Theoretische Informatik

Prof. Dr. Barbara Staehle

HTWG Konstanz
Fakultaet für Informatik

WS 2021/2022

Teil I

Wiederholung und Grundlagen

Woran Sie sich in dieser Vorlesung und in Ihrem weiteren Leben erinnern sollten

Teil I Wiederholung und Grundlagen

Abschnitt 1

Grundlagen der Mengenlehre

Definition und Beispiele

Beispiele von Mengen

- S: Die Menge aller Studierenden der HTWG
- S_I: Die Menge aller Studierenden an der Fakultät IN der HTWG
- $\mathbb{N}$: Die Menge der natürlichen Zahlen
- $\mathbb{Z}$: Die Menge der ganzen Zahlen

Definition (Cantor, 1885)

Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohl unterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen.

Achtung: Der Barbier von Sevilla rasiert alle Männer, die sich nicht selbst rasieren. Rasiert der Barbier sich selbst?

Dieser „Definitionsfehler“ heißt Russelsche Antinomie und zeigt, dass die obige Definition zu einfach ist. Für uns reicht sie aber aus, korrektere Definition durch die ZFC Axiome (nach Zermelo und Fraenkel) siehe [Hoffmann, 2011].

Schreibweisen

$a \in M$	a ist ein Element von M
$a \notin M$	a ist kein Element von M
$M_1 = M_2$	M_1 und M_2 sind gleich, enthalten exakt die gleichen Elemente.
$M_1 \neq M_2$	M_1 und M_2 sind ungleich, es existiert also mindestens ein Element, dass nur in M_1 oder in M_2 ist.
$M = \emptyset, M = \{\}$	M ist die leere Menge, M enthält kein Element.
$\lvert M \rvert = m$	M enthält genau m viele Elemente Die Kardinalität von M ist gleich m.

Folgerungen

- $|\emptyset| = 0$
- Wenn $M_1 = M_2$ gilt, dann $|M_1| = |M_2|$
- Wenn $M_1 \subseteq M_2$ gilt, dann $|M_1| \leq |M_2|$.

Beschreibung von Mengen

Aufzählende Beschreibung Explizite Auflistung der Elemente der Menge; auch für (unendlich) große Mengen möglich, falls diese aufzählend beschreibbar sind; z.B.

- $D = \{0, 1\}$
- $\mathbb{N} = \{1, 2, 3, \dots\}$
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- $A = \{a, b, c, \dots, z\}$
- $M_1 = \{2, 4, 6, 8, 10, \dots\}$
- $M_2 = \{1, 4, 9, 16, 25, \dots\}$

Deskriptive Beschreibung Eindeutige Beschreibung der Elemente durch eine charakteristische Eigenschaft; „mit der Eigenschaft“ abgekürzt als „ | “ oder „:“; z.B.

- $S = \{s : s \text{ studiert an der HTWG}\}$
- $S_I = \{s \in S \mid s \text{ studiert AIN, GIB, WIN oder MSI}\}$
- $M_3 = \{n \in \mathbb{N} \mid n \bmod 2 = 0\}$
- $M_4 = \{n^2 \mid n \in \mathbb{N}\}$

Spezielle Mengen

$\mathbb{N}$ $= \{1, 2, 3, \ldots\}$, die Menge der natürlichen Zahlen

$\mathbb{N}_0$ $=\{0, 1, 2, 3, \ldots\}$, die Menge der natürlichen Zahlen und der 0

$\mathbb{Z}$ $=\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, die Menge der ganzen Zahlen (engl. integers)

$\mathbb{Q}$ $=\{\frac{p}{q} \mid p, q \in \mathbb{Z} \wedge q \neq 0\}$, die Menge der rationalen Zahlen

$\mathbb{R}$ ist die Menge der reellen Zahlen

$\mathbb{R}^+$ ist die Menge der reellen positiven Zahlen

$\mathbb{C}$ ist die Menge der komplexen Zahlen

Achtung: Viele Informatiker betrachten die 0 als natürliche Zahl. In dieser Vorlesung ist dies NICHT der Fall, daher gilt $\mathbb{N} \neq \mathbb{N}_0$.

Beziehungen zwischen Mengen

$M_1 \subseteq M_2$ M_1 ist eine Teilmenge oder Untermenge von M_2: aus $M_1 \in M_1$ folgt $M_1 \in M_2$

$M_1 \supseteq M_2$ M_1 ist eine Obermenge von M_2: $M_2 \subseteq M_1$

$M_1 \subset M_2$ M_1 ist eine echte Teilmenge von M_2: Es gibt Elemente $M_1 \in M_2$, die nicht in M_1 sind

$M_1 \supset M_2$ M_1 ist eine echte Obermenge von M_2: $M_2 \subset M_1$

disjunkt M_1 und M_2 sind disjunkt, wenn sie keine gemeinsamen Elemente haben.

Bemerkung: Jede nicht leere Menge A hat mindestens zwei Teilmengen: $\emptyset \subseteq A$, $A \subseteq A$

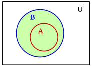


Bild: A ist in B enthalten, [Kulla, 2015]

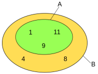


Bild: $A \subset B$, [Kulla, 2015]

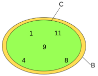


Bild: $C \subseteq B$, [Kulla, 2015]

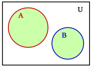


Bild: A und B sind disjunkt, [Kulla, 2015]

Verknüpfung von Mengen

Für M, M_1, M_2, Teilmengen einer nichtleeren Universalmenge U, sind folgende Verknüpfungen definiert:

Vereinigung $M_1 \cup M_2 := \{a \mid a \in M_1 \text{ oder } a \in M_2\}$
Die Menge aller Elemente, die in M_1 oder (= „und/oder“) in M_2 enthalten sind.

Schnitt $M_1 \cap M_2 := \{a \mid a \in M_1 \text{ und } a \in M_2\}$
Die Menge aller Elemente, die sowohl in M_1 als auch in M_2 enthalten sind.

Differenz $M_1 \setminus M_2 := \{a \mid a \in M_1 \text{ und } a \notin M_2\}$
Die Menge aller Elemente, die in M_1, aber nicht in M_2 enthalten sind.

Komplement $\overline{M}, M^{\mathrm{C}} := U \setminus M$
Die Menge aller Elemente (der Grundmenge), die keine Elemente von M sind.

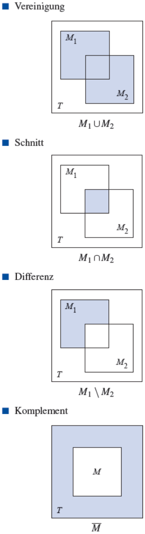


Bild: Venn-Diagramme der Mengenoperationen [Hoffmann, 2011]

Beispiele und Mengen von Mengen

- Seien $A = \{1,2,3\}$ und $B = \{3,4,5\}$ mit $A, B \subset \mathbb{N}$ gegeben.
  - Geben Sie $A \cup B$, $A \cap B$ und $A \setminus B$ an.
    Lösung: $A \cup B = \{1,2,3,4,5\}$, $A \cap B = \{3\}$ und $A \setminus B = \{1,2\}$
  - Geben Sie $\overline{A}$ und $\overline{B}$ an.
    Lösung: $\overline{A} = \{n \in \mathbb{N} \mid n > 3\}$, $\overline{B} = \{n \in \mathbb{N} \mid n < 3 \vee n > 5\}$

- Die Vereinigung aller Teilmengen von M wird Potenzmenge von M genannt.
  - $2^M, \mathcal{P}(M) := \{N \mid N \subseteq M\}$
  - Achtung: die Elemente von M sind Mengen.
  - Für alle nichtleeren Mengen M gilt $\emptyset, M \in \mathcal{P}(M)$
  - $|\mathcal{P}(M)| = 2^{|M|}$

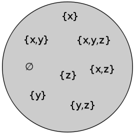


Bild: $\mathcal{P}(\{x, y, z\})$
[Kulla, 2015]

- Beispiel: $M = \{1,2,3,4\}$. Bestimmen Sie $|\mathcal{P}(M)|$ und $\mathcal{P}(M)$.
  - $|\mathcal{P}(M)| = 16 = 2^4 = 2^{|M|}$
  - $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,4\}, \{2,4\}, \{3,4\}, \{1,2,3\}, \{1,2,4\}, \{2,3,4\}, \{1,3,4\}, \{1,2,3,4\}\}$

Abschnitt 2

Relationen und Funktionen

Geordnete Paare

Wieso ist der Mengenbegriff nicht immer ausreichend?

- In Mengen spielt die Reihenfolge der Elemente keine Rolle: $\{5, 7\} = \{7, 5\}$.
- Unpraktisch, z.B. für Menge der Tore die in einem Fußballspiel geschossen wurden, Reihen / Sitzplatz im Kino, ...

Definition

Man bezeichnet (a, b) als geordnetes Paar (auch: Tupel). Zwei geordnete Paare (a, b) und (c, d) sind genau dann gleich, wenn $a = c$ und $b = d$ ist. $(a_1, a_2, \ldots, a_n)$ heißt n-Tupel.

Achtung:

- runde Klammern bezeichnen Tupel, geschweifte Klammern Mengen
- $(1, 2) \neq (2, 1)$
- $\{3, 3, 3\} = \{3, 3\} = \{3\}$
- $(3, 3, 3) \neq (3, 3) \neq (3)$

Mengenprodukte - Definition

Definition

Die Menge aller geordneten Paare wobei das erste Element immer aus der Menge A und das zweite Element immer aus der Menge B kommt, heißt kartesisches Produkt von A und B:

$$A \times B = \{(a, b) \mid a \in A \land b \in B\}$$

gelesen: „A kreuz B“. Erweiterung auf n Mengen:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1 \land \ldots \land a_n \in A_n\}.$$

Das n-fache Produkt $A \times A \times \ldots \times A$ wird auch als A^n abgekürzt.

Bemerkungen:

- Die Menge der Tupel in $A \times B$ ist $|A \times B| = |A| \cdot |B|$.
- $|A_1 \times \ldots \times A_n| = |A_1| \cdot \ldots \cdot |A_n|$

Relationen - Definition und Beispiele

Definition

Eine Relation R zwischen den Mengen A und B ist eine Teilmenge des kartesischen Produktes $A \times B$, also $R \subseteq A \times B$.
Sprechweise für $(a, b) \in R$: „a steht in Relation R zu b".
Alternative Schreibweise: aRb.
A heißt Definitionsbereich, B Wertebereich. Falls $R \subseteq A \times A$, so heißt R Relation in A oder Relation auf A.
Verknüpft $R \subseteq A \times B$ nur zwei Mengen, so heißt sie binäre Relation.
$R \subseteq A_1 \times A_2 \times \ldots \times A_n$ heißt n-stellige Relation.

Beispiele für bekannte Relationen über der Menge $A = \{2, 3, 4, 5\}$:

- $R =$„$=$": $R = \{(2, 2), (3, 3), (4, 4), (5, 5)\}$
- $S =$„$\neq$": $S = \{(2, 3), (2, 4), \ldots, (5, 4)\}$
- $T =$„$<$": $T = \{(2, 3), (2, 4), \ldots, (4, 5)\}$
- $U =$„$\geq$": $U = \{(2, 2), (3, 2), (3, 3), \ldots, (5, 5)\}$

Totale und partielle Funktionen

Definition

Seien X und Y zwei beliebige Mengen. Eine Relation $f \subseteq X \times Y$ heißt Funktion oder Abbildung, wenn jedes $x \in X$ mit höchstens einem $y = f(x) \in Y$ in Relation steht. Schreibweise: $f : X \to Y, x \mapsto f(x)$
Die Funktion f heißt

- total, wenn für jedes $x \in X$ ein Element $f(x) \in Y$ existiert.
- partiell, wenn sie für mindestens ein $x \in X$ undefiniert ist.

Beispiele:

- $g : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ ist totale Funktionn
- $h : \mathbb{R} \to \mathbb{R},\ x \mapsto \frac{1}{x}$ ist partielle Funktion (weil undefiniert bei $x = 0$)
- Jede Funktion ist eine Relation, aber nicht jede Relation ist eine Funktion.
  - Die Relation $W_1 : (x, \sqrt{x})$ ist über $\mathbb{Z}$ keine Funktion: $W_1 = \{(1, -1), (1, 1), (4, -2), (4, 2), \ldots\}$.
  - Die Relation $W_2 : (x, \left|\sqrt{x}\right|)$ ist eine Funktion über $\mathbb{Z}$: $W_2 = \{(1, 1), (4, 2), \ldots\}$.

Surjektive, injektive und bijektive Funktionen

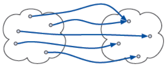
Definition

Eine totale Funktion $f : X \to Y$ heißt

- surjektiv, falls für alle $y \in Y$ ein $x \in X$ mit $f(x) = y$ existiert,
- injektiv, falls aus $f(x) = f(y)$ stets $x = y$ folgt,
- bijektiv, falls f sowohl injektiv als auch surjektiv ist

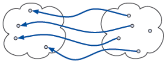
Bemerkung: Jede bijektive Funktion f ist umkehrbar. Die Umkehrfunktion ist definiert durch $f^{-1} : f(x) \mapsto x$.

- Surjektivität



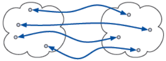
Ausnahmslos jedes Element der Zielmenge ist das Bild eines oder mehrerer Elemente der Definitionsmenge.

- Injektivität



Es liegt eine umkehrbar eindeutige Zuordnung vor. Die Bilder zweier unterschiedlicher Elemente der Definitionsmenge sind stets verschieden.

- Bijektivität



Die Eigenschaften der Surjektivität und Injektivität sind gleichermaßen erfüllt. Es besteht eine Eins-zu-eins-Zuordnung zwischen den Elementen der Definitions- und der Zielmenge.

Quelle: [Hoffmann, 2011]

Bijektive Funktionen und Mächtigkeit von Mengen

Mit Hilfe bijektiver Funktionen kann die Mächtigkeit von Mengen verglichen werden:

- Zwei Mengen M_1 und M_2 heißen gleichmächtig, $|M_1| = |M_2|$, falls eine Bijektion $f : M_1 \to M_2$ existiert.
- Eine unendliche Menge M heißt
  - abzählbar (unendlich), falls $|M| = |\mathbb{N}|$,
  - überabzählbar (unendlich), falls $|M| \neq |\mathbb{N}|$.

Bild: Welche Menge ist größer? [Hoffmann, 2011]

Beispiele:

- $\mathbb{Z}$ ist abzählbar. Eine Beispiels-Bijektion von $\mathbb{Z}$ nach $\mathbb{N}$:
$$f(x) \mapsto \begin{cases} -2x-1 & \text{für } x < 0 \\ 2x & \text{für } x \geq 0 \end{cases}$$
- $\mathbb{Q}$, die Menge der Quadratzahlen, die Menge der Primzahlen sind abzählbar unendlich.
- $\mathbb{R}$ und $\mathbb{C}$ sind überabzählbar unendlich.

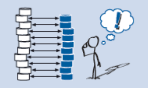


Bild: Bijektiver Vergleich bringt die Lösung. [Hoffmann, 2011]

Hilberts Hotel

David Hilbert (1892-1943) hat mit folgendem Gedankenexperiment gezeigt, was "abzählbar unendlich" bedeutet:

- Ein normales Hotel hat eine endliche Anzahl von Zimmern.
  - Sind diese Zimmer alle belegt sind, ist es voll.
  - Ein neu ankommender Gast wird abgewiesen.
- Hilberts Hotel hat jedoch unendlich viele Zimmer.
  - Auch dieses Hotel kann voll belegt sein.
  - Kommt ein neuer Gast an, wird dieser **nicht** abgewiesen.
  - Es müssen lediglich alle Gäste aus ihrem bisherigen Zimmer Nr. m in das Zimmer Nr. $m + 1$ umziehen.
  - Der neue Gast kann nun in Zimmer Nr. 1 untergebracht werden.
- Leider bleibt dies aber ein Gedankenexperiment, alle echten Hotels, Datenspeicher, ... sind endlich.

Bild: Hilberts Hotel [Hoffmann, 2011]

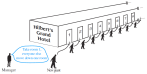


Bild: Ein neuer Gast für Hilberts Hotel [Rosen, 2012]

Abschnitt 3

Rekursion und Induktion

Rekursion - Definition

Definition

Wenn Regeln, Funktionen, oder Definitionen auf das Produkt das sie erzeugen wieder angewandt werden, bezeichnet man dies als Rekursion.
Unter einer rekursiven Definition versteht man ein Problem, eine Funktion, ein Verfahren, das durch sich selbst beschrieben wird.

Programmierung einer rekursiven Funktion: Ausprogrammierung der Basisfälle (Rekursionsanfang), Bestimmung aller anderen durch Selbstaufrufe.
Rekursive Definition: Präzise Beschreibung der einfachen Fälle (Rekursionsanfang), Bestimmung aller anderen durch wiederholte Anwendung der Basisdefinition.

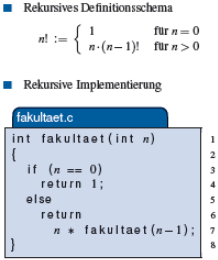


Bild: Rekursive Definition und Programmierung [Hoffmann, 2011]

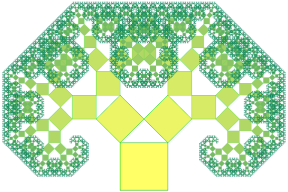
Rekursion - Vorteile, Nachteile und noch ein Beispiel

Vorteile und Nachteile

- kompakte, übersichtliche Schreibweise
- effizientere Programmierung (kleinerer Speicherverbrauch)
- erlaubt die regelmäßige Struktur zu erkennen
- Achtung: es können unendlich viele Schleifen entstehen

Beispiel: Baum des Pythagoras (eine einfache Variante)

1. Errichte über zwei gegebenen Punkten ein Quadrat.
2. Auf der Oberseite zeichne ein gleichschenkliges rechtwinkliges Dreieck.
3. Rufe diese Funktion für die beiden Schenkel dieses Dreieckes auf.



Quelle: Wikipedia

Vollständige Induktion

- Eng verwandt mit der Rekursion - nutzt die rekursive Natur von $\mathbb{N}$.
- Anwendung: Beweise für Aussagen die für Zahlen $n \in \mathbb{N}$ gelten.

Satz (Vollständige Induktion)

Seien $n_0 \in \mathbb{N}$ und $A(n)$ eine Aussage für Zahlen $n \in \mathbb{N}$. $A(n)$ ist wahr für alle $n \geq n_0$ wenn die folgenden Aussagen gelten:

1. *$A(n_0)$ ist wahr. (Induktionsbeginn)*
2. *Für alle $k \geq n_0$ gilt: Aus der Gültigkeit von $A(k)$ (Induktionsannahme) folgt die Gültigkeit von $A(k+1)$ (Induktionsschluss).*

Bemerkungen:

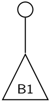
- Meistens ist $k = 1$.
- Klassisches Beispiel für einen Induktionsbeweis: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

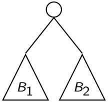
Strukturelle Induktion I

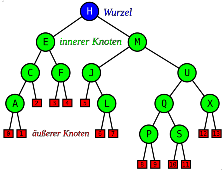
- Ähnlich zur totalen Induktion, nur für Objekte, nicht für Zahlen.
- Klassisches Werkzeug der theoretischen Informatik.
- Anwendungen: Beweis von Aussagen für rekursiv aufgebaute Strukturen (z.B. Formeln, Datenstrukturen).

Beispiel: Binärbaum

- effiziente Datenstruktur zum Suchen, Löschen und Einfügen
- Rekursive Definition eines Binärbaums über der Blättermenge B
  - Jedes Blatt $b \in B$ ist ein Binärbaum
  - Sind B_1 und B_2 Binärbäume, dann sind es

auch 

und 



Quelle: Wikipedia

Strukturelle Induktion II

Satz

Seien $k \in \mathbb{N}$ und ein Binärbaum B mit mehr als 2^k Knoten, d.h. $|B| \geq 2^k$. Dann existiert mindestens ein Pfad mit Länge $\geq k$.

Beweis: Über strukturelle Induktion, siehe Bild, sowie [Hoffmann, 2011].

Was ist wichtig für Sie als Informatiker?

- Nicht die Beweise in all ihren Details.
- Generelle Vorstellungen über Eigenschaften rekursiv aufgebauter Zahlenmengen und Strukturen aber schon.
- Letzteres hilft nämlich auch bei effizienter, schöner Programmierung.

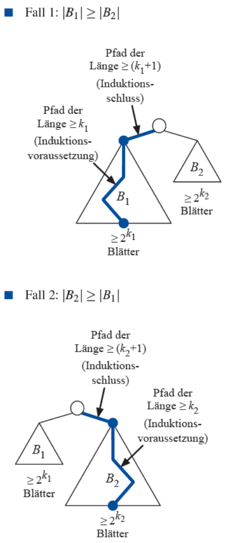


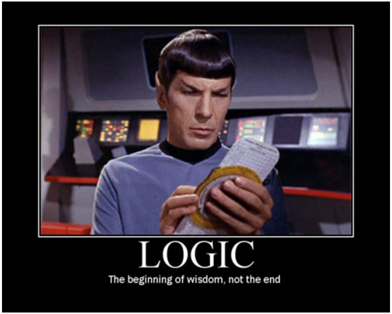
Bild: Aufbau Induktionsbeweis [Hoffmann, 2011]

Abschnitt 4

Logik

Bedeutung der Logik für Informatiker

1. Wahr / Falsch = „Denkweise" aller elektronischen Geräte (Strom an / Strom aus, 1 / 0)
2. Exakte, widerspruchsfreie Beschreibung für Aussagen, Daten, Schaltkreise und ihre Funktionen
3. Semantische Definition von Programmiersprachen, Verifikation von Programmen
4. Algorithmisches Schließen in Datenbanken und Expertensystemen
5. ...



Quelle: http://www.tarnowski.se

Aussagen

Definition

Eine elementare oder atomare Aussage hat genau einen der beiden Wahrheitswerte

- 1 alternativ: wahr, „w“, „T“, ✓
- 0 alternativ: falsch, „f“, „F“, ↯

$a \in \{0, 1\}$ heißt Wahrheitsvariable. Wahrheitsvariablen sind elementare Aussagen.

Beispiele für Aussagen?

• „Die Erde ist ein Planet.“	Wahre Aussage ✓.
• „Pluto ist ein Planet.“	Bis 2006 wahre Aussage, seitdem falsch ↯.
• „Die Erde ist eine Scheibe.“	Falsche Aussage ↯.
• „Die Sonne soll scheinen.“	Keine Aussage.
• „Wie spät ist es?“	Keine Aussage.
• $x > 5$	Keine Aussage (hängt von x ab).

Verknüpfung elementarer Aussagen

Elementare Aussage können mit Hilfe sogenannter Konnektoren zu komplexeren Aussagen verknüpft werden:

Beispiele:

- „Die Erde ist ein Planet und dreht sich um die Sonne" ✓
- „Pluto ist ein Planet oder dreht sich um die Sonne." ✓
- „Die Erde ist keine Scheibe und dreht sich um den Mond." $\lightning$

Umgangssprache	**Symbol(e)**	**Name in der Logik**
nicht	$\neg$ ($\bar{\ }$)	Negation
und	$\wedge$	Konjunktion
oder	$\vee$	Disjunktion, Alternative
wenn ... dann	$\Rightarrow$	Implikation
genau dann wenn	$\Leftrightarrow$	Äquivalenz
entweder ... oder	$\not\Leftrightarrow$ ($\oplus$)	Antivalenz, Kontravalenz, XOR

Tabelle: Konnektoren zur Verknüpfung von Aussagen

Syntax der Aussagenlogik

Eine korrekt formulierte logische Aussage ist induktiv definiert als

atomare Aussage

- 0 und 1 sind Aussagen
- Jede Variable $a \in \{0, 1\}$ ist eine Aussage

XOR

komplexe Aussage

- Ist F eine Aussage, so ist es auch $\neg F$
- Sind F und G Aussagen, so sind es auch $(F \wedge G)$, $(F \vee G)$, $(F \Rightarrow G)$, $(F \Leftrightarrow G)$, $(F \oplus G)$

Semantik der Aussagenlogik: Wahrheitstabellen

a	$\neg a$
0	1
1	0

Tabelle: Wahrheitstabelle der Negation

Interpretation:

- 1. Zeile: Falls a falsch ist, dann ist $\neg a$ wahr
- 2. Zeile: Falls a wahr ist, dann ist $\neg a$ falsch

a	b	$a \wedge b$	$a \vee b$	$a \Rightarrow b$	$a \Leftrightarrow b$	$a \oplus b$
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

Tabelle: Wahrheitstabelle für Konjunktion, Disjunktion, Implikation, Äquivalenz, Antivalenz

Interpretation der 1. Spalte:

- 1. Zeile: Falls a falsch und b falsch ist, dann ist $a \wedge b$ falsch
- 2. Zeile: Falls a falsch und b wahr ist, dann ist $a \wedge b$ falsch
- 3. Zeile: Falls a wahr und b falsch ist, dann ist $a \wedge b$ falsch
- 4. Zeile: Falls a wahr und b wahr ist, dann ist $a \wedge b$ wahr

Beispiele zum Mitdenken

Seien $f = 1$ und $g = 0$. Stellen Sie jede komplexe Aussage als Formel dar und bestimmen Sie deren Wahrheitswert!

- A: „nicht f"
  Lösung: $A = \neg f = \neg 1 = 0 =$ falsch.
- B: „f und g"
  Lösung: $B = f \wedge g = 1 \wedge 0 = 0 =$ falsch.
- C: „f oder g"
  Lösung: $C = f \vee g = 1 \vee 0 = 1 =$ wahr.
- D_1: „wenn f dann g"
  Lösung: $D_1 = f \Rightarrow g = 1 \Rightarrow 0 = 0 =$ falsch.
- D_2: „wenn g dann f"
  Lösung: $D_2 = g \Rightarrow f = 0 \Rightarrow 1 = 1 =$ wahr.
- E: „f genau dann wenn g"
  Lösung: $E = f \Leftrightarrow g = 1 \Leftrightarrow 0 = 0 =$ falsch.
- F: „entweder f oder g"
  Lösung: $F = f \oplus g = 1 \oplus 0 = 1 =$ wahr.

Semantik der Aussagenlogik: Regeln für Konnektoren

Bindungsregeln

- $\neg$ bindet stärker als $\wedge$:
  $\neg A \wedge B = (\neg A) \wedge B$
- $\wedge$ bindet stärker als $\vee$:
  $A \wedge B \vee C = (A \wedge B) \vee C$
- $\Rightarrow, \Leftrightarrow, \oplus$ binden am schwächsten und sind gleich schwach.

Kettenregeln

- Wird $\neg$ mit einer Variable mehrmals verknüpft, erfolgt die Auswertung „von rechts nach links".
- Alle anderen Operatoren die gleich, oder gleich stark sind, werden „von links nach rechts" ausgewertet.

■ Bindungsregeln

Ausdruck	Bedeutung
$\neg F \wedge G$	$((\neg F) \wedge G)$
$F \vee G \wedge H$	$(F \vee (G \wedge H))$
$F \vee G \rightarrow H$	$((F \vee G) \rightarrow H)$
$F \rightarrow G \not\leftrightarrow H$	$((F \rightarrow G) \not\leftrightarrow H)$
$F \not\leftrightarrow G \rightarrow H$	$((F \not\leftrightarrow G) \rightarrow H)$

■ Kettenregeln

Ausdruck	Bedeutung
$\neg\neg\neg F$	$\neg(\neg(\neg F))$
$F \wedge G \wedge H$	$(F \wedge G) \wedge H$
$F \vee G \vee H$	$(F \vee G) \vee H$
$F \rightarrow G \rightarrow H$	$(F \rightarrow G) \rightarrow H$
$F \leftrightarrow G \leftrightarrow H$	$(F \leftrightarrow G) \leftrightarrow H$
$F \not\leftrightarrow G \not\leftrightarrow H$	$(F \not\leftrightarrow G) \not\leftrightarrow H$

Quelle: [Hoffmann, 2011]

Beispiele zum Mitdenken

Seien die atomaren Aussagen $x = 1$, $y = 0$, $z = 1$ gegeben.

Beispiel: Bestimmung des Wahrheitswertes der Aussage $x \vee y \vee z$.
$x \vee y \vee z = (x \vee y) \vee z = (1 \vee 0) \vee 1 = 1 \vee 1 = 1.$

Bestimmen Sie den Wahrheitswert der Aussagen

Aussage	**Wahrheitswert**	**Nebenrechnung**
$x \wedge y \wedge z$	0	$= (x \wedge y) \wedge z = (1 \wedge 0) \wedge 1 = 0 \wedge 1 = 0$
$x \wedge (y \wedge z)$	0	$= 1 \wedge (0 \wedge 1) = 1 \wedge 0 = 0$
$\neg(x \Rightarrow z)$	0	$= \neg(0 \Rightarrow 1) = \neg 1 = 0$
$\neg x \Rightarrow z$	1	$= (\neg 1) \Rightarrow 1 = 0 \Rightarrow 1 = 1$
$(x \oplus z) \wedge y$	0	$= (1 \oplus 1 \wedge 0 = 0 \wedge 0 = 0$
$x \oplus z \wedge y$	1	$= 1 \oplus (1 \wedge 0) = 1 \oplus 0 = 1$

Aussageformen

Beispiel:

- x hat einen eigenen YouTube-Kanal.
  $\Rightarrow$ hat keinen Wahrheitswert, da nichts über x bekannt.
- Wahre Aussage für $x =$ Rezo, Pamela Reif, Rammstein, Bundesregierung, HTWG, Insel Mainau ...
- Falsche Aussage für $x =$ 151, Insel Reichenau, Alan Turing, Marge Simpson, ...,

Definition

Ersetzt man in einer Aussage A irgendeine Konstante durch eine Variable x, so entsteht eine Aussageform $A(x)$. Die durch $A(x)$ über x getroffene Aussage wird Prädikat genannt. Setzt man für die Variable x einen festen Wert $x = x_0$ ein, so wird die Aussageform wieder zur Aussage.

Bemerkung: Aussageformen enthalten Variablen und Prädikate. Daher sind Sie Teil der sogenannten Prädikatenlogik, welche eine Erweiterung der Aussagenlogik ist, die sich nur mit Aussagen beschäftigt.

Beispiele, Syntax und Semantik

Aussageform	**Variable**	**Prädikat**	**wahr z.B. für**	**falsch z.B. für**
$A(x)$: x hat YouTube-Kanal	x	hat YouTube-Kanal	$x =$ Rezo	$x = 151$
$C(x) : x \leq 100$	x	≤ 100	$x = \pi$	$x = 101$
$P(n)$: n is prim	n	ist prim	$n = 23$	$n = 42$
$F(n) : P(n) \wedge C(n)$	n	$\leq 100 \wedge$ ist prim	$n = 23$	$n = 101$
$G(x, y) : x + y > 1$	x, y	$x + y > 1$	$x = 0, y = 53$	$x = -23, y = 10$

Bemerkungen:

Syntax Aussageformen können wie Aussagen mit Hilfe der Konnektoren $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \oplus$ zu neuen Aussageformen verknüpft werden.

Semantik Der Wahrheitswert zusammengesetzter Aussageformen wird mit Hilfe der Bedeutung der Konnektoren, sowie der Werten der Variablen bestimmt.

Quantoren - Einführung

Frage: Wie kann man eine Aussageformen (abhängig von Variablen) in eine Aussage (mit eindeutigem Wahrheitswert) umwandeln?

Zwei Möglichkeiten:

1. Für die Variablen feste Werte einsetzen.
2. Aussageform „für alle“ oder „für ein“ gelten lassen (Quantoren).

Beispiele

- $P(n)$: n ist gerade — Wahrheitswert abhängig von n
- $P(17)$: 17 ist gerade — Falsche Aussage $\lightning$
- $P(24)$: 24 ist gerade — Wahre Aussage $\checkmark$
- Für alle $n \in \mathbb{N}$ gilt: n ist gerade — Falsche Aussage $\lightning$
- Für ein $n \in \mathbb{N}$ gilt: n ist gerade — Wahre Aussage $\checkmark$

Quantoren - Definition

Definition

Sei M eine beliebige Menge, $x \in M$ und eine Aussageform $A(x)$.

- Die Aussage „Für alle $x \in M$ gilt $A(x)$“ ist wahr genau dann, wenn $A(x)$ für alle möglichen x aus M wahr ist:

  $$\forall x \in M : A(x) \quad \text{oder} \quad \forall_{x \in M}\, A(x)$$

  $\forall$ heißt All-Quantor und wird als „für alle“ (oder „für jedes“) gelesen.
- Die Aussage „Es gibt ein $x \in M$, so dass $A(x)$“ ist wahr genau dann, wenn $A(x)$ für mindestens ein mögliches x aus M wahr ist:

  $$\exists x \in M : A(x) \quad \text{oder} \quad \exists_{x \in M}\, A(x)$$

  $\exists$ heißt Existenz-Quantor und wird als „es gibt (mindestens) ein“ (oder auch: „es existiert (mindestens) ein“ oder „für (mindestens) ein“) gelesen.

Bemerkung: Manchmal nennt man die Menge M auch Domäne für x.

Beispiele zum Mitdenken

Wahr oder falsch?

- Für alle natürlichen Zahlen n gilt: $n < n + 1$ — wahr ✓
- $\forall_{n \in \mathbb{N}}\ n < 3$ — falsch ↯
- $\exists_{n \in \mathbb{N}}\ n^2 = 4$ — wahr ✓
- Es existiert eine natürliche Zahl n mit: $n < 0$ — falsch ↯
- Es existiert eine ganze Zahl n mit: $n < 0$ — falsch ✓

Allgemein gilt: Um zu beweisen dass (für eine Menge M)

- $\forall_{x \in M}\ a(x)$ wahr ist, muss man dies für jedes einzelne $x \in M$ überprüfen.
- $\forall_{x \in M}\ a(x)$ falsch ist, muss man mindestens ein $x \in M$ finden für das $a(x)$ falsch ist. Solch ein x wird auch Gegenbeispiel genannt.
- $\exists_{x \in M}\ a(x)$ wahr ist, muss man mindestens ein $x \in M$ finden für das $a(x)$ wahr ist.
- $\exists_{x \in M}\ a(x)$ falsch ist, muss man dies für jedes einzelne $x \in M$ überprüfen.

Verneinung von All- und Existenzaussagen

Beispiele aus der Alltagssprache:

- „Alle Menschen mögen Mathematik". Verneinung: „Kein Mensch mag Mathematik" ist falsch. Richtig: „Es gibt mindestens einen Menschen, der Mathematik nicht mag."
- „In Konstanz ist das Wetter an mindestens einem Tag im Jahr schlecht". Verneinung: „In Konstanz ist das Wetter an keinem Tag im Jahr schlecht."

Negation von Quantoren

Durch die Verneinung einer All-Aussage entsteht eine Existenz-Aussage, und umgekehrt entsteht durch die Verneinung einer Existenz-Aussage eine All-Aussage:

$\neg$ (Für alle $x \in M$ gilt $A(x)$) $=$ Es existiert ein $x \in M$, so dass $\neg A(x)$

$\neg$ (Es existiert ein $x \in M$ mit $A(x)$) $=$ Für alle $x \in M$ gilt $\neg A(x)$.

$$\neg(\forall_{x \in M}\ A(x)) \quad \equiv \quad \exists_{x \in M}\ \neg A(x)$$
$$\neg(\exists_{x \in M}\ A(x)) \quad \equiv \quad \forall_{x \in M}\ \neg A(x)$$

Beispiele zum Mitdenken

- Was ist die Verneinung von
  - $\forall_{x \in M} \, (x^2 > x)$?
    Lösung: $\exists_{x \in M} \, \neg(x^2 > x) \equiv \exists_{x \in M} \, x^2 \leq x$
  - $\exists_{x \in M} \, (x^2 = x)$?
    Lösung: $\forall_{x \in M} \, \neg(x^2 = x) \equiv \forall_{x \in M} \, x^2 \neq x$

- Negieren Sie folgende Aussage!

  „Jede Mail die größer als ein Megabyte ist, wird komprimiert.“
  Lösung:
  - Benutze $S(m, y)$: „Mail m ist größer als y Megabyte”, mit $y \in \mathbb{R}^+$ und $C(m)$: „Mail m wird komprimiert.“
  - Schreibe: $\forall_{\text{Mails } m} \, S(m, 1) \Rightarrow C(m)$
  - Negiere:
    $\neg(\forall_m \, S(m, 1) \Rightarrow C(m)) \equiv \exists_m \, \neg(S(m, 1) \Rightarrow C(m)) \overset{a \Rightarrow b \equiv \neg a \vee b}{\equiv}$
    $\exists_m \, \neg(\neg S(m, 1) \vee C(m)) \overset{\text{De Morgan}}{\equiv} \exists_m \, S(m, 1) \wedge \neg C(m)$
  - In Umgangssprache: “Es gibt mindestens eine Mail, die größer als ein 1 MB ist, aber nicht komprimiert wird.”

Verwendete oder empfohlene Literatur I

[Hedtstück, 2012] Hedtstück, U. (2012).
Einführung in die theoretische Informatik: formale Sprachen und Automatentheorie.
Oldenbourg Verlag.
Als eBook in der HTWG-Bibliothek verfügbar.

[Hoffmann, 2011] Hoffmann, D. W. (2011).
Theoretische Informatik.
Carl Hanser Verlag GmbH & Co. KG, 2. Auflage.
Als eBook in der HTWG-Bibliothek verfügbar.

[Hoffmann, 2015] Hoffmann, D. W. (2015).
Theoretische Informatik.
Carl Hanser Verlag GmbH & Co. KG, 3. Auflage.
Als eBook in der HTWG-Bibliothek verfügbar.

Verwendete oder empfohlene Literatur II

[Hopcroft et al., 2011] Hopcroft, J. E., Motwani, R., and Ullman, J. D. (2011).
Einführung in die Automatentheorie, formale Sprachen und Berechenbarkeit (bzw. Komplexitätstheorie); engl.: Introduction to automata theory, languages and computation.
Pearson, 3. Auflage.
Als eBook in der HTWG-Bibliothek verfügbar.

[Kulla, 2015] Kulla, S. (2015).
Mathe für Nicht-Freaks - Grundlagen der Mathematik.
Wikibooks.

[Rosen, 2012] Rosen, K. H. (2012).
Discrete Mathematics and its Applications.
McGraw-Hill, 7th edition.

Verwendete oder empfohlene Literatur III

[Teschl and Teschl, 2013] Teschl, G. and Teschl, S. (2013).
Mathematik für Informatiker: Band 1: Diskrete Mathematik und Lineare Algebra.
Springer Vieweg, 4. Auflage.
Als eBook in der HTWG-Bibliothek verfügbar.