Beweis von $A \Rightarrow B$ durch Widerspruch

Idee:
Nimm an, dass $A \wedge \neg B$ wahr ist, und führe dies auf einen Widerspruch der Form „$C \wedge \neg C$ ist wahr" für eine mathematische Aussage C.

- Da $C \wedge \neg C$ nicht wahr sein kann, muss unsere Annahme $A \wedge \neg B$ falsch gewesen sein.
- Dann ist aber $\neg(A \wedge \neg B)$ wahr.

A	B	$\neg(A \wedge \neg B)$	$A \Rightarrow B$
w	w	w	w
w	f	f	f
f	w	w	w
f	f	w	w

- $\neg(A \wedge \neg B)$ ist genau dann wahr, wenn $A \Rightarrow B$ wahr ist.

Widerspruchsbeweis – Beispiel

Satz: („$\sqrt{2}$ ist nicht rational“) Wenn $x \in \mathbb{Q}$ und $x > 0$, dann ist $x^2 \neq 2$.

Beweis: Wir nehmen an, dass $x \in \mathbb{Q}$, $x > 0$ und $x^2 = 2$. Dann gibt es teilerfremde Zahlen $p \in \mathbb{N}, q \in \mathbb{N} \setminus \{0\}$ mit $\frac{p}{q} = x$. Es ist dann $\frac{p^2}{q^2} = 2$ und somit

$$p^2 = 2q^2. \qquad (1)$$

Also ist p^2 gerade. Nach vorigem Satz ist auch p gerade, das heißt, es existiert ein $m \in \mathbb{N}$ mit $p = 2m$. Setzt man dies in (1) ein, so erhält man

$$4m^2 = 2q^2 \quad \text{bzw.} \quad 2m^2 = q^2.$$

Also ist nach vorigem Satz auch q gerade. Damit besitzen p und q den gemeinsamen Teiler 2 ↯ (im Widerspruch zu deren Teilerfremdheit). □

Aussagen und ihre Verknüpfungen

Äquivalenz: $A \Leftrightarrow B$ (das heißt $(A \Rightarrow B) \wedge (B \Rightarrow A)$)

Sprechweise: „A (gilt) genau dann, wenn B (gilt)."
„A (gilt) dann und nur dann, wenn B (gilt)."
„A ist notwendig und hinreichend für B."
„A und B sind äquivalent."

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
w	w	w	w	w
w	f	f	w	f
f	w	w	f	f
f	f	w	w	w

Beispiel

Wir haben soeben für eine Zahl $n \in \mathbb{N}$ gezeigt:
„n ist genau dann gerade, wenn n^2 gerade ist."

Normalformen

Bemerkung

Seien $A_1, A_2, A_3, \ldots$ mathematische Aussagen. Man kann jede logische Formel F in disjunktiver Normalform schreiben, also

$$F \equiv (L_{1,1} \wedge \ldots \wedge L_{1,m_1}) \bigvee \ \ldots \ \bigvee (L_{n,1} \wedge \ldots \wedge L_{n,m_n})$$

und in konjunktiver Normalform, also

$$F \equiv (L_{1,1} \vee \ldots \vee L_{1,m_1}) \bigwedge \ \ldots \ \bigwedge (L_{n,1} \vee \ldots \vee L_{n,m_n}),$$

wobei $L_{i,j} \in \{A_1, \neg A_1, A_2, \neg A_2, A_3, \neg A_3, \ldots\}$.

- Mehr dazu in der Veranstaltung „Digitaltechnik und Rechnersysteme".

Boolesche Algebra

Eine boolesche Algebra $\mathcal{B} = (B, 0, 1, \oplus, \odot, \overline{})$ ist gegeben durch eine Menge B mit $0, 1 \in B$ (dem Null- und Einselement) und den „zweistelligen Verknüpfungen" „$\oplus$" und „$\odot$" (ergeben angewendet auf zwei Elemente aus B wieder ein Element aus B) und der „einstelligen Verknüpfung" „$\overline{}$" (ergibt angewendet auf ein Element aus B wieder ein Element aus B), so dass für alle $a, b, c \in B$ gilt:

1. $a \oplus b = b \oplus a$ und $a \odot b = b \odot a$ (Kommutativgesetze)
2. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ und $a \odot (b \odot c) = (a \odot b) \odot c$ (Assoziativgesetze)
3. $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c)$ und
   $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ (Distributivgesetze)
4. $a \oplus 0 = a$ und $a \odot 0 = 0$
   $a \oplus 1 = 1$ und $a \odot 1 = a$ (Eigenschaften von 0 und 1)
5. $a \oplus \overline{a} = 1$ und $a \odot \overline{a} = 0$ (Eigenschaften von „$\overline{}$")
6. $a \oplus (a \odot b) = a$ und $a \odot (a \oplus b) = a$ (Absorption)

Beispiele

- $(\{0,1\},0,1,+,\cdot,\overline{})$ mit
  - $0+0=0, 1+0=0+1=1+1=1,$
  - $0\cdot 0=0\cdot 1=1\cdot 0=0, 1\cdot 1=1$
  - $\overline{0}=1, \overline{1}=0$

  ist eine boolesche Algebra.

- $(\{f,w\},f,w,\vee,\wedge,\neg)$ ist eine boolesche Algebra.
  Sie ist „isomorph“ zu $(\{0,1\},0,1,+,\cdot,\overline{})$.

- Sei X eine nicht-leere Menge. Dann ist $(\mathbb{P}(X),\emptyset,X,\cup,\cap,\overline{})$, wobei „$\overline{}$“ die Komplementbildung in X bezeichnet, eine boolesche Algebra.

- $(\mathbb{N},0,1,+,\cdot,\overline{})$ mit üblicher Addition und Multiplikation kann keine boolesche Algebra sein, egal wie „$\overline{}$“ definiert ist.

De Morgansche Regeln

Aus den Eigenschaften einer booleschen Algebra kann man folgenden Satz herleiten:

Satz

Sei $\mathcal{B} = (B, 0, 1, \oplus, \odot, ^{-})$ eine boolesche Algebra. Dann gilt für alle $a, b \in B$

$$\overline{a \oplus b} = \overline{a} \odot \overline{b},$$
$$\overline{a \odot b} = \overline{a} \oplus \overline{b}.$$

Mathematische Grundlagen der Informatik

WiSe 2024/2025

KAPITEL I: Grundlagen

3. Quantoren

Dozentin: Prof. Dr. Agnes Radl (Vertretung: Prof. Dr. A. Gepperth)

Email: `alexander.gepperth@informatik.hs-fulda.de`

Quantoren

Ist M eine Menge und $A(m)$ eine Aussage über m, so schreibt man

- $\forall m \in M : A(m)$
  „Für alle Elemente m der Menge M gilt $A(m)$."
- $\exists m \in M : A(m)$
  „Es gibt (mindestens) ein Element m in der Menge M, für das $A(m)$ gilt."

(Der Doppelpunkt wird manchmal weggelassen.)

$\forall$ „Allquantor"
$\exists$ „Existenzquantor"

Quantoren

Beispiel

$A(m)$: „m ist gerade.“

$M = \{2, 8, 10, 11\}$

- $\forall m \in M : A(m)$ (falsch)
  „Jedes $m \in M$ ist gerade.“
- $\exists m \in M : A(m)$ (wahr)
  „Es gibt ein $m \in M$, das gerade ist.“

$\tilde{M} = \{2, 8, 10\}$

- $\forall m \in \tilde{M} : A(m)$ (wahr)
  „Jedes $m \in \tilde{M}$ ist gerade.“
- $\exists m \in \tilde{M} : A(m)$ (wahr)
  „Es gibt ein $m \in \tilde{M}$, das gerade ist.“

Negation des Allquantors

Beispiel

$M = \{2, 8, 10, 11\}$, $A(m)$: „m ist gerade."

Was ist die Negation von

$$\forall m \in M : A(m) \quad \text{„Jedes } m \in M \text{ ist gerade."?}$$

Die Negation in Worten erhält man, indem man einfach „Es gilt nicht, dass ..." voranstellt, also

„Es gilt nicht, dass jedes $m \in M$ gerade ist."

Das heißt aber, dass es mindestens ein $m \in M$ gibt, welches nicht gerade ist:

$$\exists m \in M : \neg A(m) \quad \text{„Es gibt ein } m \in M, \text{ welches nicht gerade ist."}$$

Beobachtung

Bei der Negation wird aus dem Allquantor ein Existenzquantor und die Aussage $A(m)$ wird negiert.

Negation des Existenzquantors

Beispiel
$M = \{2, 8, 10, 11\}$, $\quad A(m)$: „m ist gerade."

Was ist die Negation von

$$\exists m \in M : A(m) \quad \text{„Es gibt ein } m \in M \text{, das gerade ist."?}$$

Die Negation in Worten erhält man, indem man einfach „Es gilt nicht, dass ..." voranstellt, also

„Es gilt nicht, dass es ein $m \in M$ gibt, das gerade ist."

Das heißt aber, dass alle $m \in M$ nicht gerade sind:

$\forall m \in M : \neg A(m)$ „Für jedes $m \in M$ gilt, dass es nicht gerade ist."

Beobachtung
Bei der Negation wird aus dem Existenzquantor ein Allquantor und die Aussage $A(m)$ wird negiert.

Quantoren – Negation

Beispiel

$M = \{2, 8, 10, 11\}$, $A(m)$: „m ist gerade.“

- Die Negation von $\forall m \in M : A(m)$ ist $\exists m \in M : \neg A(m)$.
  „Es gibt ein $m \in M$, welches nicht gerade ist.“
- Die Negation von $\exists m \in M : A(m)$ ist $\forall m \in M : \neg A(m)$.
  „Für jedes $m \in M$ gilt, dass es nicht gerade ist.“

Allgemein

Die Negation von $\forall m \in M : A(m)$ ist

$$\exists m \in M : \neg A(m).$$

Die Negation von $\exists m \in M : A(m)$ ist

$$\forall m \in M : \neg A(m).$$

Bei der Negation wird der Quantor geändert und die Aussage negiert. Der Wahrheitswert ändert sich dabei.

Negation bei mehreren Quantoren

Beispiel

„Zu jedem $x \in \mathbb{N}$ existiert ein $y \in \mathbb{N}$, so dass $y < x$ gilt.“ (falsch)

Mit Quantoren:

$$\forall x \in \mathbb{N} \underbrace{\exists y \in \mathbb{N} : y < x}_{A} \qquad (\star)$$

Beobachtung: $(\star)$ ist von der Form $\forall x \in \mathbb{N} : A$.

1.) Negation von $\forall x \in \mathbb{N} : A$ wie oben:
$\exists x \in \mathbb{N} : \neg A$

2.) Negation von A wie oben:
$\forall y \in \mathbb{N} : \neg(y < x)$ bzw. $\forall y \in \mathbb{N} : y \geq x$

Insgesamt Negation von $(\star)$:

$$\exists x \in \mathbb{N} \, \forall y \in \mathbb{N} : y \geq x$$

„Es existiert ein $x \in \mathbb{N}$, so dass für alle $y \in \mathbb{N}$ gilt, dass y größer oder gleich x ist.“ (wahr)

Stehen mehrere Quantoren nebeneinander, werden die Quantoren der Reihe nach geändert und die übrig bleibende Aussage negiert.

Mathematische Grundlagen der Informatik

WiSe 2024/2025

KAPITEL I: Grundlagen

4. Summen- und Produktzeichen

Dozentin: Prof. Dr. Agnes Radl (Vertretung: Prof. Dr. A. Gepperth)

Email: alexander.gepperth@informatik.hs-fulda.de

Summenzeichen

Für $m, n \in \mathbb{Z}$, $m \leq n$, und $a_m, a_{m+1}, a_{m+2}, \ldots, a_n \in \mathbb{R}$ definiert man

$$\boxed{\sum_{k=m}^{n} a_k := a_m + a_{m+1} + \ldots + a_n.}$$

Falls $m > n$, so definiert man

$$\boxed{\sum_{k=m}^{n} a_k := 0.}$$

Ist c eine reelle Zahl, so bedeutet

$$\sum_{k=m}^{n} c,$$

dass $a_m = \ldots = a_n = c$ gilt.

Produktzeichen

Für $m, n \in \mathbb{Z}$, $m \leq n$, und $a_m, a_{m+1}, a_{m+2}, \ldots, a_n \in \mathbb{R}$ definiert man

$$\boxed{\prod_{k=m}^{n} a_k := a_m \cdot a_{m+1} \cdot \ldots \cdot a_n.}$$

Falls $m > n$, so definiert man

$$\boxed{\prod_{k=m}^{n} a_k := 1.}$$

Ist c eine reelle Zahl, so bedeutet

$$\prod_{k=m}^{n} c,$$

dass $a_m = \ldots = a_n = c$ gilt.

Fakultät

Definition

Für $n \in \mathbb{N}$ definiert man

$$\boxed{n! := \prod_{k=1}^{n} k.}$$

Bemerkung

- Es ist $0! = 1$.
- Für $n < 0$ ist $n!$ nicht definiert.

Binomialkoeffizienten

Definition

Für $n, k \in \mathbb{N}$ und $k \leq n$ ist

$$\boxed{\binom{n}{k} := \frac{n!}{k!(n-k)!}.}$$

Eigenschaften

- $\binom{n}{0} = 1 = \binom{n}{n}$, falls $n \in \mathbb{N}$.
- $\binom{n}{1} = n = \binom{n}{n-1}$, falls $n \in \mathbb{N}^*$.
- $\binom{n}{k} = \binom{n}{n-k}$, falls $n, k \in \mathbb{N}$ und $k \leq n$.
- $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$, falls $n, k \in \mathbb{N}$ und $k + 1 \leq n$.