrow \{0, 1\}$ eine Belegung.
M ist hierbei die Teilmenge der Formeln.

- Sind alle in F vorkommenden atomaren Formeln im Definitionsbereich von $\mathcal{A}$ enthalten, so heißt $\mathcal{A}$ zu F **passend**.
  Sei $F = A \wedge B$ mit $\mathcal{A}(A) \in \{0, 1\}$, dann ist F passend.
- Ist $\mathcal{A}$ zu F passend und gilt $\mathcal{A}(F) = 1$, so schreiben wir $\mathcal{A} \vDash F$. Wir sagen, dass F unter der Belegung $\mathcal{A}$ gilt und nennen $\mathcal{A}$ ein **Modell** für F.
- Ist $\mathcal{F}$ eine Menge von Formeln, so heißt $\mathcal{A}$ ein **Modell** für $\mathcal{F}$, wenn für alle $F \in \mathcal{F}$ gilt: $\mathcal{A} \vDash F$. In diesem Fall wird dann $\mathcal{A} \vDash \mathcal{F}$ geschrieben.
  Aufgeteilt: Falls alle Formeln in $\mathcal{F}$ die Bedingung "$\mathcal{A}$ ist passend zu F" und die Bedingung "$\mathcal{A}(F) = 1$" für alle $F \in \mathcal{F}$ erfüllt, dann ist $\mathcal{A}$ ein Modell für $\mathcal{F}$
- F ist **erfüllbar**, wenn es ein Modell für F gibt.
  Es existiert eine Belegung $\mathcal{A}$, die zu F passend ist, mit $\mathcal{A}(F) = 1$.
- F ist **gültig**, falls für alle $\mathcal{A}$, die zu F passend sind, $\mathcal{A}(F) = 1$ gilt.
- Eine **Tautologie** ist eine gültige Formel F.

1.7 Zusammenhang Erfüllbarkeit/Tautologie

$$F\ ist\ Tautologie \Leftrightarrow \neg F\ ist\ unerf\ddot{u}llbar$$

1.8 Das Spiegelungsprinzip

- Gültige Formeln werden durch Negation zu unerfüllbaren Formeln.
- Unerfüllbare Formeln werden durch Negation zu gültigen Formeln.
- Erfüllbare, nicht gültige Formeln werden durch Negation wieder zu erfüllbaren, nicht gültigen Formeln.

1.9 Wahrheitswerteverlauf

Der Wahrheitswert von F unter passender Belegung $\mathcal{A}$ hängt **nur** vom Wahrheitswert der atomaren Formeln in F ab.
Dadurch kann man Erfüllbarkeit, Gültigkeit und ähnliche Eigenschaften bei F testen, indem man Wahrheitstabellen erstellt.

Für die Spalten setzt man $A_1, ..., A_n$ und F ein.
Anzahl der Spalten ist die Anzahl aller Teilformeln von F
Für die Zeilen setzt man A_i mit $i = 1, ..., 2^n$
Anzahl der Zeilen ist $2^{Anzahl\ atomare\ Formeln}$

Beispiel:
In dem Fall hat $\equiv$ die gleiche Bedeutung wie $\Leftrightarrow$, aber es wird später mehr erläutert.
$F := (A \wedge B) \equiv (B \wedge A)$

Wahrheitstabelle

Belegung $\mathcal{A}$	A	B	$A \wedge B$	$B \wedge A$	$A \wedge B \equiv B \wedge A$
1	0	0	0	0	1
2	0	1	0	0	1
3	1	0	0	0	1
4	1	1	1	1	1

Jede einzelne Zeile entspricht einer Belegung $\mathcal{A}$
Teilformel: Eine Formel, die in F ist. Nach Definition sind atomare Formeln Formeln und alle Verknüpfungen zwischen 2 atomaren Formeln auch Formeln.

- Alle $\mathcal{A}$ sind zu F passend, weil alle atomaren Formeln im Definitionsbereich von $\mathcal{A}$ liegen.
- Bei der ersten Belegung ist $\mathcal{A}$ ein Modell für F, weil $\mathcal{A}$ passend zu F ist und $\mathcal{A}(F) = 1$ gilt.
  $\Rightarrow F$ ist erfüllbar.
- Bei allen Belegungen $\mathcal{A}$ gilt, dass alle $\mathcal{A}$ passend zu F ist und $\mathcal{A}(F) = 1$ gilt.
  $\Rightarrow F$ ist gültig und eine Tautologie.

1.10 Äquivalenz aussagenlogischer Formeln

F und G heißen **semantisch äquivalent**, wenn für alle zu beiden passenden Belegungen $\mathcal{A}$ gilt:

$$\mathcal{A}(F) = \mathcal{A}(G)$$

In diesem Fall schreiben wir $F \equiv G$.

1.11 Das Ersetzbarkeitstheorem

Sei H eine Formel, in der F als Teilformel vorkommt.
Sei G eine zu F äquivalente Formel.
Sei H' die Formel, die aus H entsteht, wenn F durch G ersetzt wird.
Dann sind H und H' äquivalent.
Äquivalentes Ersetzen von Teilformeln erhält Äquivalenz!

Beispiel:

$$\begin{aligned}
\delta &= (B \to (A \land (A \lor B))) \\
\alpha &= (A \land (A \lor B)) \\
\beta &= A \\
\delta' &= (B \to A)
\end{aligned}$$

$$\begin{aligned}
\delta &= (B \to (A \land (A \lor B))) \text{ [1]} \\
&= (B \to \alpha) \text{ [2]} \\
&= (B \to \beta) \text{ [3]} \\
&= (B \to A) \\
&= \delta'
\end{aligned}$$

[1] Formel eingesetzt.
[2] α eingesetzt, weil es gleich ist.
[3] Da $\alpha \equiv \beta$ (Beweis durch Wahrheitstabelle), wird α durch β ersetzt.

2 Normalformen der Aussagenlogik

Einheit 3 aus Vorlesung Nr.2

2.1 Äquivalenzen

- **Idempotenz:**

$$F \equiv (F \land F) \equiv (F \lor F)$$

- **Kommutativität:**

$$(F \land G) \equiv (G \land F) \quad (F \lor G) \equiv (G \lor F)$$

- **Assoziativität:**

$$((F \land G) \land H) \equiv (F \land (G \land H))$$
$$((F \lor G) \lor H) \equiv (F \lor (G \lor H))$$

- **Absorption:**

$$(F \land (F \lor G)) \equiv F \equiv (F \lor (F \land G))$$

- **Distributivität:**

$$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H))$$
$$(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H))$$

- **Doppelnegation:**

$$\neg\neg F \equiv F$$

- **deMorgan-Regeln:**

$$\neg(F \wedge G) \equiv (\neg F \vee \neg G) \quad \neg(F \vee G) \equiv (\neg F \wedge \neg G)$$

- **Tautologie:**
  Falls F eine Tautologie ist, gelten folgende Äquivalenzen:

$$(F \vee G) \equiv F \quad (F \wedge G) \equiv G$$

- **Unerfüllbarkeit:**
  Falls F unerfüllbar ist, dann gelten folgende Äquivalenzen:

$$(F \vee G) \equiv G \quad (F \wedge G) \equiv F$$

2.2 Assoziativität und Klammerung

Man darf sich erlauben, Klammerungen bei zusammengesetzten $\wedge$ oder $\vee$ Formeln (bzw. Teilformeln) wegzulassen.

Beispiel:
Wir schreiben $A \vee B \vee C$ sowohl für $((A \vee B) \vee C)$ als auch für $(A \vee (B \vee C))$

Wichtig:
Nicht zu viele Klammern wegmachen!
Was würde dann bei $A \wedge B \vee C$ passieren?

2.3 Normalformen

- Ein **positives Literal** ist eine atomare Formel.
- Ein **negatives Literal** ist die Negation einer atomaren Formel.

Definitionen:

- Eine Formel F ist in disjunkter Normalform (DNF), wenn sie eine Disjunktion von Konjunktionen von Literalen ist.
- Die Formel F ist in konjunktiver Normalform (KNF), wenn sie eine Konjunktion von Disjunktionen von Literalen ist

2.4 Satz (DNF/KNF)

Zu jeder Formel existieren äquivalente Formeln in DNF und in KNF.

2.5 KNF-Algorithmus

1. Negationen nach innen schieben (deMorgan-Regeln) und dabei Doppelnegationen eliminieren.
2. Zweites Distributivgesetz nutzen, um $\vee$-Operationen vorbei nach innen zu schieben.

Dabei wird die Ausgangsformel nur mit $\neg$, $\vee$ und $\wedge$ gebildet.

Beispiel:

$$
\begin{aligned}
(\neg(A \wedge \neg(C \vee \neg B)) \vee \neg(\neg D \vee (B \wedge A))) &\equiv (\neg(A \wedge (\neg C \wedge B)) \vee (D \wedge \neg(B \wedge A))) \text{ [1]} \\
&\equiv ((\neg A \vee (C \vee \neg B)) \vee (D \wedge (\neg B \vee \neg A))) \text{ [2]} \\
&\equiv (\neg A \vee C \vee \neg B \vee D) \wedge (\neg A \vee C \vee \neg B \vee \neg B \vee \neg A) \text{ [3]}
\end{aligned}
$$

Dabei ist die letzte Formel in KNF.
[1a] deMorgansche-Regeln bei beiden. (Doppelnegierungen werden weggestrichen)
[2a] deMorgansche-Regeln erneut.
[3a] Da spielt das 2. Distributivgesetz eine große Rolle:

$$
\begin{aligned}
((\neg A \vee (C \vee \neg B)) \vee (D \wedge (\neg B \vee \neg A))) &\equiv (\neg A \vee C \vee \neg B) \vee (D \wedge (\neg B \vee \neg A)) \text{ [1]} \\
&\equiv (\neg A \vee C \vee \neg B \vee D) \wedge (\neg A \vee C \vee \neg B \vee \neg B \vee \neg A) \text{ [2]}
\end{aligned}
$$

[1b] Rot ist F, Blau ist G und Grün ist H. Dabei erhält man die Formel $(F \vee (G \wedge H))$ und diese ist äquivalent zu $((F \vee G) \wedge (F \vee H))$ (2. Distributivformel)
[2b] Die Formel aus der Beschreibung von [1b] angewendet.

2.6 KNF aus der Wahrheitstafel

A	B	C	F
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

1. Betrachte alle Fälle, wo F gleich 0 ist.
2. Um eine Zeile mit Null zu "vermeiden", muss mindestens eine der atomaren Formeln den Wert 1 annehmen
3. Wiederhole das alles auch bei den anderen Zeilen mit Null und verknüpfe sie mit $\wedge$

Resultat:
Aus Zeile 1: $(A \vee B \vee C)$
Aus Zeile 4: $(A \vee \neg B \vee \neg C)$
Aus Zeile 8: $(\neg A \vee \neg B \vee \neg C)$
Daraus ergibt sich

$$F \equiv F' = (A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C)$$

2.7 DNF aus der Wahrheitstafel

A	B	C	F
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Für den DNF muss man umgekehrt die positiven Fälle betrachten und mit $\vee$ verknüpfen.

Also:
Zeile 2: $(\neg A \wedge \neg B \wedge C)$
Zeile 3: $(\neg A \wedge B \wedge \neg C)$
Zeile 5: $(A \wedge \neg B \wedge \neg C)$
Zeile 6: $(A \wedge \neg B \wedge C)$
Zeile 7: $(A \wedge B \wedge \neg C)$

Damit erhält man die äquivalente Formel in DNF:
$F \equiv F' = (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C)$
$\vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$

3 Prädikatenlogik erster Stufe

Einheit 4 aus Vorlesung Nr.2

3.1 Grundbegriffe der Prädikatenlogik

Die Aussagenlogik kann folgendes nicht ausdrücken:

- Für alle Objekte einer gewissen Art gilt ...
- Es gibt ein Objekt einer gewissen Art mit ...
- **Funktionen** und **Relationen**.

Deswegen gibt es die Prädikatenlogik (erster Stufe)

Man verwendet drei Sorten von Objekten

- Eine **Variable** hat die Form x_i für ein $i \in \{1, 2, ...\}$
- Ein **Prädikatsymbol** hat die Form P_i^k für ein $i \in \{1, 2, ...\}$ und ein $k \in \{0, 1, 2, ...\}$
- Ein **Funktionssymbol** hat die Form f_i^k für ein $i \in \{1, 2, ...\}$ und ein $k \in \{0, 1, 2, ...\}$

Dabei ist i ein Index, der es ermöglicht, eine beliebige Anzahl dieser Objekte zu verwenden. i heißt auch **Unterscheidungsindex**.
k ist die **Stelligkeit** oder Stellenzahl von P_i^k bzw. f_i^k

3.2 Syntax der Prädikatenlogik

Die Menge der **Terme** wird so induktiv definiert

- Wenn P ein k-stelliges Prädikatensymbol ist und $t_1, ..., t_k$ Terme sind dann ist $P(t_1, ..., t_k)$ eine **atomare Formel**.
- Mit F und G sind auch $\neg F$, $(F \wedge G)$ und $(F \vee G)$ Formeln
- Ist F eine Formel und x eine Variable, dann sind auch $\exists x F$ und $\forall x F$ Formeln

3.3 Semantik der Prädikatenlogik

Zweck ist es, den benutzten Variablen, Funktionssymbolen und Prädikatsymbolen einen realen Sinn zuzuordnen.

Dafür werden Individuen benutzt, also mögliche Werte für die Variablen und Terme,
sowie eine Zuordnung der Funktions- und Prädikatsymbole zu realen Funktionen und Prädikaten.

Prädikatenlogische Formeln wird mit einer Struktur interpretiert:

- Gegeben ist ein Paar $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$.
  Dabei ist das Paar $\mathcal{A}$ eine Struktur.
- $U_\mathcal{A}$ heißt **Menge der Individuen**.
- $I_\mathcal{A}$ ist eine Abbildung, die jedem (in der Formel benutzen) Prädikatsymbol P_i^k bzw. Funktionssymbol f_i^k ein dazu passendes Prädikat/eine passende Funktion zuordnet, sowie jeder benutzten Variablen x_i einen Wert aus $U_\mathcal{A}$.

Beispiele:

- Aus welcher Menge kommt $I_\mathcal{A}(f_3^0())$? Lösung: $U_\mathcal{A}$
- Aus welcher Menge kommt $I_\mathcal{A}(P_4^3))$? Lösung: $\mathcal{P}(U_\mathcal{A} \times U_\mathcal{A} \times U_\mathcal{A})$
- Aus welcher Menge kommt $I_\mathcal{A}(f_3^2)$? Lösung: $U_\mathcal{A} \times U_\mathcal{A} \rightarrow U_\mathcal{A}$

3.4 Beispiel für Strukturen/Werte von Termen

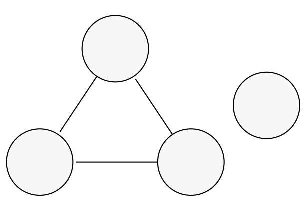
Man geht von einer gegebenen Formel aus, wie z.B:

$$F = \forall x \exists y \exists y'((P(x, y) \wedge P(x, y')) \wedge \forall z(\neg P(x, z) \vee (Q(y, z) \vee Q(y', z))))$$

Ignoriere noch diese Formel, falls du sie nicht verstehst

Als **Individuenbereich** $U_\mathcal{A}$ nimmt man häufig $\mathbb{N}$ - das muss aber nicht sein. Durch $I_\mathcal{A}$ müssen dann alle freien Variablen, Prädikate und alle Funktionen definiert werden. In dem Fall wählen wir jetzt

$U_\mathcal{A} = V$ für einen ungerichteten Graphen $G = (V, E)$
Ein ungerichteter Graph ist nicht anders als z.B. ein Graph von einem Automaten oder von einem Syntaxbaum:



Dabei ist V die Menge der Knoten (Kreise) und E die Menge der Kanten (Verbindungen zwischen 2 Knoten) mit $E \subseteq V \times V$
$I_\mathcal{A}(P) = P^\mathcal{A} = \{(u, v) \mid u, v \in V \text{ und } \{u, v\} \in E\}$ (Kantenrelation)
Anders ausgedrückt: P ist eine zweistellige Funktion und sind beide Knoten miteinander verbunden? Wahr wenn ja, falsch wenn nein.
$I_\mathcal{A}(Q) = Q^\mathcal{A} = \{(u, u) \mid u \in V\}$ (Gleichheit)
Anders ausgedrückt: Q ist eine zweistellige Funktion und sind beide Knoten gleich? Wahr wenn ja, falsch wenn nein.

Zur Funktion F gibt es zwei Teile:

$$F = \forall x \exists y \exists y' ((P(x,y) \wedge P(x,y')) \wedge \forall z(\neg P(x,z) \vee (Q(y,z) \vee Q(y',z))))$$

Die linke Seite sagt es existieren für alle Knoten x zwei andere Knoten, die mit x verbunden sind.
Die rechte Seite sagt es gilt für alle Knoten in z, dass der Knoten x entweder nicht mit dem Knoten z verbunden ist oder das der Knoten z der Knoten y oder y' ist.
Kannst die rechte Seite auch so betrachten (Implikationsformel in 1.2):

$$P(x,z) \rightarrow (Q(y,z) \vee Q(y',z))$$

"Wenn x und z zusammen eine Kante haben, dann ist z entweder y oder y'.
Die ganze Formel F sagt dann, dass ein Knoten nur mindestens eine Kante oder höchstens zwei Kanten haben kann.

Durch das Paar $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$ können nun allen Termen Werte aus $U_\mathcal{A}$ zugewiesen werden wie folgt:

- Eine (freie) Variable x_i erhält den Wert $I_\mathcal{A}(x_i)$
- Ein Term der Form $f_i^k(t_1, ..., t_k)$ erhält den Wert $I_\mathcal{A}(f_i^k)(u_1, ..., u_k)$ wenn die t_i jeweils den Wert u_i haben.

Den Wert des Terms t in der Struktur $\mathcal{A}$ bezeichnet man mit $\mathcal{A}(t)$.
Also: $\mathcal{A}(t) \in U_\mathcal{A}$ für alle Terme t.

3.5 Wahrheitswerte von Formeln

Die atomare Formel $F = P(t_1, ..., t_k)$ ist wahr, falls $(\mathcal{A}(t_1), ..., \mathcal{A}(t_k)) \in P^\mathcal{A}$ gilt.
Wir schreiben dann $\mathcal{A}(F) = 1$.
Andernfalls ist dann $\mathcal{A}(F) = 0$, bzw. F ist nicht wahr.
Die Definitionen von $\mathcal{A}(\neg F)$, $\mathcal{A}(F \wedge G)$ und $\mathcal{A}(F \vee G)$ sind gleich zum aussagenlogischen Fall

Ist $F = \forall x G$, so definieren wir $\mathcal{A}(F)$ so:

- $\mathcal{A}(F) = 1$, falls $\forall \alpha \in U_\mathcal{A} : \mathcal{A}_{[x/\alpha]}(G) = 1$
- $\mathcal{A}(F) = 0$, sonst

Ist $F = \exists x G$, so definieren wir $\mathcal{A}(F)$ so:

- $\mathcal{A}(F) = 0$, falls $\forall \alpha \in U_\mathcal{A} : \mathcal{A}_{[x/\alpha]}(G) = 0$
- $\mathcal{A}(F) = 1$, sonst

Hierbei ist $\mathcal{A}_{[x/\alpha]}$ die Struktur, die überall mit $\mathcal{A}$ übereinstimmt, nur für x gilt jetzt $\mathcal{A}_{[x/\alpha]}(x) = \alpha$, unabhängig vom ursprünglichen Wert $\mathcal{A}(x)$.

3.6 Das Zahlenbeispiel

Betrachte die Formel

$$F = \forall x P(x, f(x)) \wedge Q(g(a, z))$$

Grundbereich sei $\mathbb{N}$, P sei die <-Relation, Q die Primzahleigenschaft, f die Nachfolgerfunktion auf $\mathbb{N}$, g die Addition, a die Konstante 2. Das heißt: a ist eine nullstellige Funktion mit dem Wert 2.
Schließlich geben wir der Variablen z den Wert 3.
Übersetzte Formel mit den ganzen gegebenen Sachen:
$F = (\forall x \in \mathbb{N} : x < x + 1) \wedge (2 + 3 \text{ ist eine Primzahl})$

Mit der gegebenen Struktur hat man folgende Interpretation:
Für alle Zahlen x gilt: $x < x+1$, und die Summe von a und z ist eine Primzahl.

Dabei ist F wahr, weil $x < x + 1$ ist richtig und die Summe von 2 und 3 ist eine Primzahl.

3.7 Das abstrakte Beispiel

Man bildet jetzt $U_{\mathcal{A}}$ aus allen Termen, die man mit den beteiligten Funktionen bilden kann, ohne Variablen zu benutzen:

$$\{a, f(a), f(f(a)), f(f(f(a))), ..., g(a, a), g(f(a), a), f(g(a, a)), ...\}$$

- In a kann nichts eingesetzt werden.
- In f kann bzw. muss man jeweils einen vorher gebildeten Term einsetzen.
- In g werden jeweils zwei vorher gebildete Terme eingesetzt.

Man braucht eine induktive Definition, also:
Alle vorkommenden nullstelligen Funktionen gehören zu $U_{\mathcal{A}}$.
Wenn es keine gibt, dann $a \in U_{\mathcal{A}}$

Wenn f_i^k eine vorkommende k-stellige Funktion ist und $t_1, ..., t_k$ Elemente von $U_{\mathcal{A}}$ sind, dann gehört auch

$$f_i^k(t - 1, ..., t_k)$$

zu $U_{\mathcal{A}}$
$I_{\mathcal{A}}$ würde dann so aussehen: $\forall t \in U_{\mathcal{A}} : I_{\mathcal{A}}(t) = t$

3.8 Modelle, Gültigkeit, Erfüllbarkeit

- Die Struktur $\mathcal{A} = (U_{\mathcal{A}}, I_{\mathcal{A}})$ ist eine zu **F passende Struktur**, falls $I_{\mathcal{A}}$ jeder in F vorkommenden Variablen einen Wert aus $U_{\mathcal{A}}$ zuweist, jedem in F vorkommenden Prädikatsymbol P_i^k ein k-stelliges Prädikat über $U_{\mathcal{A}}$, und jedem in F vorkommenden Funktionssymbol f_i^k eine k-stellige Funktion auf $U_{\mathcal{A}}$ hat.

- Eine zu F passende Struktur $\mathcal{A}$ nennen wir ein **Modell für F**, wenn der Wahrheitswert der Formel in der Struktur $\mathcal{A}$ der Wert 1 ist, d.h. wenn $\mathcal{A}(F) = 1$ gilt.
  Man sagt auch "F gilt in $\mathcal{A}$" und schreibt $\mathcal{A} \vDash F$.
- Eine prädikatenlogische Formel F heißt **erfüllbar**, wenn es ein Modell für F gibt.
- Man nennt eine prädikatenlogische Formel F **allgemeingültig**, wenn alle zu F passenden Strukturen Modelle für F sind. Dann schreiben wir $\vDash F$.
- Wenn F nicht allgemeingültig ist, schreiben wir $\nvDash F$

4 Churchsche These

Einheit 5 aus Vorlesung Nr.3

4.1 Berechenbarkeitstheorie

- Intuitiver Berechenbarkeitsbegriff.
- Funktion $f : \mathbb{N}^k \to \mathbb{N} \Leftrightarrow$ Algorithmus.
- Partielle Funktionen (unendliche Schleife) zugelassen.

  Beispiel:

  ```
  INPUT(n);
  REPEAT UNTIL FALSE
  ```

  Dabei ist $f : \mathbb{N} \to \mathbb{N}, f(n)$ undefiniert $\forall n$. Diese Funktion wird oft als Ω notiert und "nirgends definierte Funktion" bezeichnet.

4.2 Beispiele

$$f(n) = \begin{cases} 1, & \text{Falls n } \textbf{Anfangsabschnitt} \text{ der Dezimalbruchentwicklung von } \pi \textbf{ ist}. \\ 0, & \text{sonst} \end{cases}$$

$$g(n) = \begin{cases} 1, & \text{Falls n } \textbf{Anfangsabschnitt} \text{ der Dezimalbruchentwicklung von } \pi \textbf{ vorkommt}. \\ 0, & \text{sonst} \end{cases}$$

Dabei ist f berechenbar und von g weiß man nicht.

$$h(n) = \begin{cases} 1, & \text{falls in der Dezimalbruchentwicklung von } \pi \text{ an irgendeiner Stelle } \textbf{n mal hintereinander} \text{ eine 7} \\ 0, & \text{sonst} \end{cases}$$

Sei $n = 2$, dann würde $f(n) = 1$ sein, wenn z.B: $\pi = 3.14...77...$ vorkommt. (Ich habe das nicht überprüft, ob das wahr ist.)

$$i(n) = \begin{cases} 1, & \text{falls Problem } \mathbf{X} \text{ (X sei ein offenes Problem) positiv lösbar.} \\ 0, & \text{sonst} \end{cases}$$

4.3 Chursche These

Die durch die formale Definition der **Turing-Berechenbarkeit** (oder auch WHILE-Berechenbarkeit, GOTO-Berechenbarkeit, μ-Rekursivität) beschriebene **Klasse von Funktionen** stimmt mit der Klasse der **im intuitiven Sinne** berechenbaren Funktionen überein.

4.4 Turing-Berechenbarkeit

4.4.1 Definition

$f : \mathbb{N}^k \to \mathbb{N}$ heißt **Turing-Berechenbar**, falls es eine DTM M gibt, so dass $f(n_1, ..., n_k) = m$ genau dann gilt, wenn M, gestartet in Anfangszustand mit dem k-Tupel $n_1, ..., n_k$ auf ihrem Band (in Binärdarstellung, mit Trennzeichen zwischen den Komponenten) nach endlich vielen Schritten einen Endzustand erreicht mit Bandinhalt m. Bei einem undefinierten Wert läuft die Maschine unendlich lange.
Das auch Analog zu $f : \Sigma^* \to \Sigma^*$

4.4.2 Beispiele

- Man betrachte die Dekrement Funktion:
  $f : \mathbb{N} \to \mathbb{N}$
  $f(n) = n - 1$, falls $n > 0$
  $f(0) = 0$

  Man schreibt $f(n) = n - 1$ und man spricht von **modifizierter** Substraktion.

  Es gilt allg. $a - b = max\{0, a - b\}$

- Auch die nirgends definierte Funktion ist Turing-berechenbar:

  $\Omega : \mathbb{N} \to \mathbb{N}$
  $\Omega(n)$ ist undefiniert $\forall n$.
  Beweis:
  $(q_0, x) \mapsto (q_0, x, R) \quad \forall x$

- $$f : \mathbb{N}^2 \to \mathbb{N} \quad f(a, b) = a + b$$

- $$g : \mathbb{N}^2 \to \mathbb{N} \quad g(a,b) = a - b$$

- $$h : \mathbb{N}^2 \to \mathbb{N} \quad h(a,b) = a \cdot b$$

- $$i : \mathbb{N}^2 \to \mathbb{N} \quad i(a,b) = \lfloor a/b \rfloor, \text{ falls } b \neq 0$$
  $$i(a,0) = a$$

Bedeutung von $\lfloor a/b \rfloor$:
Die "Klammer" um a/b ist nichts anderes als eine Abrundung von Dezimalzahlen. Bsp: $\lfloor 1,8 \rfloor = 1$. Das wird in der Funktion angewendet, damit das Ergebnis in den natürlichen Zahlen bleibt.

5 Mehrband-Turingmaschinen

Einheit 6 aus Vorlesung Nr.3

5.1 Definition

- Das gleiche wie eine 1-Band-TM, aber nur mit mehreren Bändern.
- Pro Band ein Schreib- und Lesekopf.
- Übergangsfunktion: $Q \times \Gamma^k$ nach $Q \times \Gamma^k \times \{L, R, N\}^k$.

Satz:
Zu jeder Mehrband-Turingmaschine M gibt es eine 1-Band-TM M' mit $L(M) = L(M')$ bzw. bei Funktionenberechnung so, dass M und M' dieselbe Funktion berechnen.

5.2 Notation für spezielle Turingmaschinen

Sei M eine 1-Band-TM:

- $M(i,k)$ bezeichnet die k-Band-Maschine, die wie M arbeitet, wobei Band i als Arbeitsband benutzt wird. Die übrigen Bänder bleiben ungenutzt.

  In dem Fall bedeutet das, dass der Übergang von M
  $$\delta(q,a) = (q', b, y)$$
  in $M(i,k)$ zu folgendem Übergang wird
  $$\delta(q, c_1, ..., c_{i-1}, a, c_{i+1}, ..., c_k) =$$
  $$(q', c_1, ..., c_{i-1}, b, c_{i+1}, ..., c_k, N, ..., N, y, N, ..., N)$$

- Wenn der Wert von k uninteressant ist, schreiben wir $M(i)$.

5.3 Weitere Schreibweisen

- $Band := Band + 1$ oder $Band := Band - 1$
- $Bandi := Bandi + 1$ oder $Bandi := Bandi - 1$
  Sei M eine Maschine, die die Inkrement-Funktion berechnet.
  M' entsprechend für die Dekrement-Funktion.
  Dann sind $M(i)$ und $M'(i)$ die Maschinen für $Bandi := \pm 1$.
- $Bandi := 0$
  Man beginnt mit einer Maschine M für $Band := 0$.
  Dann ist $M(i)$ die gesuchte Maschine.
- $Bandi := Bandj$

5.4 Hintereinanderausführung

- **Flussdiagrammnotation:**

$$start \rightarrow M_1 \rightarrow M_2 \rightarrow stop$$

- **Programmiersprachen-Notation:**

$$M_1; M_2$$

- **Bedeutung:**

  Die Maschinen M_i seien als 7-Tupel $(Q_i, \Sigma, \Gamma_i, \delta_i, q_i, \Box, F_i)$ gegeben.
  Dabei sei ohne Beschränkung der Allgemeinheit $Q_1 \cap Q_2 = \varnothing$.
  Als $M_1; M_2$ bezeichnet man dann folgende Maschine M:

$$M = (Q_1 \cup Q_2, \Sigma, \Gamma_1 \cup \Gamma_2, \delta, q_1, \Box, F_2)$$

  mit

$$\delta = \delta_1 \cup \delta_2 \cup \{(q, a, q_2, a, N) \mid q \in F_1, a \in \Gamma_1\}$$