

Diskrete Mathematik

Simon Krenger

October 21, 2011

Chapter 1

Logik (Boolesche Algebra)

Nach George Bool, 1815 bis 1864, Cork (Irland)

1.1 Aussagen

Wir betrachten Aussagen (Sätze), die entweder wahr (1) oder falsch (0) sind.

Heute ist Freitag \rightarrow wahr

Morgen schneit es in Bern \rightarrow falsch

Schauen Sie einmal! \rightarrow keine Aussage

Aussagen bezeichnen wir mit a, b, c, d, \dots

Definition 1. Ist a eine Aussage, somit heisst $\neg a$ die Negation von a

Beispiel 1. a : *Xaver isst gerne Kuchen* $\neg a$: *Xaver isst nicht gerne Kuchen*

1.2 Konjunktion

Wir verbinden zwei Aussagen a, b mit Hilfe von “und” zu einer einzigen Aussage

$$a \wedge b \tag{1.1}$$

Beispiel 2. *Morgen ist Sonntag und ich werde ausschlafen*

Die Wahrheitstabelle von $a \wedge b$ sind abhängig von denjenigen von a als auch von b . Dies stellen wir in einer Wahrheitstabelle dar. Wir finden sofort die Regeln

$$a \wedge \neg a = \text{falsch} \tag{1.2}$$

Definition 2. Eine Aussage, die immer falsch ist, heisst Kontradiktion.

$$a \wedge 1 = a \quad (1.3)$$

$$a \wedge 0 = 0 \quad (1.4)$$

Weiter finden wir Gesetze

Kommutativgesetz (Vertauschungsgesetz)

$$a \wedge b = b \wedge a \quad (1.5)$$

Beweis 1. Wir beweisen mit einer Wahrheitstabelle

a	b	$a \wedge b$	$b \wedge a$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Assoziativgesetz (Verbindungsgesetz)

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c \quad (1.6)$$

Beweis 2. Wir beweisen mit einer Wahrheitstabelle

a	b	c	$a \wedge (b \wedge c)$	$(a \wedge b) \wedge c$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	0	0
1	1	0	0	0
1	1	1	1	1

Idempotenzgesetz

$$a \wedge a = a \quad (1.7)$$

1.3 Disjunktion

Zwei Aussagen a , b werden mit der Disjunktion "oder" zu einer neuen Aussage verbunden. Dafür schreiben wir:

$$a \vee b \quad (1.8)$$

und definieren

a	b	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

Nicht verwechseln mit "entweder oder" (XOR)! Wir finden die Regeln

$$a \vee 1 = 1 \quad (1.9)$$

$$a \vee 0 = a \quad (1.10)$$

$$a \vee \neg a = 1 \quad (1.11)$$

Definition 3. Eine Aussage, die stets wahr ist, heisst Tautologie.

Es gelten die Gesetze

Kommutativgesetz

$$a \vee b = b \vee a \quad (1.12)$$

Assoziativgesetz

$$a \vee (b \vee c) = (a \vee b) \vee c \quad (1.13)$$

Idempotenzgesetz

$$a \vee a = a \quad (1.14)$$

In der Algebra in \mathbb{R} gilt

$$a(b + c) = ab + ac \quad (1.15)$$

was in der Logik zu

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad (1.16)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad (1.17)$$

dem Distributivgesetz (Verteilungsgesetz) führt. Der folgende Beweis zeigt, dass die Gleichung 1.16 gilt.

Beweis 3. Wir beweisen mit einer Wahrheitswerttabelle

a	b	c	$b \vee c$	$a \wedge (b \vee c)$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Das zweite Distributivgesetz kann analog dazu bewiesen werden.

In der Logik gibt es zu jedem Gesetz ein duales Gesetz. Dies entsteht durch wechseln von \vee zu \wedge und umgekehrt. Weiter finden wir

Absorbtionsgesetz

$$a \wedge (a \vee b) = a \quad (1.18)$$

$$a \vee (a \wedge b) = a \quad (1.19)$$

Beweis 4. Wir beweisen mit einer Wahrheitswerttabelle

a	b	$a \vee b$	$a \wedge (a \vee b)$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	1	1

Gesetz von de Morgan

$$\neg(a \wedge b) = \neg a \vee \neg b \quad (1.20)$$

$$\neg(a \vee b) = \neg a \wedge \neg b \quad (1.21)$$

Wir verwenden die Gesetze, um die Aussagen zu vereinfachen.

Beispiel 3. Folgende Beispiele zeigen, wie sich Aussagen mittels den oben genannten Gesetzen vereinfachen lassen.

1. $[a \wedge (b \vee a)] \vee \neg a$
 $= a \vee \neg a$
 $= 1$
2. $[\neg(a \wedge b) \vee \neg b] \wedge a$
 $= (\neg a \vee \neg b \vee \neg b) \wedge a$
 $= (\neg a \vee \neg b) \wedge a$
 $= (\neg a \wedge a) \vee (\neg b \wedge a)$
 $= 0 \vee (\neg b \wedge a)$
 $= \neg b \wedge a$
3. $(a \wedge b) \vee \neg b$
 $= (a \vee \neg b) \wedge (b \vee \neg b)$
 $= (a \vee \neg b) \wedge 1$
 $= (a \vee \neg b)$
4. $b \wedge [(a \wedge b) \vee (\neg a \wedge b)]$
 $= b \wedge [b \wedge (a \vee \neg a)]$
 $= b \wedge (b \wedge 1)$
 $= b \wedge b = b$

1.4 Implikation

Mathematische Lehrsätze haben die Form "Wenn ein Dreieck rechtwinklig ist mit Hypotenuse c und Katheten a, b , dann ist $c^2 = a^2 + b^2$ ". Sie bestehen also aus Voraussetzung(en):

Das Dreieck ist rechtwinklig

und Behauptung

$$\text{Es ist } a^2 + b^2 = c^2$$

und einem Beweis

Beweis. Gemäss "Indischer Beweis":

$$\begin{aligned} c^2 &= 4 \frac{ab}{2} + (a-b)^2 \\ c^2 &= 2ab + a^2 - 2ab + b^2 \\ c^2 &= a^2 + b^2 \end{aligned} \tag{1.22}$$

□

Im obigen Beispiel haben wir einen direkten Beweis geführt. Von der Voraussetzung durch Rechnung zur Behauptung.

Wenn wir zwei Aussagen a, b mit "wenn a, dann b" oder "wenn a so b" oder "aus a folgt b (a impliziert b)" verknüpfen, so schreiben wir dafür

$$a \rightarrow b \tag{1.23}$$

und definieren

a	b	$a \rightarrow b$
0	0	1
0	1	1
1	0	0
1	1	1

Wir finden sofort, das "aus a folgt b"

$$a \rightarrow b = \neg a \vee b \tag{1.24}$$

Beispiel 4. Vereinfache

1. $(a \rightarrow b) \rightarrow b$
 $= (\neg a \vee b) \rightarrow b = \neg(\neg a \vee b) \vee b$
 $= (a \wedge \neg b) \vee b = (a \vee b) \wedge (\neg b \vee b)$
 $= (a \vee b) \wedge 1 = (a \vee b)$
2. $b \rightarrow (a \rightarrow b)$
 $= b \rightarrow (\neg a \vee b) = \neg b \vee (\neg a \vee b)$
 $= \neg b \vee b \vee \neg a = 1 \vee \neg a = 1$
3. $[(a \vee c) \wedge (c \rightarrow a)] \vee (a \wedge \neg b) \vee (a \wedge c) \vee [\neg a \wedge (b \rightarrow c)]$
 $= [(a \vee c) \wedge (\neg c \vee a)] \vee (a \wedge \neg b) \vee (a \wedge c) \vee [\neg a \wedge (\neg b \vee c)]$
 $= [(a \vee c) \wedge (\neg c \vee a)] \vee [a \wedge (\neg b \vee c)] \vee [\neg a \wedge (\neg b \vee c)]$
 $= [a \vee (c \wedge \neg c)] \vee [(\neg b \vee c) \wedge (a \vee \neg a)]$
 $= [a \vee 0] \vee [(\neg b \vee c) \wedge 1]$
 $= a \vee (\neg b \vee c) = a \vee \neg b \vee c$
 $(= a \vee (b \rightarrow c))$

Ein mathematischer Satz besteht aus Voraussetzung a , Behauptung b und Beweis. Der Satz wird als $a \rightarrow b$ formuliert.

Der direkte Beweis ist eine Folge von Implikationen

$$a \rightarrow x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow \dots \rightarrow b \quad (1.25)$$

Beispiel 5. Vereinfache

1. *Voraussetzung:* Ein Dreieck ABC mit Innenwinkel α, β, γ

Behauptung: Die Innenwinkelsumme ist 180° , d.h.

$$\alpha + \beta + \gamma = 180^\circ \quad (1.26)$$

Beweis. Wir beweisen mit einer Zeichnung:



Wähle $p \parallel c$ durch C. Dann ist $\epsilon + \delta + \gamma = 180^\circ$. Es ist $\alpha_1 = \alpha_2$: Stufenwinkel an Parallelen und $\alpha_1 = \alpha_3$: Wechselwinkel an Parallelen, eine weitere Voraussetzung.

Also ist $\alpha = \epsilon$ und $\beta = \delta$ und somit

$$\alpha + \beta + \gamma = 180^\circ \quad (1.27)$$

□

2. *Voraussetzung:* Es ist mit $n \in \mathbb{N}, a \in \mathbb{R}$

$$a^n := a \cdot a \cdot \dots \cdot a \text{ (} n \text{ Faktoren)}$$

die Potenz definiert. *Behauptung:*

$$a^m \cdot a^n = a^{m+n} \quad (1.28)$$

Beweis. Wir zeigen auf, dass m Faktoren mit n Faktoren multipliziert werden. Durch die grundlegenden Rechengesetze können wir die Klammern wegfallen lassen

$$\begin{aligned} & a^m \cdot a^n \\ &= (a \cdot a \cdot a \cdot \dots \cdot a)(a \cdot a \cdot \dots \cdot a) \\ &= a \cdot a \cdot a \cdot a \cdot \dots \cdot a \text{ (m+n Faktoren)} \end{aligned}$$

$$= a^{m+n} = a^m \cdot a^n \quad (1.29)$$

□

3. Voraussetzung: $x, y \in \mathbb{R}$

Behauptung:

$$x^y = y^x \rightarrow x = y \quad (1.30)$$

Die Behauptung ist falsch. Wollen wir zeigen, dass ein Satz falsch ist, so genügt ein einziges Beispiel, dass wir Gegenbeispiel nennen, um die Behauptung zu widerlegen.

Gegenbeispiel: Für 3 ist das Gegenbeispiel $x = 2, y = 4$, denn $2^4 = 4^2 = 16$, aber $x \neq y$.

1.4.1 Umkehrung, Kontraposition

Definition 4. Hat eine Aussage die Form

$$a \rightarrow b \quad (1.31)$$

so heisst

$$b \rightarrow a \quad (1.32)$$

die Umkehrung.

Ist eine Aussage, ein Satz wahr, so muss die Umkehrung nicht wahr sein, wie zum Beispiel:

”Wenn ich Geburtstag habe, so esse ich einen Kuchen”

”Wenn ein Mensch glücklich ist, so trinkt er Sinalco”

Wir finden aber, dass

$$\begin{aligned} \neg b \rightarrow \neg a &= \neg(\neg b) \vee \neg a \\ &= b \vee \neg a = \neg a \vee b = a \rightarrow b \end{aligned} \quad (1.33)$$

Definition 5. Wir nennen

$$\neg b \rightarrow \neg a \quad (1.34)$$

die Kontraposition von

$$a \rightarrow b \quad (1.35)$$

Wir haben gezeigt, dass $\neg b \rightarrow \neg a = a \rightarrow b$ ist, was bedeutet, dass bei einem wahren Satz auch dessen Kontraposition wahr ist.

Satz: ”Wenn es heute Freitag ist, so gehe ich ein Bier trinken.”

Kontraposition: ”Wenn ich nicht ein Bier trinken gehe, so ist heute Freitag”

Manchmal ist der direkte Beweis eines Satzes zu schwierig oder nicht möglich, dann beweisen wir die Kontraposition.

Satz: Ist $n \in \mathbb{N}$ und n^2 eine gerade Zahl, so ist n auch eine gerade Zahl.

Beweis 5. *Der direkte Beweis*

$$\begin{aligned} n^2 &= 2p \wedge p \in \mathbb{N} \\ \rightarrow n &= \sqrt{2} \cdot \sqrt{p} \end{aligned} \quad (1.36)$$

gelingt nicht. Grund dafür ist, dass eine irrationale Zahl ($\sqrt{2}$) per Definition ein nichtperiodischer, nichtendlicher Dezimalbruch ist.

Also beweisen wir die Kontraposition:

Kontraposition: "Ist $n \in \mathbb{N}$ und n ungerade, so ist auch n^2 ungerade"

Beweis 6.

$$\begin{aligned} n &= 2p + 1 \quad \wedge p \in \mathbb{N}_0 \\ \rightarrow n^2 &= (2p + 1)^2 \\ n^2 &= 4p^2 + 4p + 1 \\ n^2 &= 2(2p^2 + 2p) + 1 \end{aligned} \quad (1.37)$$

Also ist n^2 eine ungerade Zahl. □

1.5 Aequivalenz

Wenn zwei Aussagen gleichwertig (aequivalent) sind, wenn also

$$(a \rightarrow b) \wedge (b \rightarrow a) \quad (1.38)$$

so schreiben wir dafür

$$a \iff b \quad (1.39)$$

und finden die Wahrheitswerte

a	b	$a \iff b$
0	0	1
0	1	0
1	0	0
1	1	1

Wir finden die Umformung

$$\begin{aligned} a \iff b &= (a \rightarrow b) \wedge (b \rightarrow a) \\ &= (\neg a \vee b) \wedge (\neg b \vee a) \\ &= (\neg a \wedge b) \vee (\neg a \wedge a) \vee (b \wedge \neg b) \vee (a \wedge b) \\ &= (a \wedge b) \vee (\neg a \wedge \neg b) \end{aligned} \quad (1.40)$$

Ausserdem ist

$$a \iff b = \neg(a \vee b) \quad (1.41)$$

also

$$\begin{aligned} a \vee b &= [(a \wedge b) \vee (\neg a \wedge \neg b)] \\ &= \neg(a \wedge b) \wedge \neg(\neg a \wedge \neg b) \\ &= (\neg a \vee \neg b) \wedge (a \vee b) \end{aligned} \quad (1.42)$$

Beispiel 6. Vereinfache

1. $(\neg a \vee \neg b) \wedge (a \vee b)$
 $= a \vee b$ nach oberiger Herleitung
2. $(a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge c)$
 $= a \wedge [(\neg b \wedge \neg c) \vee (b \wedge c)]$
 $= a \wedge (b \iff c)$

Wenn wir in der Mathematik einen Satz finden, dessen Umkehrung auch wahr ist, so wählen wir die Formulierung mit

”dann und nur dann” oder ”genau dann”

im Englischen

”if and only if” oder ”iff”

Beispiel 7. Folgende Beispiele zeigen solche Sätze

1. Zwei Dreiecke ABC und $A_1B_1C_1$ sind genau dann ähnlich, wenn zwei Winkel gleich sind. *TODO*
2. Sind a, b reelle Zahlen, so ist das Produkt dann und nur dann 0, wenn a oder b Null ist.

Voraussetzung: $a, b \in \mathbb{R}$

Satz: $(a \cdot b = 0) \iff (a = 0 \vee b = 0)$

Anwendung:

$$\begin{aligned} a^2 - 7x + 12 &= 0 \quad (x \in \mathbb{R}) \\ (x - 3)(x - 4) &= 0 \\ \rightarrow x - 3 = 0 \quad \vee \quad x - 4 = 0 \\ x_1 &= 3 \quad x_2 = 4 \end{aligned} \quad (1.43)$$

Wie zeigen wir, dass zwei Terme gleich sind?

Behauptung:

$$\sin 2\alpha = 2 \sin \alpha \cos \alpha \quad (1.44)$$

Wir wählen die linke Seite und formen diese so lange um, bis die rechte Seite entsteht (oder umgekehrt).

Es ist falsch

$$\sin 2\alpha = 2 \sin \alpha \cos \alpha \quad (1.45)$$

so lange umzuformen, bis eine Identität wie z.B. $1 = 1$ entsteht!

Beispiel 8. *Richtig ist*

$$\begin{aligned} \sin 2\alpha &= \sin \alpha + \alpha \\ \text{denn } \sin \alpha + \beta &= \sin \alpha \cos \beta + \sin \beta \cos \alpha \\ \sin \alpha + \alpha &= \sin \alpha \cos \alpha + \sin \alpha \cos \alpha \\ &= 2 \sin \alpha \cos \alpha \end{aligned} \quad (1.46)$$

□

Manchmal gelingt es nicht, die linke Seite in die rechte Seite umzuformen. Dann verwenden wir die Eigenschaft

”Wenn $l = x$ und $r = x$, so ist $l = r$ ”

Wir formen also die linke Seite zuerst einmal um und dann unabhängig davon die rechte Seite und hoffen, dass wir beide Male das gleiche Resultat (x) erhalten.

Beispiel 9. *Wir versuchen, dieses Konzept anzuwenden:*

Voraussetzung:

$$\tan \delta = \frac{\sin \delta}{\cos \delta} \quad \text{und} \quad \cot \delta = \frac{1}{\tan \delta} \quad (1.47)$$

Behauptung:

$$\tan \delta + \cot \delta = \frac{2}{\sin 2\delta} \quad (1.48)$$

Beweis:

1.

$$\begin{aligned} \tan \delta + \frac{1}{\tan \delta} &= \frac{\sin \delta}{\cos \delta} + \frac{\cos \delta}{\sin \delta} \\ &= \frac{\sin^2 \delta + \cos^2 \delta}{\sin \delta \cdot \cos \delta} = \frac{1}{\sin \delta \cdot \cos \delta} \end{aligned} \quad (1.49)$$

2.

$$\frac{2}{\sin 2\delta} = \frac{2}{2 \sin \delta \cdot \cos \delta} = \frac{1}{\sin \delta \cdot \cos \delta} \quad (1.50)$$

□

Genau gleich behandeln wir Behauptungen der Logik wenn es um die Äquivalenz zweier Aussagen geht.

Beispiel 10. 1. *Behauptung:*

$$[\neg(a \vee b) \wedge a] \iff [\neg(a \vee b) \wedge b] \quad (1.51)$$

Beweis:

(a)

$$\begin{aligned} \neg(a \vee b) \wedge a &= \neg a \wedge \neg b \wedge a \\ &= \neg a \wedge a \wedge \neg b = 0 \wedge \neg b = 0 \end{aligned} \quad (1.52)$$

(b)

$$\begin{aligned} \neg(a \vee b) \wedge b &= \neg a \wedge \neg b \wedge b \\ &= \neg a \wedge b \wedge \neg b = \neg a \wedge b = 0 \end{aligned} \quad (1.53)$$

Beide Terme sind äquivalent □

2. *Behauptung:*

$$a \rightarrow (b \wedge c) = (a \rightarrow b) \wedge (a \rightarrow c) \quad (1.54)$$

Beweis:

$$\begin{aligned} \neg a \vee (b \wedge c) &= (\neg a \vee b) \wedge (\neg a \vee c) \\ &= (a \rightarrow b) \wedge (a \rightarrow c) \end{aligned} \quad (1.55)$$

1.6 Logische Schlüsse

Wir gehen aus von verschiedenen Prämissen wie

$$\begin{array}{ll} \text{Prämisse 1} & p_1 = a \wedge b \\ \text{Prämisse 2} & p_2 = \neg a \\ \text{Prämisse 3} & p_3 = a \wedge \neg b \end{array} \quad (1.56)$$

und ziehen daraus eine Konklusion $k : a \vee b$. Nun fragen wir uns, ob die Konklusion bei diesen Prämissen richtig ist. Ist dies der Fall, so sprechen wir von einem logischen Schluss (wenn also das die richtige Konklusion ist).

Es muss also

$$(p_1 \wedge p_2 \wedge \dots \wedge p_n) \rightarrow k = 1 \quad (1.57)$$

eine Tautologie sein. Im Beispiel ist also

$$[(a \wedge b) \wedge \neg a \wedge (a \wedge \neg b)] \rightarrow (a \vee b) \quad (1.58)$$

so lange umgeformt werden, bis erkenntlich ist, ob eine Tautologie vorliegt oder nicht.

$$\begin{aligned}
& [(a \wedge b) \wedge \neg a \wedge (a \wedge \neg b)] \rightarrow (a \vee b) \\
& = (a \wedge b \wedge \neg a \wedge a \wedge \neg b) \rightarrow (a \vee b) \\
& = 0 \rightarrow (a \vee b) \\
& = \neg 0 \vee (a \vee b) = 1 \vee (a \vee b) = 1
\end{aligned} \tag{1.59}$$

und damit liegt ein logischer Schluss vor.

In der Logik schreiben wir Prämissen und Konklusion untereinander wie zum Beispiel

$$\frac{a \rightarrow b \quad a \wedge b \rightarrow c \quad c}{a} \tag{1.60}$$

Beispiel 11. *Handelt es sich hierbei um einen logischen Schluss?*

$$\begin{aligned}
& [(a \rightarrow b) \wedge \{(a \wedge b) \rightarrow c\} \wedge c] \rightarrow a \\
& = [(\neg a \vee b) \wedge \{\neg(a \wedge b) \vee c\} \wedge c] \rightarrow a \\
& = \neg[(\neg a \vee b) \wedge (\neg a \vee \neg b \vee c) \wedge c] \vee a \\
& = \neg[(\neg a \vee b) \wedge c] \vee a \\
& = \neg[(\neg a \wedge c) \vee (b \wedge c)] \vee a \\
& = [\neg(\neg a \wedge c) \wedge \neg(b \wedge c)] \vee a \\
& = [(a \vee \neg c) \wedge (\neg b \vee \neg c)] \vee a \\
& = (a \vee \neg c \vee a) \wedge (a \vee \neg b \vee \neg c) \\
& = (\neg c \vee a) \wedge (\neg b \vee \neg c \vee a) \\
& = (\neg c \vee a) \wedge \neg b
\end{aligned} \tag{1.61}$$

Also kein logischer Schluss □

Verschiedene bekannte logische Schlüsse besitzen einen Namen, wie zum Beispiel die Folgenden:

1. modus ponens (Abtrennungsregel)

$$\frac{a \rightarrow b \quad a}{b} \tag{1.62}$$

ist ein logischer Schluss, denn

$$\begin{aligned}
& [(a \rightarrow b) \wedge a] \rightarrow b \\
& = [(\neg a \vee b) \wedge a] \rightarrow b \\
& = (a \wedge b) \rightarrow b \\
& = \neg(a \wedge b) \vee b \\
& = \neg a \vee \neg b \vee b = \neg a \vee 1 = 1
\end{aligned} \tag{1.63}$$

Es ist die Art und Weise, wie wir einen mathematischen Satz $a \rightarrow b$ anwenden.

Beispiel 12. *Beispielsweise Kosinussatz:*

$a \rightarrow b$: In einem Dreieck ABC gilt $c^2 = a^2 + b^2 - 2ab \cdot \cos \gamma$

a : $a = 10, b = 7, \gamma = 70$

dann tritt b ein, d.h. c kann nun berechnet werden.

2. modus tollens (Aufhebende Schlussweise)

$$\frac{a \rightarrow b \quad \neg b}{\neg a} \quad (1.64)$$

ist ein logischer Schluss, denn

$$\begin{aligned} & [(a \rightarrow b) \wedge \neg b] \rightarrow \neg a \\ = & [(\neg a \vee b) \wedge \neg b] \rightarrow \neg a \\ = & [(b \wedge \neg b) \vee (\neg a \wedge \neg b)] \rightarrow \neg a \\ = & (\neg a \wedge \neg b) \rightarrow \neg a \\ = & \neg(\neg a \wedge \neg b) \vee \neg a \\ = & a \vee b \vee \neg a = 1 \vee b = 1 \end{aligned} \quad (1.65)$$

3. reductio ad absurdum (zurückführen auf einen Widerspruch)

$$\frac{a \rightarrow (b \wedge \neg b)}{\neg a} \quad (1.66)$$

ist ein logischer Schluss, denn

$$\begin{aligned} & [a \rightarrow (b \wedge \neg b)] \rightarrow \neg a \\ = & [a \rightarrow 0] \rightarrow \neg a \\ = & [\neg a \vee 0] \rightarrow \neg a \\ = & \neg a \rightarrow \neg a = a \vee \neg a = 1 \end{aligned} \quad (1.67)$$

Dieser logische Schluss führt uns zum Beweis mit Gegenannahme.

Wollen wir beweisen, dass ein Satz s wahr ist und gelingt uns dies nicht mit einem direkten Beweis oder mit einem Beweis mit Kontraposition, so wählen wir die Gegenannahme:

$\neg s$ ist wahr

und zeigen, dass dies zu einem Widerspruch führt wie $\neg b \wedge b$ oder $1 = 2$ oder ähnlich.

Dann sagt uns die "reductio ad absurdum", dass meine Gegenannahme falsch ist und damit die Aussage s wahr ist.

Beispiel 13. 1. Satz: "Es gibt unendlich viele Primzahlen"
Beweis mit Gegenannahme (Euklid, ca. 300 v.Chr., Alexandria):

"Es gibt nur endlich viele Primzahlen"

$$p_1 < p_2 < p_3 < \dots < p_{n-1} < p_n \quad (1.68)$$

wobei p_n die Grösste sei.

Nun bilden wir eine neue Zahl

$$z = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1 \quad (1.69)$$

die sicher keine der Zahlen $p_1, p_2, p_3, \dots, p_n$ als Primfaktoren besitzt.

Nun ist z entweder

(a) eine Primzahl, dann ist dies ein Widerspruch

(b) keine Primzahl und damit in Primfaktoren zerlegbar. Es muss also neben p_1, p_2, \dots, p_n einen weiteren Primfaktor geben, dies ist ein Widerspruch

zur Gegenannahme.

Also ist die Gegenannahme falsch und damit die ursprüngliche Behauptung wahr. \square

2. Behauptung: $\sqrt{2}$ ist irrational

Beweis mit Gegenannahme:

$\sqrt{2}$ ist rational

also ist $\sqrt{2} = \frac{p}{q} \wedge p, q \in \mathbb{N}$ und vollständig gekürzt. Somit

$$\begin{aligned} 2 &= \frac{p^2}{q^2} \\ p^2 &= 2q^2 \end{aligned} \quad (1.70)$$

Also ist p^2 eine gerade Zahl und damit auch p (Beweis siehe 1.37). Somit ist $p = 2x \wedge p \in \mathbb{N}$, was eingesetzt in 1.70 zu

$$(2x)^2 = 2q^2 \quad (1.71)$$

führt. Weiter ist

$$\begin{aligned} 4x^2 &= 2q^2 \\ 2x^2 &= q^2 \end{aligned} \quad (1.72)$$

Also ist q^2 gerade und damit auch q . Somit ist

$$q = 2y \wedge y \in \mathbb{N} \quad (1.73)$$

Wir haben also gefunden

$$\sqrt{2} = \frac{p}{q} = \frac{2x}{2y} \quad (1.74)$$

und damit erhalten wir einen Widerspruch zu "vollständig gekürzt". Somit ist die Gegenannahme falsch und damit die Behauptung richtig.

Einen Beweis mit Gegenannahme nennen wir auch einen indirekten Beweis. Dieses Beweisverfahren können wir auch für logische Schlüsse anwenden.

Ist

$$\frac{a \wedge \neg b \quad a \rightarrow b}{a \vee b} \quad (1.75)$$

ein logischer Schluss?

Gegenannahme: Es ist liegt kein logischer Schluss vor und damit ist

$$[(a \wedge \neg b) \wedge (a \rightarrow b)] \rightarrow (a \vee b) = 0 \quad (1.76)$$

Nun zeigen wir, dass die Gegenannahme zu einem Widerspruch führt. Wir haben die Aussage

$$x \rightarrow y = 0$$

Also muss $x = 1$ und $y = 0$ sein.

Es ist $x = p_1 \wedge p_2 \wedge \dots \wedge p_n$ (Alle Prämissen und damit muss auch

$$p_1 = p_2 = \dots = p_n = 1$$

sein. Um den Widerspruch zu sehen, machen wir eine Tabelle:

	$a \wedge \neg b$	$a \rightarrow b$	\rightarrow	$a \vee b$
1)	<u>1</u>	1		0
2)				$a = 0, b = 0$
3)	<u>$0 \wedge 1 = 0$</u>			

(1.77)

Bei den unterstrichenen Werten haben wir einen Widerspruch hergeführt. Die Gegenannahme ist falsch, also liegt ein logischer Schluss vor.

Beispiel 14. 1. Ist

$$\frac{a \wedge \neg d \quad \neg a \vee c \quad (b \wedge \neg c) \rightarrow a}{a \vee c \vee d} \quad (1.78)$$

ein logischer Schluss?

Gegenannahme:

$$\{(a \wedge \neg d) \wedge (\neg a \vee c) \wedge [(b \wedge \neg c) \rightarrow a]\} \rightarrow (b \vee c \vee d) = 0 \quad (1.79)$$

also

	$a \wedge \neg d$	$\neg a \vee c$	$(b \wedge \neg c) \rightarrow a$	\rightarrow	$b \vee c \vee d$
1)	1	<u>1</u>	1		0
2)					$b = 0, c = 0, d = 0$
3)	$a = 1$				
4)		<u>$0 \vee 0 = 0$</u>			

(1.80)

Bei den unterstrichenen Werten haben wir einen Widerspruch hergeführt. Die Gegenannahme ist falsch, also liegt ein logischer Schluss vor.

2. Wir untersuchen, ob

$$\frac{a \rightarrow \neg b \quad \neg c \rightarrow d \quad c \rightarrow a \quad e \rightarrow b}{b \rightarrow (d \vee c)} \quad (1.81)$$

ein logischer Schluss ist. Gegenannahme:

$$[(a \rightarrow \neg b) \wedge (\neg c \rightarrow d) \wedge (c \rightarrow a) \wedge (e \rightarrow b)] \rightarrow [b \rightarrow (d \vee e)] = 0 \quad (1.82)$$

also

	$a \rightarrow \neg b$	$\neg c \rightarrow d$	$c \rightarrow a$	$e \rightarrow b$	\rightarrow	$b \rightarrow (d \vee e)$
1)	1	<u>1</u>	1	1		0
2)						1 \rightarrow 0, b = 1, d \vee e = 0, d = e = 0
3)	a = 0		c = 0			
4)		<u>1 \rightarrow 0 \neq 1</u>				

(1.83)

Also liegt ein logischer Schluss vor.

1.7 Prädikatenlogik

Einige Aussagen wie

- Informatiker(innen) besitzen einen Laptop
- Katzen schnurren
- Hunde bellen
- $a \cdot b = b \cdot a$

verlangen eine Präzisierung wie

- Nicht alle Informatiker(innen) besitzen einen Laptop
- Einige Katzen schnurren
- Alle Hunde bellen
- Für alle $a, b \in \mathbb{R}$ ist $a \cdot b = b \cdot a$

Wir brauchen also ein Prädikat (Aussage) über Größen aus einer bestimmten Menge und einen Quantor. Wir nennen \forall den Allquantor. Damit bedeutet

$$x \in M : \forall x (P(x))$$

(Für alle x gilt $P(x)$)

dass alle Elemente der Menge M das Prädikat P besitzen.

Beispiel 15. *Prädikatenlogik*

$$\begin{aligned} M &= \{x \mid x \text{ ist ein Hund}\} \\ B(x) &: x \text{ bellt} \end{aligned}$$

und es ist $x \in M : \forall x(B(x))$

Wählen wir

$$\begin{aligned} M &= \{s \mid s \text{ ist Student(in)}\} \\ q(s) &: s \text{ ist in der Klasse I1q} \end{aligned}$$

so können wir formulieren

$$s \in M : \forall s(q(s)) \quad (1.84)$$

was natürlich falsch ist. Korrekt ist

$$\neg \forall s(q(s)) \quad \text{oder auch} \quad \nexists s(q(s)) \quad (1.85)$$

geschrieben. Dieses "nicht alle" ist gleichbedeutend mit

"Es gibt (mindestens) ein(e)"

was wir mit dem Existenzquantor \exists so schreiben:

$$\exists s(\neg q(s)) \quad (1.86)$$

Wir haben also

$$\neg \forall x(P(x)) = \exists x(\neg P(x)) \quad (1.87)$$

Betrachten wir

$$\begin{aligned} K &= \{k \mid k \text{ ist eine Katze}\} \\ s(k) &: k \text{ schnurrt} \end{aligned}$$

und

$$k \in K : \exists k(s(k)) \quad (1.88)$$

was "es gibt mindestens eine Katze, die schnurrt" bedeutet. Verneinen wir die Aussage

$$\neg \exists k(s(k)) \quad \text{oder} \quad \nexists k(s(k)) \quad (1.89)$$

so bedeutet dies: "Es gibt keine Katze, die schnurrt.", was gleichbedeutend ist mit "Alle Katzen schnurren nicht", also

$$\neg \exists k(s(k)) = \forall k(\neg s(k)) \quad (1.90)$$

Auch in der Mathematik werden die Quantoren verwendet wie zum Beispiel

1.

$$a, b \in \mathbb{R} : \forall a \forall b(ab = ba) \quad (1.91)$$

oder auch

$$a, b \in \mathbb{R} : \forall a, b(ab = ba) \quad (1.92)$$

2.

$$a \in \mathbb{R} \setminus \{0\}, x \in \mathbb{R} : \forall a \exists x(ax = 1) \quad (1.93)$$

Wir nennen $x = a^{-1}$ das zu a inverse Element.

1.7.1 Zwei Prädikate

Oft ist es einfacher, wenn eine Aussage mit Hilfe von zwei Prädikaten formuliert wird. Für

”Alle Informatik-Studierenden besitzen ein iPhone”

wählen wir

$s = \{s \mid s \text{ ist Student(in)}\}$
 $i(s) : s \text{ studiert Informatik}$
 $p(s) : s \text{ besitzt ein iPhone}$

und schreiben

$$s \in S : \forall s(i(s) \rightarrow p(s)) \quad (1.94)$$

ist die Aussage falsch, weil nicht alle Informatik-Studierenden ein iPhone besitzen, so schreiben wir

$$\neg \forall s(i(s) \rightarrow p(s)) \quad (1.95)$$

was gleichbedeutend ist mit

$$\exists s(\neg[i(s) \rightarrow p(s)]) \quad (1.96)$$

Dies kann mit Hilfe der Gesetze der Logik umgeformt werden zu

$$\begin{aligned} & \exists s(\neg[\neg i(s) \vee p(s)]) \\ &= \exists s(i(s) \wedge \neg p(s)) \end{aligned} \quad (1.97)$$

Wir sehen also, dass der Existenzquantor eine Verbindung der Prädikate mit ”und” verlangt. Wollen wir ”Grosskatzen jagen und fressen Fleisch” formulieren, so wählen wir

$G = \{g \mid g \text{ ist eine Grosskatze}\}$
 $j(g) : g \text{ jagt}$
 $f(g) : g \text{ frisst Fleisch}$

und erhalten

$$g \in G : \exists g(j(g) \wedge f(g)) \quad (1.98)$$

weil wir nicht genau wissen, ob es vegetarische Grosskatzen gibt. Negation ergibt

$$\begin{aligned} \neg \exists g(j(g) \wedge f(g)) &= \forall g(\neg[j(g) \wedge f(g)]) \\ &= \forall g(\neg j(g) \vee \neg f(g)) \\ &= \forall g(j(g) \rightarrow [\neg f(g)]) \end{aligned} \quad (1.99)$$

Wir beachten also, dass

1. \forall verlangt Implikation (\rightarrow)

2. \exists verlangt Konjunktion (\wedge)

Bei

”Es gibt Leute, die beim Torten-Essen gerne einen Kaffee dazu trinken”

schreiben wir

$M = \{m \mid m \text{ ist ein Mensch} \}$

$T(m) : m$ isst ein Stück Torte

$K(m) : m$ trinkt Kaffee

$$m \in M : \exists m(T(m) \wedge K(m)) \quad (1.100)$$

und die Negation

$$\begin{aligned} & \neg \exists m(T(m) \wedge K(m)) \\ &= \forall m(\neg(T(m) \wedge K(m))) \\ &= \forall m(\neg T(m) \vee \neg K(m)) \\ &= \forall m(T(m) \rightarrow \neg K(m)) \quad \text{oder} \quad \forall m(K(m) \rightarrow \neg T(m)) \end{aligned} \quad (1.101)$$

1.7.2 Zweiwertige Prädikate

Sei

$M = \{x \mid x \text{ ist ein Mensch}\}$

so lassen sich für $x, y \in M$ z.B. die zweistelligen Prädikate

$L(x, y) : x$ liebt y

$K(x, y) : x$ kennt y

$S(x, y) : x$ streitet mit y

formulieren. Beachte, dass

$$\begin{aligned} K(x, y) &\neq K(y, x) \\ L(x, y) &\neq L(y, x) \end{aligned} \quad (1.102)$$

so bedeutet

$$x, y \in M : \forall x \exists y(K(x, y)) \quad (1.103)$$

dass alle Leute die Person y kennen. Und

$$x, y \in M : \exists x \forall y(K(y, x)) \quad (1.104)$$

bedeutet ”Es gibt einen Menschen x , der allen y bekannt ist”.

Chapter 2

Mengen

2.1 Mächtigkeit

Die Mengenlehre geht zurück auf Georg Cantor, 1845 bis 1918, in Halle. Heute definieren wir eine Menge, in dem wir ihre Element angeben.

2.1.1 Aufzählung

$$A = \{-3, a, \diamond, \sqrt{3}, x\}$$

$B = \{2, 2, 3, 4, 5\}$ ist nicht möglich: Jedes Element genau einmal, also ist

$$B = \{2, 3, 4, 5\}$$

$$C = \{10, 14, 18, 22, \dots\}$$

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$ heisst Menge der natürlichen Zahlen.

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ heisst Menge der ganzen Zahlen.

2.1.2 Charakterisierung

$$M = \{m | m \in \mathbb{N} \wedge 8 < m < 21\}$$

$$N = \{x | x \in 2^{2^{-n}} \wedge n \in \mathbb{N}\} \text{ also ist } N = \{2, 1, \frac{1}{2}, \frac{1}{4}, \dots\}$$

$A = \{x | x \in \mathbb{R} \wedge x^2 = -1\}$, A hat keine Elemente, die leere Menge \emptyset .

$\mathbb{Q} = \{x | x = \frac{a}{b} \wedge a, b \in \mathbb{Z} \wedge b \neq 0\}$ ist die Menge der rationalen Zahlen.

$\mathbb{R} = \{x | x \text{ ist als Dezimalbruch darstellbar}\}$ ist die Menge der reellen Zahlen.

2.1.3 Euler-Venn-Diagramm

Nach Leonard Euler, Riehen b. Basel, Petersburg, Berlin, 1707 bis 1783. TODO:
IMAGE

algebraische Zahl: Lösung einer (Polynom-) Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \quad (2.1)$$

mit rationalen Koeffizienten $a_i \in \mathbb{Q}$ ($i = 0, 1, \dots, n$)

transzendente Zahl: Nicht-algebraisch, aber irrational. Nach L. Euler: "quod algebrae vires transcendit" (lat. "Was die Kraft der Algebra übersteigt")
 π , e sind transzendente Zahlen.

Definition 6. Wir nennen die Anzahl der Elemente einer Menge A die Mächtigkeit $\|A\|$.

Beispiel 16. Wir untersuchen die Mächtigkeit der Menge A :

$$A = \{2, 7, 12, \dots, 122\}$$

$$\rightarrow \|A\| = 24$$

In $\mathbb{N} = \{1, 2, 3, \dots\}$ hat es unendlich viele Elemente.

Definition 7. Die Mächtigkeit von \mathbb{N} ist \aleph_0 ("Aleph-null").

Welches ist nun die Mächtigkeit von $G = \{2, 4, 6, \dots\}$?

Definition 8. Zwei Mengen A und B sind gleichmächtig $\|A\| = \|B\|$, wenn jedem Element von A genau eines von B zugeordnet werden kann und umgekehrt.

Es muss also eine Funktion von A nach B existieren, die umkehrbar ist.

Beispiel 17. Wir versuchen herauszufinden, ob folgende zwei Mengen (A und B) gleichmächtig sind:

$$A = \{4, 7, 10, \dots, 94\}$$

$$B = \{6, 10, 14, \dots, 82\}$$

Mit einer Funktion f

4	7	10	...	94
6	10	14	...	82

muss $f(a) = \frac{4}{3}(a-1)+2$ sein. So wird $f(94) = \frac{4}{3}(93)+2 = 4 \cdot 31 + 2 = 126 \neq 82$ und somit ist $\|A\| > \|B\|$.

Gehen wir nun zurück zu $G = \{2, 4, 6, 8, \dots\}$,

\mathbb{N}	1	2	3	4	...
\mathbb{G}	2	4	6	8	...

Mit $f(n) = 2n$ haben wir eine umkehrbare, eindeutige Funktion gefunden. Also ist $\|G\| = \aleph_0$

Betrachten wir nun

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \quad (2.2)$$

und versuchen eine Zuweisung mit \mathbb{N} zu bilden.

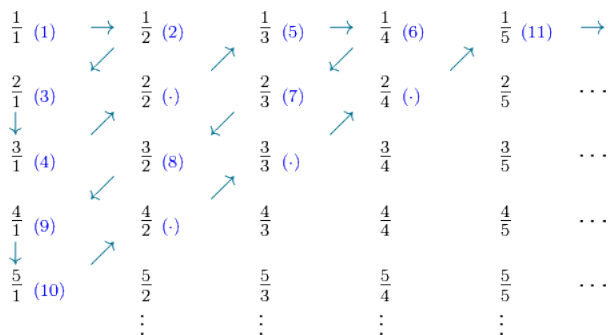
\mathbb{N}	1	2	3	4	5
\mathbb{Z}	0	1	-1	2	-2

und finden $\|\mathbb{Z}\| = \aleph_0$ mit

$$f(x) = \begin{cases} \frac{x}{2} & \text{wenn } x \text{ gerade, } x \in \mathbb{N} \\ \frac{-x-1}{2} & \text{wenn } x \text{ ungerade, } x \in \mathbb{N} \end{cases}$$

Definition 9. Eine Menge A mit $\|A\| = \aleph_0$ besitzt abzählbar-unendlich viele Elemente.

Wie ist es nun mit \mathbb{Q} und der Mächtigkeit? Wir versuchen das Cantorsche Diagonalverfahren.



Zusätzlich definieren wir als erstes Element in der Menge die Zahl 0. Kommt eine Zahl zum

- ersten Mal vor, so zählen wir diese
- zweiten Mal vor, so wählen wir diese negativ.
- dritten, vierten Mal vor, so überspringen wir diese

Die 0 kommt an den Anfang. Also ist $\|\mathbb{Q}\| = \aleph_0$.

Betrachten wir nun \mathbb{R} :

Wir versuchen zu ordnen: 0.1, 0.01, 0.001, ...

Es gelingt nicht, eine Funktion von \mathbb{N} nach \mathbb{R} zu finden.

Definition 10. Die Menge \mathbb{R} ist überabzählbar-unendlich und ihre Mächtigkeit ist \aleph_1 .

2.2 Vollständige Induktion

Nach Giuseppe Peano, Turin, 1858 bis 1932

Peano hat gezeigt, dass die natürlichen Zahlen auf den Axiomen

Axiom 1. Es gibt eine kleinste Zahl

Axiom 2. Jede Zahl besitzt einen Nachfolger

Axiom 3. *Gilt eine Aussage für n und auch für $n+1$, so gilt sie für alle $n \in \mathbb{N}$, falls sie für $n=1$ gilt.*

beruhen (Peano-Axiome genannt).

Axiom (3) führt uns zum Beweis mit vollständiger Induktion. Dieser Beweis besteht aus drei Teilen.

1. Induktionsverankerung (Induktionsanfang)
Die Behauptung stimmt für $n=1$
2. Induktionsschritt
Unter der Voraussetzung, dass die Behauptung für n gilt, ist zu zeigen, dass sie auch für $n+1$ gilt.
3. Induktionsvererbung (Induktionsschluss)

Beispiel 18. 1. *Behauptung:* $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$
Beweis mit vollständiger Induktion

(a) *Behauptung ist für $n=1$ richtig, denn*

$$\frac{n(n+1)(2n+1)}{6} \quad \text{wird} \quad \frac{1 \cdot (1+1)(2+1)}{6} = 1 \quad (2.3)$$

und

$$1^2 = 1 \quad (2.4)$$

(b) *Voraussetzung:* $s_n = 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$
Behauptung: $s_{n+1} = 1^2 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2$
damit

$$\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} = \frac{(n+1)(n+2)(2n+3)}{6} \quad (2.5)$$

Beweis 7.

$$\begin{aligned} s_{n+1} &= 1^2 + 2^2 + 3^2 + \dots + (n+1)^2 \\ &= s_n + (n+1)^2 \\ &= \frac{1}{6}n(n+1)(2n+1) + (n+1)^2 \\ &= \frac{1}{6}(n^2+n)(2n+1) + n^2 + 2n + 1 \\ &= \frac{1}{6}(2n^3 + n^2 + 2n^2 + n) + n^2 + 2n + 1 \\ &= \frac{1}{6}(2n^3 + 3n^2 + n + 6n^2 + 12n + 6) \\ &= \frac{1}{6}(2n^3 + 9n^2 + 13n + 6) \end{aligned} \quad (2.6)$$

und

$$\begin{aligned}
\frac{(n+1)(n+2)(2n+3)}{6} &= \frac{1}{6}(n^2+3n+2)(2n+3) \\
&= \frac{1}{6}(2n^3+6n^2+3n^2+4n+9n+6) \\
&= \frac{1}{6}(2n^3+9n^2+13n+6) \quad (2.7)
\end{aligned}$$

(a) Nach (1a) gilt die Behauptung für $n = 1$ und nach 1b gilt sie für $n + 1$, falls sie für n gilt.
Also gilt sie für $n = 2$ und nach 1b für $n + 1$, ist 3 usw. Also gilt die Behauptung für alle $n \in \mathbb{N}$