Diskrete Strukturen in der Informatik

Logik & Naive Mengenlehre

PD Dr. Stefan Milius

WS 2015/2016

Überblick

Inhalt

Vorlesungsziele

dieses Kapitel

1. Basiswissen Prädikatenlogik
2. Einführung Mengen
3. Grundoperationen mit Mengen

Bitte Fragen direkt stellen!

Grundlagen der Logik

Aussagenlogik

Inhalt

Aussagenlogik – Notation

Wiederholung

$\neg$	Negation	nicht
$\wedge$	Konjunktion	und
$\vee$	Disjunktion	oder
$\rightarrow$	Implikation	wenn . . . , dann . . .
$\leftrightarrow$	Äquivalenz	genau dann wenn

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Aussagenlogik — Tautologien

§1.13 Definition

Eine Formel ist

- eine Tautologie, falls sie immer wahr ist
  (unabh. von der Belegung der Atome)
- unerfüllbar, falls sie immer falsch ist
  (unabh. von der Belegung der Atome)
- erfüllbar, falls sie nicht unerfüllbar ist

Beispiel

- $(A \wedge A) \leftrightarrow A$ ist eine Tautologie (Idem. $\wedge$)
- Gerade $\leftrightarrow \neg$Ungerade ist erfüllbar, aber keine Tautologie
  (auch wenn diese Aussage mit Fachwissen immer wahr ist)

Aussagenlogik — Tautologien

klassische Tautologien	Bezeichnung
$A \vee \neg A$	ausgeschlossenes Drittes
$((A \vee B) \wedge (A \to C) \wedge (B \to C)) \to C$	Fallunterscheidung
$(A \wedge (A \to B)) \to B$	*modus ponens*
$((A \to B) \wedge (B \to C)) \to (A \to C)$	Syllogismus (Transitivität von $\to$)
$(A \to B) \leftrightarrow (\neg B \to \neg A)$	Kontraposition
$((A \to B) \wedge (A \to \neg B)) \to \neg A$	*reductio ad absurdum* (indirekter Beweis)
$(A \wedge B) \to A$	Abschwächung für $\wedge$
$A \to (A \vee B)$	Abschwächung für $\vee$
$A \leftrightarrow B$	für äquivalente Aussagen A und B

Aussagenlogik – Schlusskette

Theorem (§1.14 – modus ponens)

$F = (A \wedge (A \to B)) \to B$ ist eine Tautologie.

(gelten A und "wenn A, dann B", dann gilt auch B)

Beweis.

Mit Fallunterscheidung:

- falls B wahr ist, dann ist $F = \cdots \to B$ wahr
- falls B falsch ist, dann ist entweder
  - A wahr, womit $A \wedge (A \to B)$ falsch ist
  - A falsch, womit $A \wedge (A \to B)$ auch falsch ist

  Da $F' = A \wedge (A \to B)$ falsch ist, ist $F = F' \to B$ wahr $\square$

Aussagenlogik – Schlusskette

Theorem (§1.15)

$((A \to B) \wedge (B \to C)) \to (A \to C)$ ist eine Tautologie.

(Transitivität von $\to$)

Beweis.

Kontraposition: $F = \neg(A \to C) \to \underbrace{\neg((A \to B) \wedge (B \to C))}_{F'}$

Fallunterscheidung:

- Falls $\neg(A \to C)$ falsch ist, dann ist F wahr.
- Falls $\neg(A \to C)$ wahr ist, dann ist $A \to C$ falsch, woraus A wahr und C falsch folgen
  - Sei B falsch. Dann ist $A \to B$ falsch und damit F' wahr
  - Sei B wahr. Dann ist $B \to C$ falsch und damit F' wahr

  Da F' wahr ist, ist auch F wahr □

Aussagenlogik – Indirekter Beweis

§2.1 Theorem (indirekter Beweis)

$\underbrace{((A \to B) \wedge (A \to \neg B))}_{F'} \to \neg A$ ist eine Tautologie.

in Worten: wenn man aus A einen Widerspruch ableiten kann, dann kann A nicht gelten

Beweis.

Wahrheitswertetabelle:

A	B	$A \to B$	$\neg B$	$A \to \neg B$	F'	$\neg A$	$F' \to \neg A$
0	0	1	1	1	1	1	1
0	1	1	0	1	1	1	1
1	0	0	1	1	0	0	1
1	1	1	0	0	0	0	1

Offensichtlich gilt sogar $F' \leftrightarrow \neg A$ □

Aussagenlogik – Indirekter Beweis

§2.2 Theorem

Es gibt keine rationale Zahl x mit $x^2 = 2$.

Beweis (indirekt).

Sei $x \in \mathbb{Q}$, so dass $x^2 = 2$. Negation der Aussage

Dann existieren teilerfremde $m, n \in \mathbb{Z}$ mit $n \neq 0$, so dass $x = \frac{m}{n}$.

Also $2n^2 = m^2$, womit m^2 gerade ist. Gemäß §1.12 (aus der letzten VL) ist somit auch m gerade, so dass $m = 2k$ mit $k \in \mathbb{Z}$.

$$2n^2 = m^2 = (2k)^2 = 4k^2 \qquad \Rightarrow \qquad n^2 = 2k^2$$

Also ist auch n^2 gerade und damit ist n gerade gemäß §1.12.

Da m und n gerade sind, sind sie nicht teilerfremd (gemeinsamer Teiler 2). Folglich gilt das Theorem. □

Aussagenlogik – Indirekter Beweis

Theorem (§2.2)

$\underbrace{\text{Es gibt keine rationale Zahl } x \text{ mit } x^2 = 2.}_{\neg A}$

Beweisstruktur.

$\underbrace{\text{Es existieren teilerfremde } m, n \in \mathbb{Z} \text{ mit } n \neq 0 \text{ und } (\frac{m}{n})^2 = 2}_{B}$

Wir zeigten zunächst $A \to B$ und danach $\neg B$

Damit gilt auch $A \to \neg B$, da $\neg B$ wahr ist.

Wir haben also $A \to B$ und $A \to \neg B$ gezeigt. Folglich gilt $\neg A$ gemäß §2.1. □

Aussagenlogik – Indirekter Beweis

Notizen

- äquivalent: $(A \to (B \wedge \neg B)) \to \neg A$
- anstatt $B \wedge \neg B$ kann jede unerfüllbare Aussage stehen
- indirekte Beweise sind nicht konstruktiv;
  sie zeigen nur Widerspruch auf

$\to$ lieber *direkt* als *indirekt* beweisen

Prädikatenlogik

Prädikatenlogik – Motivation

Theorem (§1.12)

Sei $n \in \mathbb{Z}$ beliebig. Falls n^2 gerade ist, so ist auch n gerade.

Probleme

- dies ist natürlich eine Aussage,
  aber deren interne Struktur können wir nicht modellieren
- die Abhängigkeit von n können wir nicht modellieren
  QuadratGerade = "n^2 gerade" und ZahlGerade = "n gerade"
  für eine Konstante n

  $\rightarrow$ Aussagenschablonen
- auch die beliebige Wahl von n können wir nicht modellieren

  $\rightarrow$ Quantoren

Prädikatenlogik – Motivation

Intuition

- eine Aussagenschablone ist ein Satz, der Variablen verwendet, so dass für jede Belegung der Variablen eine Aussage entsteht
- Quantoren verlangen Wahrheit der Aussagen für alle oder für eine der Instanziierungen einer Aussagenschablone

Formalisierung von §1.12

Sei $n \in \mathbb{Z}$ beliebig. Falls n^2 gerade ist, so ist auch n gerade.

$$(\forall n \in \mathbb{Z}).\Big(\text{QuadratGerade}(n) \rightarrow \text{ZahlGerade}(n)\Big)$$

Prädikatenlogik – Grundbegriffe

§2.3 Begriffe

- Variablen (üblicherweise kleingeschrieben)
  können als Parameter von Prädikaten auftreten
- Prädikat – Aussagenschablone
  bildet zusammen mit Variablen als Parameter ein Atom

Beispiele

- Atom: ZahlGerade(n) Wahrheit hängt nun von n ab
  - Prädikat: ZahlGerade ZahlGerade(2) ist wahr
  - Variable: n ZahlGerade(3) ist falsch
- Atom: Summe(x, y, z)
  - Prädikat: Summe Summe(x, y, z) wahr
  - Variablen: x, y, z gdw. $x + y = z$

Prädikatenlogik – Grundbegriffe

Notizen

- die bekannten Junktoren $\vee, \wedge, \neg, \rightarrow, \leftrightarrow$
  können weiterhin verwendet werden
  (auch zur Verknüpfung von Aussagenschablonen)
- die Wahrheit einer Aussagenschablone lässt sich erst bei Kenntnis der Belegung der Variablen bestimmen

$\rightarrow$ Mechanismus für Umwandlung Aussagenschablone in Aussage

Prädikatenlogik – Quantoren

§2.4 Quantoren

Sei F eine prädikatenlogische Formel.

- $(\forall x \in X).F$ ist eine Formel, die wahr ist, gdw. F für alle $x \in X$ wahr ist

  $\forall$A = für Alle
  Allquantor

- $(\exists x \in X).F$ ist eine Formel, die wahr ist, gdw. $x \in X$ existiert, so dass F für dieses x wahr ist

  $\exists$E = Existiert ein
  Existenzquantor

Durch Quantifizierung aller Variablen erhält man eine Aussage.

Beispiel (§2.2)

Es gibt keine rationale Zahl x mit $x^2 = 2$.

Formalisierung: $\neg(\exists x \in \mathbb{Q}).(x^2 = 2)$

Prädikatenlogik – Beispiele

weitere Beispiele

- Jede ganze Zahl ist größer 0. falsch

$$(\forall n \in \mathbb{Z}).\text{Größer0}(n) \qquad (\forall n \in \mathbb{Z}).(n > 0)$$

- Jede gerade natürliche Zahl $n > 2$ ist die Summe zweier Primzahlen.
  unbekannt

$$(\forall n \in \mathbb{N}).\Big(\big((n > 2) \wedge \text{ZahlGerade}(n)\big) \rightarrow (\exists i, j \in \mathbb{N}).\big(\text{Prim}(i) \wedge \text{Prim}(j) \wedge (i + j = n)\big)\Big)$$

Prädikatenlogik – komplexe Beispiele

komplexe Beispiele

- Cauchy-Konvergenz einer Folge $(x_i)_{i \in \mathbb{N}}$

$$(\forall \epsilon \in \mathbb{R}_{>0}).(\exists n \in \mathbb{N}).(\forall i \in \mathbb{N}).(\forall j \in \mathbb{N}).$$
$$((i \geq n) \wedge (j \geq n)) \rightarrow (|x_j - x_i| < \epsilon)$$

- Grenzwert $\lim_{i \rightarrow n} f(i)$ einer Funktion $f : \mathbb{R} \rightarrow \mathbb{R}$ ist ℓ gdw.

$$(\forall \epsilon \in \mathbb{R}_{>0}).(\exists \delta \in \mathbb{R}_{>0}).(\forall i \in \mathbb{R}).$$
$$(0 < |i - n| < \delta) \rightarrow (|f(i) - \ell| < \epsilon)$$

Augustin-Louis Cauchy (* 1789; † 1857)

- franz. Mathematiker
- Pionier der Analysis
- Verfechter des formalen Beweises

Prädikatenlogik – Rechenregeln

weitere äquivalente Formeln		Bezeichnung
$\neg(\forall x \in X).F$	$(\exists x \in X).\neg F$	Negation Allquantor
$\neg(\exists x \in X).F$	$(\forall x \in X).\neg F$	Negation Existenzquantor
$\rightarrow$ siehe Übung		

Mengenlehre

Mengenlehre

Inhalt

Mengenlehre – Grundbegriffe

§2.5 Definition (Menge – nach [Cantor, 1895])

Eine Menge ist eine Zusammenfassung von unterscheidbaren Objekten zu einem Ganzen. Die zusammengefassten Objekte heißen Elemente von M.

Original [Cantor, 1895]

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

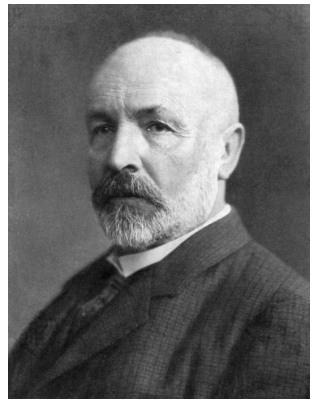
Notiz

verbale Definition $\rightarrow$ naive Mengenlehre

Mengenlehre – Grundbegriffe

Georg Cantor (* 1845; † 1918)

- deutscher Mathematiker
- Begründer der modernen Mengenlehre
- Kardinal- und Ordinalzahlen



§ 1.

Der Mächtigkeitsbegriff oder die Cardinalzahl.

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.

§2.6 Definition (Menge)

- Menge als Zusammenfassung von bestimmten Objekten (ihren Elementen)
- für jede Menge M und jedes Objekt m ist m entweder
  - ein Element von M $m \in M$
  - oder nicht $\neg(m \in M)$ oder besser: $m \notin M$
- "entweder ... oder ..." entspricht exklusivem Oder

$$(A \vee B) \wedge \neg(A \wedge B)$$

- jede Menge ist unterscheidbar von jedem ihrer Elemente

$\{3\} \neq 3$

Mengenlehre – Mengen

Beispiele

- Menge aller Lastkraftwagen

  Definition mit Eigenschaft

- Menge aller Lastkraftwagen,
  die (jetzt) frischen Fisch transportieren

  Einschränkung einer anderen Menge

- Menge mit den Elementen 1, 2 und 3

  (vollständige) Aufzählung

- Menge mit den Elementen 0, 1, 2, usw.

  (unvollständige) Aufzählung

§2.7 Notation zur Definition von Mengen

- Leere Menge: $\emptyset$ hat keine Elemente
- Basismengen: sei Lkw die Menge aller Lastkraftwagen

  textuelle Definition
- Einschränkung: $\{L \in \text{Lkw} \mid \text{hatFisch}(L)\}$
  enthält genau die Elemente L von Lkw,
  für die hatFisch(L) wahr ist

  $M = \{x \in X \mid F\}$ mit Aussagenschablone F
- vollständige Aufzählung: $\{1, 2, 3\}$

  funktioniert nur bei endlichen Mengen
- unvollständige Aufzählung: $\{0, 1, 2, \ldots\}$

  Muster muss klar erkennbar sein

Mengenlehre – Mengen

Notizen

- Elemente unterscheidbar (Mehrfachnennungen unnütz)

$$\{1, 2, 3, 1\} = \{1, 2, 3\} \qquad \text{und} \qquad \left\{0{,}5\right\} = \left\{\frac{1}{2}, \frac{2}{4}, 2 \cdot \frac{6}{24}\right\}$$

- nur Gruppierung; keine Anordnung (Reihenfolge irrelevant)

$$\{3, 2, 1\} = \{1, 2, 3\}$$

- dies gilt allgemein für Mengen, nicht nur für Aufzählungen
- Klassiker: bei $x, y, z \in \{1, 2, 3\}$

  formal: $(x \in \{1, 2, 3\}) \wedge (y \in \{1, 2, 3\}) \wedge (z \in \{1, 2, 3\})$

  kann $x = y = z$ gelten

Mengenlehre – Äquivalenz

§2.8 Definition (Gleichheit)

Mengen M und N sind gleich (Notation: $M = N$),
wenn sie (exakt) die gleichen Elemente haben

Formal: $M = N$ gdw. $(\forall m \in M).(m \in N) \wedge (\forall n \in N).(n \in M)$

Beispiel

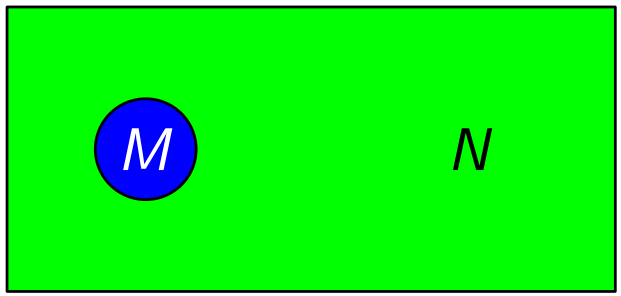
- $M_2 = \{n \in \mathbb{N} \mid n \text{ ist durch 2 teilbar}\}$ nat. Zahlen mit Teiler 2
- $G = \{n \in \mathbb{N} \mid \text{ZahlGerade}(n)\}$ gerade nat. Zahlen
- es gilt $M_2 = G$

Mengenlehre – Teilmenge

§2.9 Definition (Teilmenge)

Menge M ist eine Teilmenge von der Menge N (Notation: $M \subseteq N$), falls jedes Element von M auch Element von N ist

Formal: $M \subseteq N$ gdw. $(\forall m \in M).(m \in N)$



Beispiel

- $M_4 = \{n \in \mathbb{N} \mid n \text{ ist durch 4 teilbar}\}$ nat. Zahlen mit Teiler 4
- $G = \{n \in \mathbb{N} \mid \text{ZahlGerade}(n)\}$ gerade nat. Zahlen
- es gilt $M_4 \subseteq G$

Mengenlehre – Teilmenge

Notizen

- Alternativen zu $M \subseteq N$ (M ist Teilmenge von N):
  - $N \supseteq M$ (N ist Obermenge von M)
  - manchmal auch: $M \subset N$ (werden wir nicht verwenden)
- Was bedeutet: $M \not\subseteq N$?

$$
\begin{aligned}
& M \not\subseteq N \\
\text{gdw.} \quad & \neg(M \subseteq N) \\
\text{gdw.} \quad & \neg(\forall m \in M).(m \in N) \\
\text{gdw.} \quad & (\exists m \in M).\neg(m \in N) \\
\text{gdw.} \quad & (\exists m \in M).(m \notin N)
\end{aligned}
$$

in Worten: $M \not\subseteq N$ gdw. es ein Element m von M gibt, welches kein Element von N ist

Mengenlehre – Zwischenfrage

Fragen

Welche Aussagen gelten für $M = \{\emptyset, \{\emptyset\}\}$?

- $\emptyset \in M$ ✓
- $\{\emptyset\} \in M$ ✓
- $\{\{\emptyset\}\} \in M$ ✗
- $\emptyset \subseteq M$ ✓
- $\{\emptyset\} \subseteq M$ ✓
- $\{\{\emptyset\}\} \subseteq M$ ✓

Mengenlehre – Teilmenge

§2.10 Theorem

Für alle Mengen M und N gilt: $M = N$ gdw. $M \subseteq N$ und $N \subseteq M$.

Beweis.

Direkt durch Einsetzen der Definitionen:

$$
\begin{array}{lll}
 & M = N & \\
\text{gdw.} & (\forall m \in M).(m \in N) \wedge (\forall n \in N).(n \in M) & \S 2.8 \\
\text{gdw.} & (M \subseteq N) \wedge (\forall n \in N).(n \in M) & \S 2.9 \\
\text{gdw.} & (M \subseteq N) \wedge (N \subseteq M) & \S 2.9
\end{array}
$$

□

Mengenlehre – Standardmengen

Beispiele

- $\emptyset = \{\}$ — leere Menge (hat keine Elemente)
- $\mathbb{N} = \{0, 1, 2, \ldots\}$ — natürlichen Zahlen (manchmal auch ohne 0)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ — ganzen Zahlen
- $\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z},\ n \in \mathbb{Z},\ n \neq 0\}$ — rationalen Zahlen (‘,’ heißt “und” in Eigenschaften)
- $\mathbb{R}$ = Menge aller reellen Zahlen — reellen Zahlen

Operationen auf Mengen

Mengenlehre – Grundoperationen

§2.11 Definition (Vereinigung, Schnitt, Differenz)

Seien M und N Mengen.

- Vereinigung $M \cup N$ von M und N besteht aus den Elementen, die Element von M oder Element von N sind

$$M \cup N = \{x \mid x \in M \text{ oder } x \in N\}$$

- Schnitt $M \cap N$ von M und N besteht aus den Elementen, die Element von M und Element von N sind

$$M \cap N = \{x \mid x \in M, x \in N\} = \{x \in M \mid x \in N\}$$

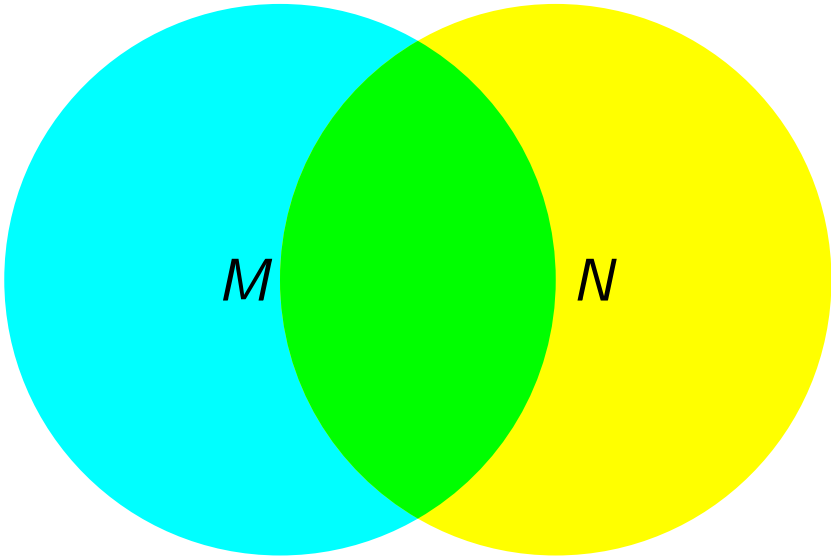
- Differenz $M \setminus N$ von M ohne N besteht aus den Elementen, die Element von M aber nicht Element von N sind

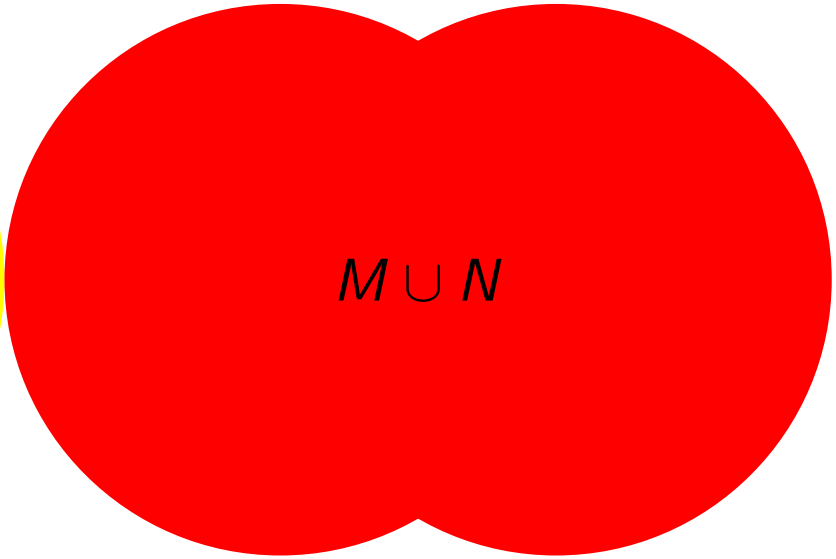
$$M \setminus N = \{x \mid x \in M, x \notin N\} = \{x \in M \mid x \notin N\}$$

Mengenlehre – Grundoperationen

Grafische Darstellung

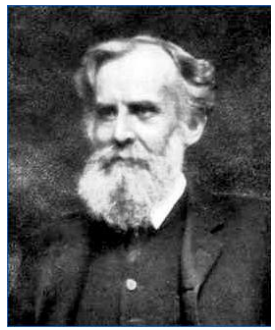
- Venn-Diagramme
- Vereinigung $M \cup N$, Schnitt $M \cap N$, Differenz $M \setminus N$



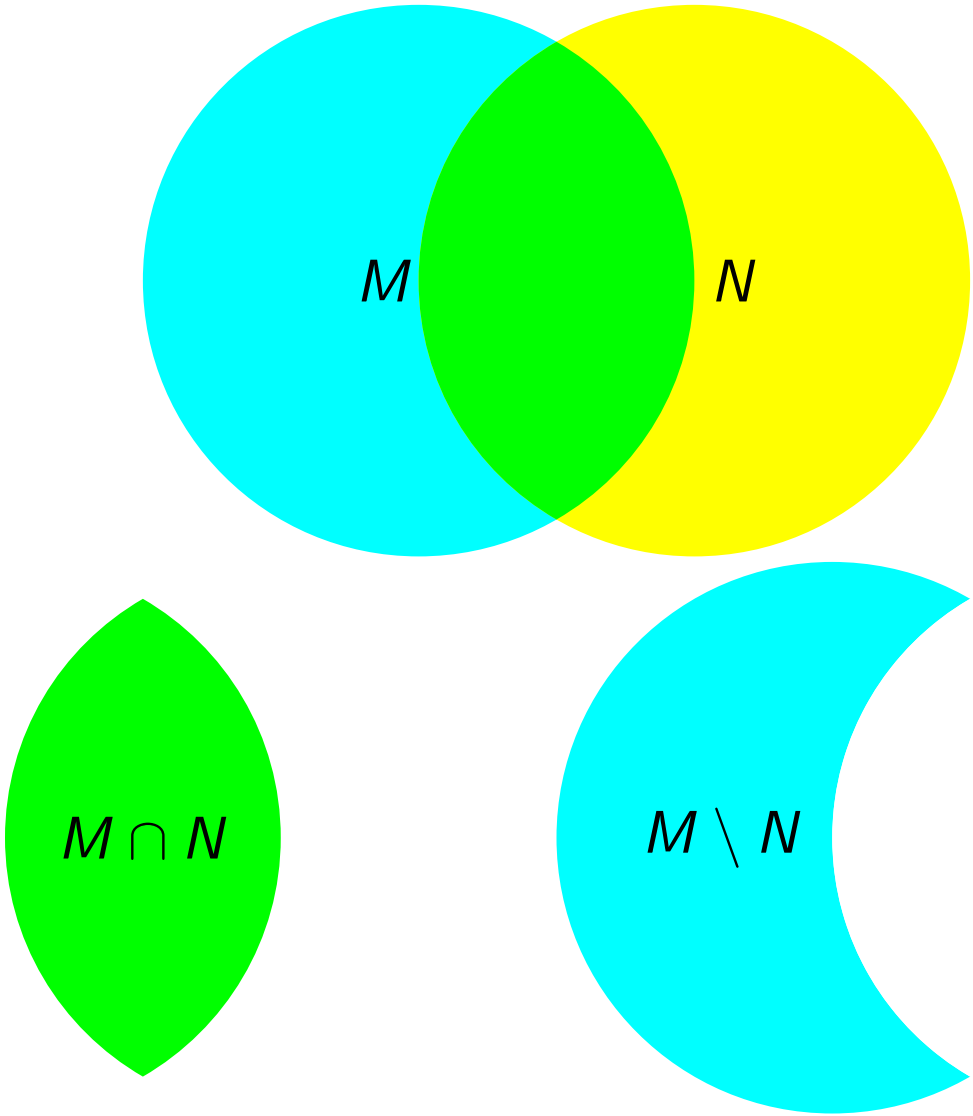


John Venn (* 1834; † 1923)

- engl. Mathematiker
- Lehrer der Logik in Cambridge



Mengenlehre – Grundoperationen



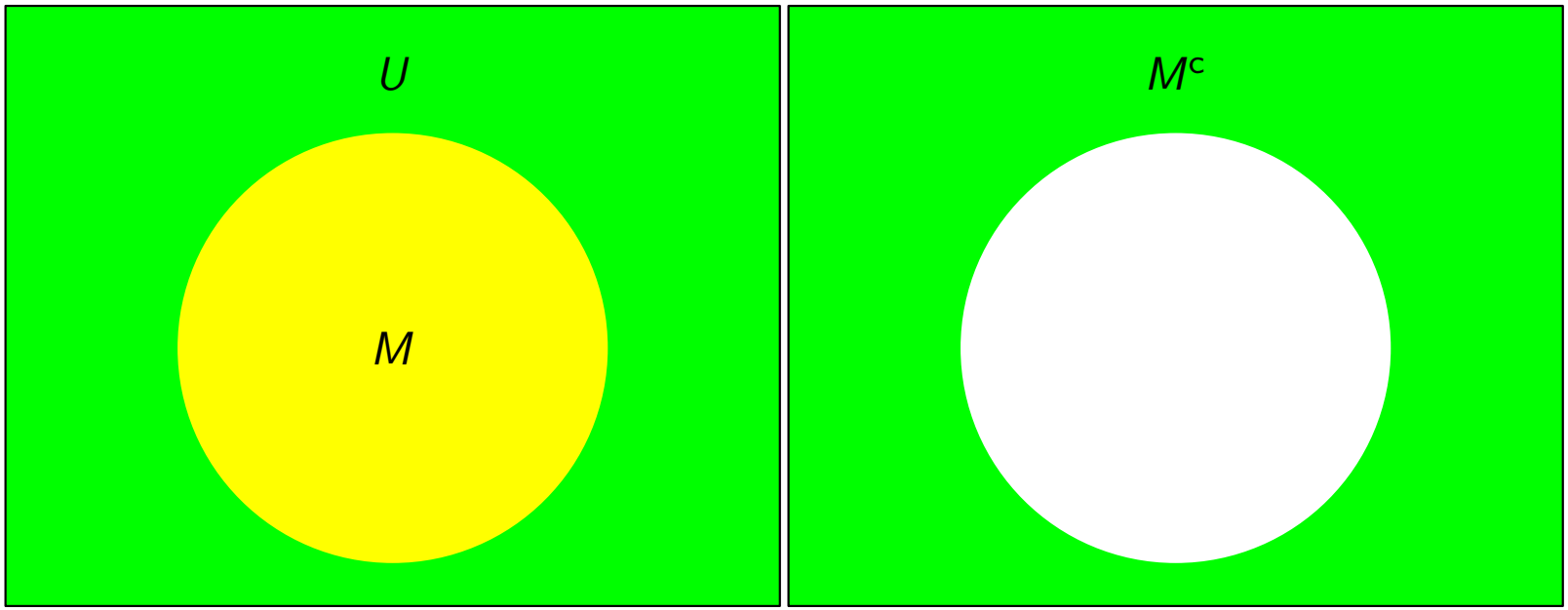
Mengenlehre – Komplement

Grundmenge U sei gegeben (häufig implizit)

§2.12 Definition (Komplement)

Das Komplement M^c von $M \subseteq U$ beinhaltet genau die Elemente von U, die nicht Elemente von M sind.

$$M^c = \{u \in U \mid u \notin M\} = U \setminus M$$



Mengenlehre – Einfache Eigenschaften

§2.13 Theorem

1. $x \in \{y \mid F(y)\}$ gdw. $F(x)$ wahr
2. $x \notin M$ gdw. $x \in M^c$ Grundmenge U und $x \in U$

Beweis.

1. Beidseitige Implikationen
   - $(\leftarrow)$ Falls $F(x)$ gilt, dann auch $x \in \{y \mid F(y)\}$.
   - $(\rightarrow)$ Falls $F(x)$ nicht gilt, dann gilt auch $x \notin \{y \mid F(y)\}$.
     Per Kontraposition gilt daher $F(x)$, falls $x \in \{y \mid F(y)\}$.
2. Beiseitige Implikationen
   - $(\leftarrow)$ Sei $x \in M^c = U \setminus M = \{y \mid y \in U, y \notin M\}$.
     Nach 1 gilt daher $x \in U$ und $x \notin M$.
   - $(\rightarrow)$ Sei $x \in U$ und $x \notin M$.
     Dann gilt nach 1 auch $x \in \{y \mid y \in U, y \notin M\} = U \setminus M = M^c$. □

Mengenlehre – Rechenregeln

gleiche Mengen		Bezeichnung
$A \cap B$	$B \cap A$	Kommutativität von $\cap$
$A \cup B$	$B \cup A$	Kommutativität von $\cup$
$(A \cap B) \cap C$	$A \cap (B \cap C)$	Assoziativität von $\cap$
$(A \cup B) \cup C$	$A \cup (B \cup C)$	Assoziativität von $\cup$
$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$	Distributivität von $\cap$
$A \cup (B \cap C)$	$(A \cup B) \cap (A \cup C)$	Distributivität von $\cup$
$A \cap A$	A	Idempotenz von $\cap$
$A \cup A$	A	Idempotenz von $\cup$
$(A^c)^c$	A	Involution $\cdot^c$
$(A \cap B)^c$	$A^c \cup B^c$	deMorgan-Gesetz für $\cap$
$(A \cup B)^c$	$A^c \cap B^c$	deMorgan-Gesetz für $\cup$

Mengenlehre – Rechenregeln

§2.13 Theorem

Für alle Mengen M, N, P gilt

$$M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$$

Beweis.

Direkt durch Anwendung der Definitionen:

$$\begin{aligned}
M \cup (N \cap P) &= \{x \mid (x \in M) \vee (x \in N \cap P)\} \\
&= \{x \mid (x \in M) \vee (x \in \{y \mid (y \in N) \wedge (y \in P)\})\} \\
&= \{x \mid \underbrace{(x \in M)}_{A} \vee (\underbrace{(x \in N)}_{B} \wedge \underbrace{(x \in P)}_{C})\} && \text{§2.13} \\
&= \{x \mid (\underbrace{(x \in M)}_{A} \vee \underbrace{(x \in N)}_{B}) \wedge (\underbrace{(x \in M)}_{A} \vee \underbrace{(x \in P)}_{C})\} \\
&= \{x \mid (x \in M \cup N) \wedge (x \in M \cup P)\} \\
&= (M \cup N) \cap (M \cup P)
\end{aligned}$$

□

Zusammenfassung

- Grundwissen Prädikatenlogik
- Grundbegriffe Mengenlehre
- Definition von Mengen
- Beziehungen zwischen Mengen (Gleichheit, Teilmengen)
- Operationen und Rechenregeln für Mengen

Zweite Übungsserie erscheint demnächst im OLAT.