Theoretische Informatik
WS 2024/2025

Kapitel 0
Einführung

0.3
Mengenlehre, Aussagenlogik und Prädikatenlogik
(Grundlagen zum Nachschlagen)

Prof. Dr. Robert Preis
Fachbereich Informatik
Fachhochschule Dortmund
Robert.Preis@fh-dortmund.de

Wie beschreiben wir unendlich große Mengen/Sprachen ?

Die Menge

$$L = \{ w \in \{a,b,c\}^* \mid w = avc \wedge v \in \{a,b,c\}^* \}$$

ist unendlich groß, so dass wir sie nicht aufzählen, sondern die Wörter über deren Eigenschaften definieren:

- $w \in \{a,b,c\}^*$ Alle Wörter w, die aus a, b und c gebildet werden können…
- $\mid$ … mit der Eigenschaft, dass…
- $w=avc$ … w muss als avc geschrieben werden können …
- $\wedge$ … und …
- $v \in \{a,b,c\}^*$ … v ist selbst irgendein Wort gebildet aus a, b oder c.

Für die Beschreibung der Eigenschaften verwenden wir Elemente aus der

1. Mengenlehre (Durchschnitt, Vereinigung, Komplement, …)
2. **Aussagenlogik** (u.a. Junktoren, z.B. $\wedge$)
3. **<u>Prädikatenlogik</u>** (u.a. Prädikate, Variablen und Quantoren)

Definitionen Mengenlehre

Mit einer Menge kann man mehrere (auch unterschiedliche) Elemente zusammenfassen, z.B.

- {1, 2, 3}
- {rot, blau, grün, gelb}
- {1, gelb, Euro, 3.1415926, „Wer hilft mir?“}

Eine Menge kann leer sein: {} oder Ø

Eine Menge kann aus Mengen bestehen: {{1, 2, 3}, {rot, blau, grün, gelb}, {1, gelb, Euro, 3.1415926, „Wer hilft mir?“}}

Besonderheiten:

- die Elemente sind ungeordnet,
  d.h. {1, 2, 3} = {3, 2, 1}
- die Menge betrachtet keine Mehrfachheiten (bzw. zählen nur einmal),
  d.h. {1, 3, 2, 2, 1, 1, 2} = {1, 2, 3}

Bekannte Zahlenmengen

- Menge der natürlichen Zahlen

  $\mathbf{N_+} = \{1, 2, 3, \ldots\}$
- Menge der nichtnegativen ganzen Zahlen

  $\mathbf{N_0} = \{0, 1, 2, 3, \ldots\}$
- Menge der ganzen Zahlen

  $\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- Menge der rationalen Zahlen

  Q = {zusätzlich Brüche von Zahlen aus Z}
- Menge der reellen Zahlen

  R = {zusätzlich π, e, …}
- Menge der komplexen Zahlen

  C = {zusätzlich imaginäre Zahl i}

Es gilt:

$$\mathbf{N_+} \subset \mathbf{N_0} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

Notationen

- Anzahl der (verschiedenen) Elemente einer Menge (Kardinalität): $|A|$
  - $|\{1,2,3\}|=3$
- Mengenzugehörigkeit oder Nicht-Zugehörigkeit: $x \in Z$, $x \notin Z$
  - $2 \in \{1,2,3\}$, $4 \notin \{1,2,3\}$
- Teilmenge $A \subseteq B$: A ist eine Teilmenge von B wenn alle Elemente aus A auch in B sind (für alle $x \in A$ gilt $x \in B$)
  - $\{1,2\} \subseteq \{1,2,3\}$, $\{1,2,3\} \subseteq \{1,2,3\}$
- Echte Teilmenge $A \subset B$: A ist eine echte Teilmenge von B wenn $A \subseteq B$ und es zusätzlich ein Element in B gibt, das nicht in A ist ($y \in B$ mit $y \notin A$)
  - $\{1,2\} \subset \{1,2,3\}$
- Die leere Menge ist Teilmenge jeder Menge.
  - $\{\} \subseteq \{1,2,3\}$
- Mengengleichheit $A=B$: wenn $A \subseteq B$ und $B \subseteq A$
  - Aus $\{1,2,3\} \subseteq \{3,2,1\}$ und $\{3,2,1\} \subseteq \{1,2,3\}$ folgt $\{1,2,3\} = \{3,2,1\}$

Potenzmenge

Die Menge aller Teilmengen nennt man Potenzmenge. Es ist eine Menge von Mengen.

- A = {1,2,3}

  P(A) = { {}, — 0-elementig
  {1}, {2}, {3}, — 1-elementig
  {1,2}, {1,3}, {2,3}, — 2-elementig
  {1,2,3} } — 3-elementig

- B = {{},{a,3},5}

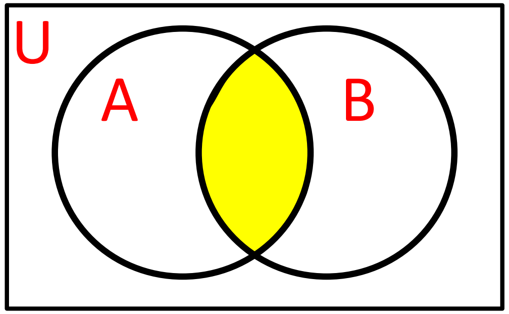
  P(B) = { {}, — 0-elementig
  {{}}, {{a,3}}, {5}, — 1-elementig
  {{},{a,3}}, {{},5}, {{a,3},5}, — 2-elementig
  {{},{a,3},5} } — 3-elementig

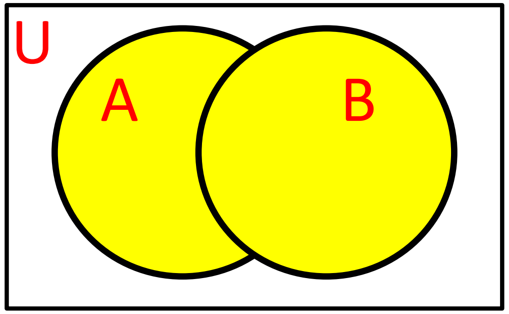
Die Kardinalität der Potenzmenge *P*(A) mit $|A|=n$ ist $|P(A)| = 2^{|A|} = 2^n$.

Wie viele n-elementige Teilmengen gibt es? Pascal'sches Dreieck !

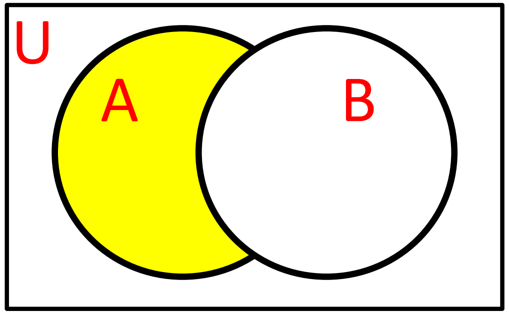
Mengenoperationen

- Schnittmenge
  $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$

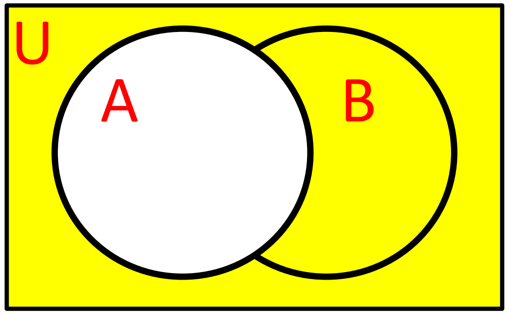




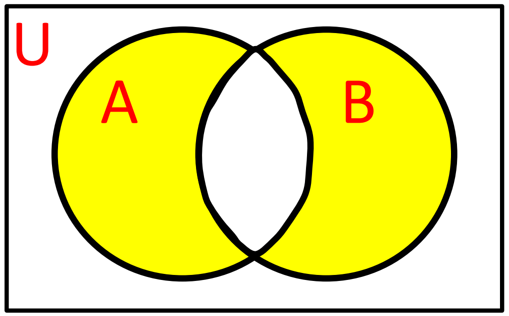
- Vereinigung
  $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$



- Mengendifferenz
  $A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}$



- Komplement bezüglich einer zugehörigen Grundmenge U (das Universum)
  $A^c = \{x \in U \mid x \notin A\} = U \setminus A$



- Symmetrische Differenz (in genau einer der beiden Mengen) $A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B \cup B \setminus A)$

Gesetze der Mengenlehre

Doppeltes Komplement	$(A^c)^c = A$	
Idempotenzgesetz	$A \cap A = A$	$A \cup A = A$
Inverses Element	$A^c \cap A = A \cap A^c = \emptyset$	$A^c \cup A = A \cup A^c = U$
Neutrales Element	$U \cap A = A \cap U = A$	$\emptyset \cup A = A \cup \emptyset = A$
Auslöschendes Elem.	$\emptyset \cap A = A \cap \emptyset = \emptyset$	$U \cup A = A \cup U = U$
Kommutativgesetz	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Assoziativgesetz	$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$
Distributivgesetz	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	

Absorptionsgesetz

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

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

De Morgan Gesetz	$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$	$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$
oder auch	$(A \cap B)^c = A^c \cup B^c$	$(A \cup B)^c = A^c \cap B^c$

Vereinfachung von Mengen durch Gesetze

Kann ich die Menge auch einfacher darstellen?

$$(A \cap B^c)^c \cap ((A^c \cap B)^c \cup (B^c \cap A)^c)$$

$(A \cap B^c)^c \cap ((A^c \cap B)^c \cup (B^c \cap A)^c)$	Kommutativgesetz
$= (A \cap B^c)^c \cap ((A^c \cap B)^c \cup (A \cap B^c)^c)$	Absorptionsgesetz
$= (A \cap B^c)^c$	De Morgan
$= A^c \cup B^{c^c}$	Doppeltes Komplement
$= A^c \cup B$	

Warum gilt das Absorptionsgesetz?

$A \cap (A \cup B)$	Neutrales Element
$= (A \cup \emptyset) \cap (A \cup B)$	Distributivgesetz
$= A \cup (\emptyset \cap B)$	Auslöschendes Element
$= A \cup \emptyset$	Neutrales Element
$= A$	

Geordnete Mengen (Tupel)

Eine Menge, in der n Elemente $x_1, \ldots, x_n$ geordnet sind, heißt n-Tupel und wird mit runden Klammern

$(x_1, \ldots, x_n)$ z.B. (3, 1, 17, 4, 3)

aufgeführt.

- Die einzelnen Elemente heißen Komponenten bzw. i-te Komponente.
- Die Elemente sind geordnet, d.h. $(1,2,3) \neq (3,2,1)$.
- Zwei Tupel a und b der Länge n sind gleich, wenn alle ihre Komponenten paarweise gleich sind, d.h. falls für alle $i \in \{1, \ldots, n\}$: $a_i = b_i$.
  $(1,2,3) = (1,2,3)$
- Mehrfachheiten sind wichtig:
  $(1, 2, 3, 2, 1) \neq (1, 1, 2, 2, 3) \neq (1, 2, 3)$

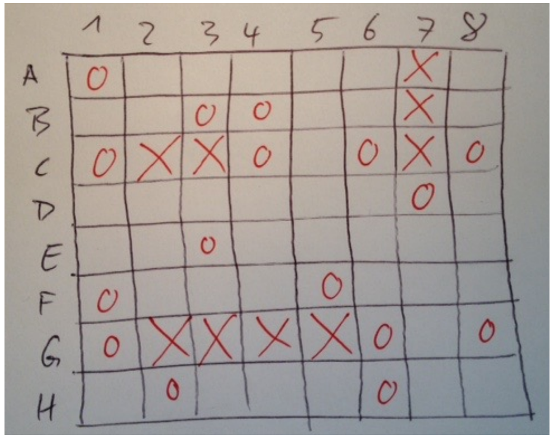
Beispiele:

- Ein Tupel:
  (Robert, Preis, Professor, robert.preis@fh-dortmund.de)
- Eine Menge von Tupel:
  {(Volvo, XC90, 200PS, 2012), (Mini, Mayfair Chrom, 55PS, 1994)}

Kartesisches Produkt

Für zwei Mengen A und B ist die Menge aller geordneten Paare (x, y) mit $x \in A$ und $y \in B$ das kartesische Produkt (Kreuzprodukt, Mengenprodukt)

$$A \times B = \{(x,y) \mid x \in A,\ y \in B\}.$$



- $\{1,2\} \times \{1,a,X\} = \{(1,1), (1,a), (1,X), (2,1), (2,a), (2,X)\}$
- Dies ist ungleich dem kartesischen Produkt
  $\{1,a,X\} \times \{1,2\} = \{(1,1), (1,2), (a,1), (a,2), (X,1), (X,2)\}$
- Schiffeversenken:
  $\{A,B,C,D,E,F,G,H,I,J\} \times \{1,2,3,4,5,6,7,8,9,10\}$
  $= \{(A,1), (A,2), (A,3), \ldots (J,10)\}$
- Kardinalität des kartesischen Produktes: $|A \times B| = |A| * |B|$
- Für $A \times A$ schreibt man auch A^2.
- Das kartesische Koordinatensystem bildet den $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ ab.
- Kartesisches Produkt auch in mehreren Dimensionen:
  $\{1,2,3\} \times \{a,b,c\} \times \{I,II\} = \{(1,a,I), (1,a,II), (1,b,I), (1,b,II), (1,c,I), (1,c,II),$
  $(2,a,I), (2,a,II), (2,b,I), (2,b,II), (2,c,I), (2,c,II),$
  $(3,a,I), (3,a,II), (3,b,I), (3,b,II), (3,c,I), (3,c,II)\}$

Aussagenlogik

Beispiele für Aussagen:

- *„2 ist eine gerade Zahl"* ist eine wahre Aussage
- *„4 ist eine Primzahl"* ist eine falsche Aussage (aber trotzdem eine Aussage!)
- *„Wie alt sind Sie?"* ist keine Aussage

Definition:

Eine Aussage ist ein Satz einer menschlichen oder künstlichen Sprache, dem eindeutig einer der beiden Wahrheitswerte wahr oder falsch zugeordnet werden kann.

- Logische Aussagen können nur wahr (w) oder falsch (f) sein, d.h. für eine Aussage x gilt $x \in \{f, w\}$.
- In technischen Bereichen wird oft f=0 und w=1 kodiert.
- Aussagen oder Verknüpfungen von Aussagen nennt man Ausdrücke.
- *„Ich sage jetzt nicht die Wahrheit."* ist keine Aussage !

Logische Verknüpfungen

x	y	¬x	¬y	x∧y	x∨y	x⊕y	x↔y	x⇒y	x|y	x↓y
f	f	w	w	f	f	f	w	w	w	w
f	w	w	f	f	w	w	f	w	w	f
w	f	f	w	f	w	w	f	f	w	f
w	w	f	f	w	w	f	w	w	f	f

Verknüpfung	**Notation**	**Sprechweise**
Verneinung, Negation	¬x; !x; $\overline{x}$	*Nicht x*
Konjunktion, UND	∧, *	*x und y*
Disjunktion, ODER	∨, +	*x oder y*
Exklusives ODER	⊕, XOR	*x exklusiv oder y*
Äquivalenz	↔	*x genau dann wenn y*
Implikation	→	*wenn x dann y*
Sheffer Operator, NAND:	|, ¬∧	*x NAND y*
Peirce Operator, NOR	↓, ¬∨	*x NOR y*

Bindungsstärke bei Verknüpfungen

Ist $\neg w \rightarrow f \leftrightarrow w \vee f \wedge f$ wahr oder falsch?

Reihenfolge zur Priorisierung von aussagenlogischen Verknüpfungen:

$(\,)\qquad \neg \qquad \wedge \qquad \vee \qquad \rightarrow \qquad \leftrightarrow$

Von Links nach Rechts:

$\neg w \rightarrow f \leftrightarrow w \vee f \wedge f$

$\approx f \rightarrow f \leftrightarrow w \vee f \wedge f$

$\approx w \leftrightarrow w \vee f \wedge f$

$\approx w \vee f \wedge f$

$\approx w \wedge f$

$\approx f$

Mit Beachtung der Priorisierung:

$((\neg w) \rightarrow f) \leftrightarrow (w \vee (f \wedge f))$

$\approx (f \rightarrow f) \leftrightarrow (w \vee (f \wedge f))$

$\approx w \leftrightarrow (w \vee (f \wedge f))$

$\approx w \leftrightarrow (w \vee f)$

$\approx w \leftrightarrow w$

$\approx w$

Definition: Zwei aussagenlogische Formeln α und β heißen **(semantisch) äquivalent** g.d.w. $\alpha \leftrightarrow \beta$ allgemeingültig ist. Wir schreiben $\alpha \approx \beta$.

Wahrheitstafeln für komplexe Aussagen

Ist $(x \rightarrow y) \wedge (x \vee y)$ *wahr oder falsch?*

...das kommt darauf an, wie x und y sind!

Besser: Für welche Werte von x und y ist der Ausdruck wahr bzw. falsch?

Lösung: Herleitung über Hilfsspalten bis hin zur Gesamtspalte:

x	y	$x \rightarrow y$	$x \vee y$	$(x \rightarrow y) \wedge (x \vee y)$
f	f	w	f	f
f	w	w	w	w
w	f	f	w	f
w	w	w	w	w

Aufwand: Bei einem Ausdruck mit n Variablen und m Operationen gibt es 2^n Belegungen (Zeilen) und m neue Teilausdrücke (Spalten).

Erfüllbarkeitsproblem (Satisfiability/SAT)

Gibt es mindestens eine Belegung von x, y, und z, so dass

$$(x \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (x \vee \neg y \vee z) \wedge (x \vee y) \wedge (\neg y \vee \neg z)$$

wahr ist?

Das Erfüllbarkeitsproblem der Aussagenlogik:

Gibt es für einen beliebigen logischen Ausdruck eine Belegung, so dass der Ausdruck wahr wird, d.h. gibt es mindestens ein w in der Spalte?

- Hört sich einfach an, denn man kann es mit Wahrheitstafeln lösen!
- Aber bei n Variablen gibt es 2^n Belegungen und im schlimmsten Fall muss man alle ausrechnen! ….geht das auch schneller?
- Problem der Komplexitätstheorie, es in effizienter (polynomieller) Zeit zu schaffen (NP-vollständiges Problem).
- 1,000,000 US$ Preisgeld für die Lösung vom Clay Mathematics Institut.
- …der Ruhm wäre mindestens so hoch wie beim Nobelpreis !

Äquivalenzbeweise

Sind die Aussagen $x \rightarrow y$ und $\neg x \vee y$ immer gleich, egal was x und y sind?

Anders gefragt:

- *Sind die Spalten von $x \rightarrow y$ und $\neg x \vee y$ gleich?*

Anders gefragt:

- *Besteht die Spalte $x \rightarrow y \Leftrightarrow \neg x \vee y$ nur aus w?*

x	y	$x \rightarrow y$	$\neg x$	$\neg x \vee y$	$x \rightarrow y \leftrightarrow \neg x \vee y$
f	f	w	w	w	w
f	w	w	w	w	w
w	f	f	f	f	w
w	w	w	f	w	w

Tautologie

Für welche Belegungen von x und y wird der Ausdruck

$$x \rightarrow y \vee \neg y$$

wahr ?

x	y	¬y	y ∨ ¬y	x → y ∨ ¬y
f	f	w	w	w
f	w	f	w	w
w	f	w	w	w
w	w	f	w	w

Eine Tautologie ist ein logischer Ausdruck, der für alle Belegungen wahr ist.

„Wenn der Hahn kräht auf dem Mist,

ändert sich das Wetter oder es bleibt wie es ist.“

Die Aussage lautet formal

$$x \rightarrow y \vee \neg y$$

mit x= „der Hahn kräht auf dem Mist“ und y=„das Wetter ändert sich“.

Größe der Wahrheitstafel: alle Funktionen mit zwei Variablen

Wie viele mögliche Belegungen und Funktionen gibt es bei n Variablen?

- Bei 2 Variablen gibt es 2^2=4 Belegungen und $2^{(2^2)}$=16 Funktionen.

x	y	f	$x \wedge y$		x		y	$x \oplus y$	$x \vee y$	$x \downarrow y$	$x \leftrightarrow y$	$\neg y$	$y \rightarrow x$	$\neg x$	$x \rightarrow y$	$x \mid y$	w
f	f	f	f	f	f	f	f	f	f	w	w	w	w	w	w	w	w
f	w	f	f	f	f	w	w	w	w	f	f	f	f	w	w	w	w
w	f	f	f	w	w	f	f	w	w	f	f	w	w	f	f	w	w
w	w	f	w	f	w	f	w	f	w	f	w	f	w	f	w	f	w
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

- Bei 3 Variablen gibt es 2^3=8 Belegungen und $2^{(2^3)}=2^8$=256 Funktionen.
- Bei n Variablen gibt es 2^n Belegungen und $2^{(2^n)}$ mögliche Funktionen.

Müssen alle möglichen Funktionen in Hardware realisiert werden?

Suche nach Ausdruck und Funktionale Vollständigkeit

Wenn ich eine Spalte habe, welcher Ausdruck passt dazu?

x	y	???		
f	f	w	wahr, wenn x falsch und y falsch, d.h.:	$\neg x \wedge \neg y$
f	w	f		
w	f	w	wahr, wenn x wahr und y falsch, d.h.:	$x \wedge \neg y$
w	w	w	wahr, wenn x wahr und y wahr, d.h. :	$x \wedge y$

1. In jeder „w"-Zeile bilde Konjunktion von Variablen, damit Zeile wahr wird.
2. Bilde Disjunktion dieser Konjunktionen.

Lösung: $(\neg x \wedge \neg y) \vee (x \wedge \neg y) \vee (x \wedge y)$

Für die Realisierung aller logischer Verknüpfungsmöglichkeiten sind die Verknüpfungen ¬, ^ und ˅ ausreichend (funktionale Vollständigkeit).

Geht das eventuell auch mit nur zwei Verknüpfungen? Oder nur einer?

Logikgesetze

Doppelte Verneinung	$\neg(\neg x) \approx x$	
Idempotenzgesetz	$x \wedge x \approx x$	$x \vee x \approx x$
Inverses Element	$\neg x \wedge x \approx x \wedge \neg x \approx f$	$\neg x \vee x \approx x \vee \neg x \approx w$
Neutrales Element	$w \wedge x \approx x \wedge w \approx x$	$f \vee x \approx x \vee f \approx x$
Auslöschendes Elem.	$f \wedge x \approx x \wedge f \approx f$	$w \vee x \approx x \vee w \approx w$
Kommutativgesetz	$x \wedge y \approx y \wedge x$	$x \vee y \approx y \vee x$
	(wichtig z.B. bei Schleifenauswertungen !)	
Assoziativgesetz	$x \wedge (y \wedge z) \approx (x \wedge y) \wedge z$	$x \vee (y \vee z) \approx (x \vee y) \vee z$
Distributivgesetz	$x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z)$	$x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z)$
Absorptionsgesetz	$x \wedge (x \vee y) \approx x \wedge (y \vee x) \approx (x \vee y) \wedge x \approx (y \vee x) \wedge x \approx x$	
	$x \vee (x \wedge y) \approx x \vee (y \wedge x) \approx (x \wedge y) \vee x \approx (y \wedge x) \vee x \approx x$	
De Morgan Gesetz	$\neg(x \wedge y) \approx (\neg x) \vee (\neg y)$	$\neg(x \vee y) \approx (\neg x) \wedge (\neg y)$

Algebraische Äquivalenzbeweise: Vereinfachen von Ausdrücken

Beweis der Äquivalenz von logischen Ausdrücken mit Wahrheitstabellen wird sehr schnell aufwändig (Anzahl Belegungen für n Variablen 2^n).

Als Alternative kann man die logischen Gesetze verwenden.

Gilt für alle x, y, z $\in \{f,w\}$

$$x \wedge (y \vee z) \approx ((\neg\neg x \wedge x) \wedge y) \vee (x \wedge \neg(\neg x \wedge \neg z) \wedge z)\ ?$$

	$((\neg\neg x \wedge x) \wedge y) \vee (x \wedge \neg (\neg x \wedge \neg z) \wedge z)$	De Morgan
$\approx$	$((\neg\neg x \wedge x) \wedge y) \vee (x \wedge (\neg\neg x \vee \neg\neg z) \wedge z)$	3 x Doppelte Verneinung
$\approx$	$((x \wedge x) \wedge y) \vee (x \wedge (x \vee z) \wedge z)$	Idempotenz
$\approx$	$(x \wedge y) \vee (x \wedge (x \vee z) \wedge z)$	Absorptionsgesetz
$\approx$	$(x \wedge y) \vee (x \wedge z)$	Distributivgesetz
$\approx$	$x \wedge (y \vee z)$	

Prädikatenlogik: Erste Beispiele

Für jede natürliche Zahl a gibt es eine natürliche Zahl b, die größer als a ist:

$$\forall a \in \mathbf{N}_+ \ \exists b \in \mathbf{N}_+ : a<b$$

Für alle natürlichen Zahlen a, b, c gilt, dass wenn a kleiner als b ist und b kleiner als c ist, dann ist a kleiner als c:

$$\forall a \in \mathbf{N}_+ \ \forall b \in \mathbf{N}_+ \ \forall c \in \mathbf{N}_+ : (a<b) \wedge (b<c) \rightarrow a<c$$

Prädikatenlogik erweitert Ausdrücke über Aussagen (Aussagenlogik) und Mengen (Mengenlehre) um z.B.

- Variablen wie z.B. a, b, c, …
- Quantoren $\forall$ und $\exists$

Prädikat

Beispiel: Sie kennen Aussagen, die wahr oder falsch sind wie z.B.

„Der Dozent ist ein Professor.“

Ich benutze jetzt die Menge M = {Alle Personen hier im Raum} und sage:

Für $x \in M$: *„x ist ein Professor.“*

(manchmal wahr und manchmal falsch, je nachdem, was ich für x einsetze)

Wir nennen:

- x ist eine Variable
- *„x ist ein Professor.“* ist ein Prädikatsform, d.h. eine Aussageform, die von einer (oder mehreren) Variablen abhängt.

Beispiel: Für $n \in \mathbf{N}$ (Definition des Grundbereiches) gibt es das Prädikat

prim(n) : n ist prim.

Dann ist prim(5) wahr und prim(6) falsch.

Formeln

Wie in der Aussagenlogik besteht eine Formel aus einem einzigen Prädikat:

prim(2)

oder man kann durch Verknüpfungen größere Formeln generieren, z.B.:

prim(2) ^ prim(5) $\rightarrow$ kleiner(1,5*2)

Zugrunde liegen die Aussageformen

- prim(x): x ist eine Primzahl
- kleiner(x,y): x ist kleiner als y

deren Platzhalter (d.h. Variablen) x und y hier durch Konstanten 2 bzw. 5 ersetzt worden sind. Dadurch entstehen aus Aussagenformen ganz konkrete Aussagen.

Man kann die Variablen auch durch Quantoren binden, um Aussagen zu erhalten:

Quantoren

Allquantor $\forall$:

Trifft Aussagen für eine Formel und alle Elemente eines Grundbereichs.

$$\forall n \in \mathbf{N}_+ : P(n)$$

Für alle n Element der natürlichen Zahlen gilt P(n).

Existenzquantor $\exists$:

Trifft Existenzaussagen für ein Prädikat und mindestens ein Element des Grundbereichs.

$$\exists n \in \mathbf{N}_+ : P(n)$$

Es existiert mindestens ein Element n der natürlichen Zahlen für das P(n) gilt.

Quantoren: Beispiel

„Everybody loves somebody sometime“

(Irving Taylor/Dean Martin)

Prädikatenlogik: $\forall x \, \exists y \, \exists t : loves\,(x,y,t)$

Es geht auch: $\forall x \, \exists t \, \exists y : loves\,(x,y,t)$

Aber etwas anderes ist: $\exists t \, \forall x \, \exists y : loves\,(x,y,t)$

Achtung: Nur Quantoren gleicher Art sind vertauschbar:

- $\forall x \, \forall y$ ist identisch zu $\forall y \, \forall x$
- $\exists x \, \exists y$ ist identisch zu $\exists y \, \exists x$

Achtung:

- $\forall x \, \exists y$ ist NICHT identisch zu $\exists y \, \forall x$:
  - $\forall x \, \exists y \; mutter\,(y,x)$ Jeder hat eine Mutter.
  - $\exists y \, \forall x \; mutter\,(y,x)$ Es gibt jemanden, der die Mutter von allen ist.

Prädikatenlogik: weitere Beispiele

- „Brüder sind Geschwister“:
  $\forall x\ \forall y\ (bruder(x,y) \rightarrow geschwister(x,y)\ )$
- „bruder“ ist symmetrisch:
  $\forall x\ \forall y\ (bruder(x,y) \leftrightarrow bruder(y,x))$
- „Mütter sind weibliche Elternteile“:
  $\forall x\ \forall y\ (mutter(x,y) \leftrightarrow weiblich(x) \wedge ist\_elternteil\_von(x,y))$
- „Ein Cousin ersten Grades ist das Kind eines Geschwisters eines Elternteils“:
  $$\forall x\ \forall y\ (cousin(x,y) \leftrightarrow \exists px\ \exists py\ (ist\_elternteil\_von(px,x) \wedge ist\_elternteil\_von(py,y) \wedge geschwister(px,py)\ )\ )$$

Umformungen von prädikatenlogischen Formeln

Alle Regeln (Umformungen, Äquivalenzen) aus der Aussagenlogik gelten auch für prädikatenlogische Formeln. Es gibt aber auch noch weitere:

- $\neg\forall x\text{: } p(x) \leftrightarrow \exists x\text{: } \neg p(x)$

  „Nicht für alle Studenten gilt, dass Sie einen Kaffee getrunken haben“

  Das ist äquivalent (Zeichen: „ $\approx$“) zu:

  „Es existiert mindestens ein Student, der keinen Kaffee getrunken hat“.

- $\neg\exists x\text{: } p(x) \leftrightarrow \forall x\text{: } \neg p(x)$

Es gilt auch:

- $\exists x\text{: } (p(x) \vee q(x)) \approx (\exists x\text{: } p(x) \vee \exists x\text{:} q(x))$
- $\forall x\text{: } (p(x) \wedge q(x)) \approx (\forall x\text{: } p(x) \wedge \forall x\text{:} q(x))$

Prüfen Sie bitte einmal kritisch: Wie sieht es mit

- $\exists x\text{: } (p(x) \wedge q(x)) \approx (\exists x\text{: } p(x) \wedge \exists x\text{:} q(x))$ bzw. mit
- $\forall x\text{: } (p(x) \vee q(x)) \approx (\forall x\text{: } p(x) \vee \forall x\text{:} q(x))$ aus?

Wozu das Ganze?
Ein Blick in die Zukunft…

Wir werden die Prädikatenlogik verwenden, um Mengen und damit Sprachen auszudrücken. Man verwendet Sie aber auch allgemein, um Sachverhalte oder Erkenntnisse formal auszudrücken.

Das schwierigste Thema in dieser Veranstaltung ist das

Pumping Lemma (werden wir in ein paar Wochen behandeln):

Für jede reguläre Sprache L gibt es eine Zahl $n \in \mathbf{N}_+$, so dass jedes Wort $w \in L$ mit Länge $m=|w| \geq n$ zerlegt werden kann in $w = xyz$ mit den Eigenschaften

1. $y \neq \varepsilon$ *(der Kreis ist nicht leer)*
2. $|xy| \leq n$ *(der Kreis ergibt sich nach höchstens n Übergängen)*
3. *für alle* $k \in \mathbf{N}_0$ *ist* $xy^kz \in L$ *(man kann auch öfter den Kreis durchlaufen)*

… wie sieht das Pumping Lemma als Prädikatenlogik-Formal aus?

Zusammenfassung

Mengenlehre, Aussagenlogik und Prädikatenlogik sind Grundkonzepte der Mathematik und Informatik und finden sich dort überall.

- Mengen sind i.a. nicht geordnet. Geordnete Mengen heißen Tupel.
- Vorsicht vor dem exponentiellen Wachstum der Potenzmenge einer Menge!
- Mit Hilfe von Wahrheitstabellen kann man den Wahrheitsgehalt von logischen Ausdrücken bestimmen, aber die Tabellen haben exponentiell viele Zeilen.
- Mengen und Aussagen kann man durch Gesetze vereinfachen.
- Das Erfüllbarkeitsproblem ist ein Standardproblem der Informatik. Es ist bisher ungelöst, ob es auch ein effizientes Verfahren dafür gibt.
- In der Prädikatenlogik werden Prädikate auch auf Argumente (Variablen, Konstanten, oder allgemein: „Terme“) angewendet. Die Argumente (Terme) können auch Funktionsausdrücke sein.
- Die PL hat einen All-Quantor und einen Existenz-Quantor für Variablen.
- Verschiedenartige Quantoren darf man nicht vertauschen.
- Alle Rechenregeln der AL gelten auch in der PL, und Regeln mit Quantoren.