1

Prof. Dr. Hartmut Ring
Universität Siegen

Diskrete Mathematik für Informatiker
Wintersemester 2010/2011

1. Logik und Mengen

Aussagen

Wer Banknoten nachmacht
oder verfälscht
oder nachgemachte oder verfälschte
sich verschafft
und in Verkehr bringt,
wird mit Freiheitsstrafe
nicht unter zwei Jahren
bestraft.

Aussagen

Wer Banknoten nachmacht oder verfälscht oder nachgemachte oder verfälschte sich verschafft und in Verkehr bringt, wird mit Freiheitsstrafe nicht unter zwei Jahren bestraft.

Wer

Banknoten nachmacht

oder

verfälscht

oder

nachgemachte oder verfälschte sich verschafft

und

in Verkehr bringt,

wird mit Freiheitsstrafe nicht unter zwei Jahren bestraft.

Aussagen

Interpretation A:

Wer

Banknoten nachmacht

oder

verfälscht

oder

nachgemachte oder verfälschte sich verschafft

und

in Verkehr bringt,

wird mit Freiheitsstrafe nicht unter zwei Jahren bestraft.

Aussagen

Interpretation B:

Wer

Banknoten nachmacht

oder

verfälscht

oder

nachgemachte oder verfälschte sich verschafft

und

in Verkehr bringt,

wird mit Freiheitsstrafe nicht unter zwei Jahren bestraft.

Lösung in § 146 StGB: `http://www.jusline.de/146_Geldfälschung_StGB.html`

Aussagen

Definition 1.1

Eine **Aussage** ist ein Satz, der entweder wahr oder falsch ist.

Definition 1.3

Die ***Negation*** (Verneinung) einer Aussage a ist genau dann wahr, wenn a falsch ist.
Schreibweise: $\neg a$

Definition 1.5

Die ***Konjunktion*** (Und-Verknüpfung) zweier Aussagen a und b ist genau dann wahr, wenn beide Aussagen wahr sind.
Schreibweise: $a \wedge b$

Definition 1.5

Die ***Disjunktion*** (Oder-Verknüpfung) zweier Aussagen a und b ist genau dann wahr, wenn mindestens eine der beiden Aussagen wahr ist.
Schreibweise: $a \vee b$

Die ***exklusive Oder-Verknüpfung*** zweier Aussagen a und b ist genau dann wahr, wenn die Wahrheitswerte der beiden Aussagen verschieden sind.
Schreibweise z.B. $a \text{ xor } b$

Wahrheitswerttafeln

Einstellige Verknüpfung

Negation

a	$\neg a$
0	1
1	0

Zweistellige Verknüpfungen

Konjunktion

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

Disjunktion

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

Exklusives Oder

a	b	a xor b
0	0	0
0	1	1
1	0	1
1	1	0

Subjunktion, Implikation

Definition 1.15

Subjunktion

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

Eine (verknüpfte) Aussage heißt ***allgemeingültig***, wenn sie bei jeder möglichen Belegung der Wahrheitswerte wahr wird.

Definition 1.17

Eine allgemeingültige Aussage der Form $a \rightarrow b$ heißt ***Implikation*** (oder Wenn-dann-Aussage).

Man schreibt dann $a \Rightarrow b$ und sagt

- aus a folgt b,
- wenn a, dann b,
- a ist hinreichend für b,
- b ist notwendig für a.

Bijunktion, Äquivalenz

Definition 1.15

Bijunktion

a	b	$a \leftrightarrow b$
0	0	1
0	1	0
1	0	0
1	1	1

$a \rightarrow b \Leftrightarrow \neg a \vee b$

Definition 1.20

Eine allgemeingültige Aussage der Form $a \leftrightarrow b$ heißt ***Äquivalenz***.

Man schreibt dann $a \Leftrightarrow b$ und sagt:
- a (gilt) genau dann, wenn b,
- a (gilt) dann und nur dann, wenn b,
- a ist äquivalent mit b,
- a ist notwendig und hinreichend für b.

Satz 1.18

Es gelten die folgenden Äquivalenzen:
$a \rightarrow b \Leftrightarrow \neg b \rightarrow \neg a$
$a \leftrightarrow b \Leftrightarrow \neg a \leftrightarrow \neg b$

De Morgan'sche Regeln

$\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$
$\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b$

Weitere Äquivalenzregeln

Satz 1.42

Es gelten die folgenden Äquivalenzen:

Kommutativregeln
$a \vee b \Leftrightarrow b \vee a$
$a \wedge b \Leftrightarrow b \wedge a$

Assoziativregeln
$(a \vee b) \vee c \Leftrightarrow a \vee (b \vee c)$
$(a \wedge b) \wedge c \Leftrightarrow a \wedge (b \wedge c)$

Distributivregeln
$a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c)$
$a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c)$

Absorptionsregeln
$a \wedge (a \vee b) \Leftrightarrow a$
$a \vee (a \wedge b) \Leftrightarrow a$
$a \vee (\neg a \wedge b) \Leftrightarrow a \vee b$
$a \wedge (\neg a \vee b) \Leftrightarrow a \wedge b$

Alle zweistelligen Verknüpfungen

nor $\neg(a \lor b)$

nand $\neg(a \land b)$

a	b	0	$\land$		a		b	xor	$\lor$		$\leftrightarrow$	$\neg b$		$\neg a$	$\rightarrow$		1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Aussageformen

Definition 1.7

Eine ***Aussageform*** $a(x)$ ist ein Satz, in dem eine Konstante durch die Variable x ersetzt wird.

Definition 1.10

Allquantor:
$\forall x$: $a(x)$ ist die Aussage, die genau dann wahr ist, wenn $a(x)$ für alle in Frage kommenden x wahr ist.

Existenzquantor:
$\exists x$: $a(x)$ ist die Aussage, die genau dann wahr ist, wenn es unter den in Frage kommenden Objekten mindestens ein x gibt, für das $a(x)$ wahr ist.

Satz 1.13

Es gelten die folgenden Äquivalenzen:
$\neg \forall x: a(x) \Leftrightarrow \exists x: \neg a(x)$
$\neg \exists x: a(x) \Leftrightarrow \forall x: \neg a(x)$

Auch Aussageformen mit mehreren Variablen möglich!
Es gilt:
$\exists x: \forall y: a(x,y) \Rightarrow \forall y: \exists x: a(x,y)$
aber nicht:
$\cancel{\forall x: \exists y: a(x,y) \Rightarrow \exists y: \forall x: a(x,y)}$

Beweistypen

Direkter Beweis

- Eine Folgerung $a \Rightarrow b$ wird bewiesen,
  indem man ausgehend von a
  in einer logischen Schlusskette schließlich zu b kommt.

Indirekter Beweis

- *Widerspruchsbeweis*: Aus der Annahme,
  die Voraussetzung (a) sei wahr
  und die zu beweisende Behauptung (b) sei falsch,
  wird in einer Schlusskette gezeigt,
  dass daraus eine bekanntermaßen falsche Aussage folgt.
- *Kontraposition*:
  $a \Rightarrow b$ ist logisch äquivalent zu $\neg b \Rightarrow \neg a$

Beweis durch vollständige Induktion

- Nur anwendbar auf Aussagen, die für alle natürlichen Zahlen (oder aufzählbare Mengen) gelten.

Direkter Beweis: Beispiel

Eine Folgerung $a \Rightarrow b$ wird bewiesen,
indem man ausgehend von a in einer logischen Schlusskette
schließlich zu b kommt.

Behauptung:
Wenn eine natürliche Zahl n keine Primzahl ist,
dann hat sie mindestens einen Primfaktor p mit $1 < p \leq \sqrt{n}$.

Beweis:
Da n keine Primzahl ist,
kann man sie als Produkt aus zwei verschiedenen natürlichen Zahlen schreiben: $n = a\,b$ (mit $1 < a \leq b < n$)
Also ist $n = a\,b \geq a^2$ und damit $a \leq \sqrt{n}$.
Entweder ist a Primzahl
oder a (und damit auch n) hat einen Primfaktor $p < a \leq \sqrt{n}$

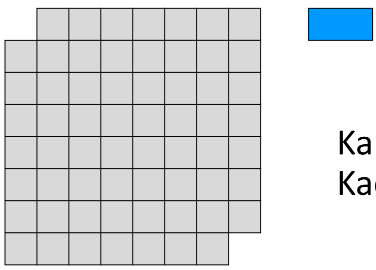
Übung:
Wie sieht die Kontraposition der Behauptung aus?

Schwierige Beweise

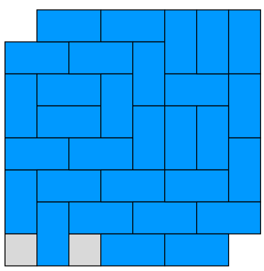
- Beweis leicht zu verstehen, aber schwer zu finden
  - nicht durch „Transfer“ bekannten Wissens sondern durch „Geistesblitz“
  - Mini-Beispiel: nächste Folie
- Technisch umfangreicher Beweis (evtl. nur durch Computerhilfe)
  - Beispiel: Vierfarbensatz

Problemlösung mit „Trick“

Diskrete Mathematik für Informatiker © Hartmut Ring, 2011

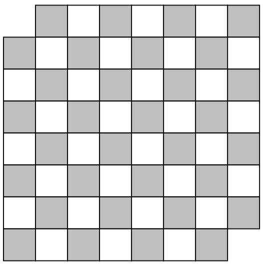


Kann man diese „Wand“ mit 31 Kacheln bedecken?



Ein gescheiterter Lösungsversuch

Problemlösung mit „Trick“



Die Wand hat 32 schwarze und 30 weiße Felder

30 Kacheln bedecken 30 weiße und 30 schwarze Felder

Die 31. Kachel müsste zwei schwarze Felder bedecken. Das ist unmöglich!

Mengen

Definition 1.22

Eine ***Menge*** ist eine Zusammenfassung von beliebigen Objekten. Die Reihenfolge spielt keine Rolle.

Georg Cantor
1845-1918

Unter einer „Menge“ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unsrer Anschauung oder unseres Denkens (welche die „Elemente“ von M genannt werden) zu einem Ganzen.

Mengen können beschrieben werden, indem man

(a) alle Elemente angibt (nur für endliche Mengen möglich),

(b) eine charakterisierende Eigenschaft angibt.

Beispiel

$\{2, 3, 5, 7\} = \{7, 3, 5, 3, 2, 7\}$ **(a)**

$= \{ x \in \mathbb{N} \mid x \text{ ist Primzahl und } x < 10 \}$ **(b)**

Wichtige Zahlenmengen

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

$\mathbb{N}_0$ = {0, 1, 2, 3, …}

$\mathbb{Z}$ Menge der ganzen Zahlen

$\mathbb{Q}$ Menge der rationalen Zahlen

$\mathbb{R}$ Menge der reellen Zahlen

$\mathbb{C}$ Menge der komplexen Zahlen

Grundbegriffe (1)

Schreibweise	Bedeutung		
$x \in A$	x ist ***Element*** der Menge A		
$x \notin A$	x ist nicht Element der Menge A		
$\emptyset$	die ***leere Menge***	oder: {}	
$A \cup B$	***Vereinigung*** von A und B	$A \cup B = \{x \mid x \in A \vee x \in B\}$	Def. 1.29
$A \cap B$	***Durchschnitt*** von A und B	$A \cap B = \{x \mid x \in A \wedge x \in B\}$	Def. 1.27
$A \subseteq B$	A ist ***Teilmenge*** von B	$\forall x \in A$ gilt $x \in B$	Def. 1.25
$A \subset B$	A ist ***echte Teilmenge*** von B	$A \subseteq B$ und $A \neq B$	
A und B *disjunkt*	$A \cap B = \emptyset$		
$A \setminus B$	***Differenzmenge***	$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$	Def. 1.32

Grundbegriffe (2)

$\mathcal{P}(A)$	***Potenzmenge*** Menge aller Teilmengen von *A*	$\mathcal{P}(A) = \{M \mid M \subseteq A\}$
$\lvert A \rvert$	Anzahl der Elemente von *A* (nur für endliche Menge *A*)	andere Schreibweise: card(*A*) andere Bezeichnungen: Mächtigkeit, Kardinalzahl

Für endliche Mengen A gilt $\lvert\mathcal{P}(A)\rvert = 2^{\lvert A\rvert}$

Bezüglich einer Grundmenge U („universelle" Menge)
wird definiert:

$\overline{A}$	*Komplement* der Menge *A*	$\overline{A} = U \setminus A$	Def. 1.32
$A \,\Delta\, B$	*Symmetrische Differenz*	$A \,\Delta\, B = A \cup B \setminus A \cap B$	
$A \times B$	*Kartesisches Produkt*	$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$	Def. 1.37

Einfache Mengengesetze

Satz

Für beliebige Mengen *A*, *B*, *C* gilt:

(1)	$A = B \iff A \subseteq B \wedge B \subseteq A$		
(2a) (2b)	$A \cup B = B \cup A$ $A \cap B = B \cap A$	Kommutativ- gesetze	Satz 1.31
(3a) (3b)	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	Assoziativ- Gesetze	Satz 1.31
(4a) (4b)	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributiv- gesetze	Satz 1.31
(5a) (5a)	$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgan'sche Regeln	Satz 1.34
(5a) (5b) (5c)	$A \cup \varnothing = A$ $A \cap \varnothing = \varnothing$ $A \setminus \varnothing = A$		

Beweis von Mengengleichungen

Satz

Zwei Teilmengen A und B einer Grundmenge M sind gleich, wenn für alle Elemente $x \in M$ gilt:
$x \in A \Leftrightarrow x \in B$

Beispiel

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Beweis:

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \wedge x \in (B \cup C) \\ &\Leftrightarrow x \in A \wedge (x \in B \vee x \in C)) \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)) \\ &\Leftrightarrow (x \in A \cap B) \vee (x \in A \cap C)) \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

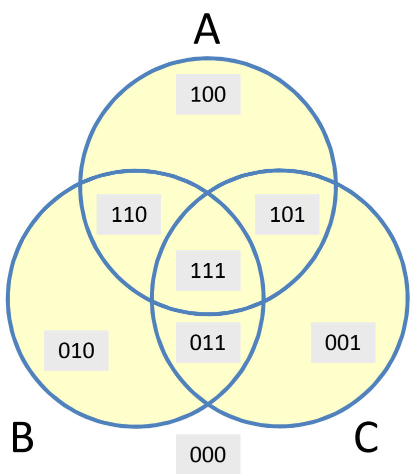
Beweis von Mengengleichungen durch Fallunterscheidung

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

3 Mengen: 2^3 Fälle

$x \in A$	0	0	0	0	1	1	1	1
$x \in B$	0	0	1	1	0	0	1	1
$x \in C$	0	1	0	1	0	1	0	1
$x \in B \cup C$	0	1	1	1	0	1	1	1
$x \in A \cap (B \cup C)$	0	0	0	0	0	1	1	1
$x \in A \cap B$	0	0	0	0	0	0	1	1
$x \in A \cap C$	0	0	0	0	0	1	0	1
$x \in (A \cap B) \cup (A \cap C)$	0	0	0	0	0	1	1	1

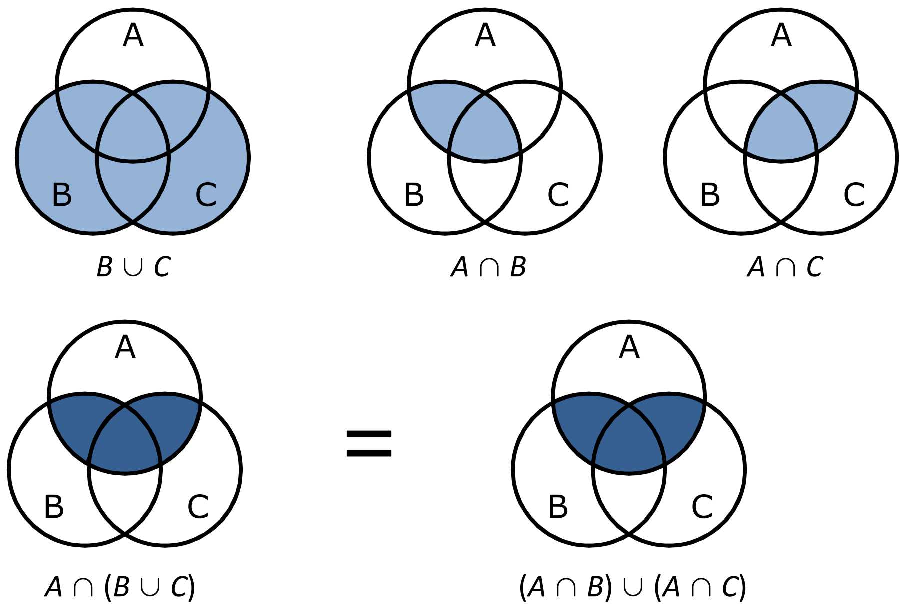
Beweis von Mengengleichungen: Fallunterscheidung im Venn-Diagramm



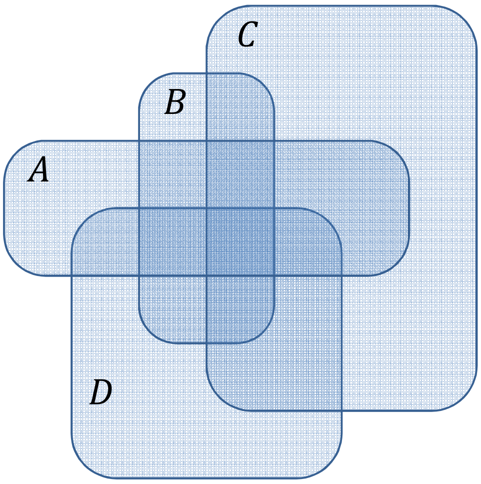
Bodo Pareigis
Lineare Algebra für Informatiker,
Springer, Berlin, 2000:

Man stellt sich Mengen oft als Teilmengen der Ebene, eingegrenzt durch Kurven, vor. Diese Vorstellung hilft, Beweise für die genannten Rechenregeln zu finden. Sie ersetzt aber nicht einen exakten Beweis.

Beweis (?) von Mengengleichungen mit Venn-Diagramm



Venn-Diagramm für 4 Mengen



Erweiterung von Element-Operationen auf Mengen

Ist $\otimes$ eine zweistellige Operation auf Elementen,
so kann diese auf Mengen ausgedehnt werden:

$A \otimes B = \{a \otimes b \mid a \in A \wedge b \in B\}$

Beispiele

$\{1,2,3\} + \{2,3,4\} = \{3,4,5,6,7\}$
$\mathbb{N} + \mathbb{N} = \mathbb{N} \setminus \{1\}$
$\mathbb{Z} / \mathbb{N} = \mathbb{Q}$
$\mathbb{N} - \mathbb{N} = \mathbb{Z}$

Auch andere Operationen
lassen sich analog erweitern.

Beispiele

$\sqrt{\{1,4,9\}} = \{1,2,3\}$
$3 \cdot \mathbb{N} = \{3,6,9,12, \ldots\}$

Abschluss unter einer Operation

Eine Menge A heißt *abgeschlossen*
unter einer zweistelligen Operation ⊗,
falls für alle $a, b \in A$ gilt: $a \otimes b \in A$.

$\mathbb{N}$ unter + ?
$\mathbb{N}$ unter − ?
$\mathbb{Z}$ unter + ?
$\mathbb{Z}$ unter − ?

Der *Abschluss* einer Menge A
unter einer zweistelligen Operation ⊗
ist die kleinste Menge,
die A umfasst und *abgeschlossen* unter ⊗ ist.

Abschluss von
$\mathbb{N}$ unter − ?