

Diskrete Strukturen

für die Studiengänge

- Angewandte Informatik
- Technische Informatik

02 Logik

Prof. Dr. David Sabel
Wintersemester 2024/25

Stand der Folien: 17. November 2024

Inhalt

- 1 Aussagen und Aussagenlogik
- 2 Gesetze der Aussagenlogik
- 3 Vollständige Mengen von Junktoren
- 4 Anwendungen der Aussagenlogik
- 5 Quantoren und prädikatenlogische Formeln

Einführendes zur Logik

- Wichtige Grundlage der Informatik:
 - Kontrollfluss in Programmen wird durch Logik gesteuert
 - Digitale Schaltungen basieren auf Schaltungslogik
 - Logische Programmiersprachen basieren auf Logiken
 - Inferenzsysteme verwenden logische Schlüsse
 - Spezifikationen in der Programmverifikation werden in Logiken formuliert
 - ...
- Eine Logik ist formal aufgebaut aus
 - Syntax: Wie sehen formal aus?
 - Semantik: Welche Bedeutung haben (syntaktisch richtige) Formeln?

Aussagen

Definition (Aussage)

Eine **Aussage** ist ein sprachlicher Satz, der entweder **falsch** oder **wahr** ist (aber nie beides gleichzeitig).

Definition (Wahrheitswerte)

Eine **wahre** Aussage hat den Wahrheitswert „*w*“ (oder „1“ oder „true“)
Eine **falsche** Aussage hat den Wahrheitswert „*f*“ (oder „0“ oder „false“).

Beispiele für Aussagen



- Wiesbaden ist die Landeshauptstadt von Hessen. (w)
- Es gibt beliebig große Primzahlen. (w)
- $10+20 = 42$ (f)
- Alle Informatikstudierende lieben die Mathematik (unklar, vermutlich f)
- Jede gerade Zahl größer als 2 ist die Summe zweier Primzahlen (unbekannt). Dies ist die Goldbach-Vermutung, die bis heute unbewiesen ist.
- Jedes Java-Programm terminiert. (f)

Keine Aussagen



- Guten Morgen!
- $5+3$
- Wann ist die Vorlesung endlich vorbei?
- **Keine** Aussage ist folgendes Paradoxon:

„Ich lüge gerade.“

Sowohl die Annahme, es sei wahr, als auch die Annahme, es sei falsch, führen zu einem Widerspruch!

Welche der folgenden Sätze sind Aussagen?



- Die Erde ist eine Scheibe.
- Lasst uns feiern!
- 2 ist eine Primzahl.
- Wann machen wir Pause?
- Dieser Satz ist falsch.
- Die Kreiszahl π enthält jede beliebige Ziffernfolge.

Wahrheitsgehalt der Aussagen?

Syntax der Aussagenlogik



Aussagen werden durch Variablen A, B, \dots repräsentiert (= **aussagenlogische Variablen**)

Definition (Aussagenlogische Formeln)

Aussagenlogische Variablen und Wahrheitswerte sind **aussagenlogische Formeln**

Wenn F und G aussagenlogische Formeln sind, dann auch

$(\neg F)$	(Negation)	„nicht F “
$(F \wedge G)$	(Konjunktion) logisches Und	„ F und G “
$(F \vee G)$	(Disjunktion) logisches Oder	„ F oder G “
$(F \oplus G)$	(Kontravalenz), exklusives Oder	„ F entweder oder G “
$(F \rightarrow G)$	(Implikation)	„wenn F , dann G “
$(F \leftrightarrow G)$	(Äquivalenz) Biimplikation	„ F genau dann, wenn G “

Beispiel: $(A \vee (B \wedge \neg(C \rightarrow w)))$

Junktoren

Die aussagenlogischen Operatoren $\neg, \vee, \wedge, \dots$ nennt man auch **Junktoren**

Wir zählen auch w und f zu den Junktoren (0-stellige Junktoren).

Bedeutung der Junktoren: Sie sind Funktionen auf Wahrheitswerten, d.h. für Eingaben berechnen sie Ausgaben.

Wir legen sie fest durch Wahrheitstabellen.

Eselsbrücke: \vee „Oder ist oben offen“

Semantik der Negation

A	$\neg A$
w	f
f	w

D.h. $\neg A$ ist genau dann eine wahre Aussage, wenn A falsch ist.

Z.B. ist $\neg(\text{Die Erde ist eine Scheibe})$ eine wahre Aussage.

Semantik der Konjunktion

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

D.h. $(A \wedge B)$ ist genau dann eine wahre Aussage, wenn **beide** Aussagen A und B wahr sind.

Semantik der Disjunktion

A	B	$(A \vee B)$
f	f	f
f	w	w
w	f	w
w	w	w

D.h. $(A \vee B)$ ist genau dann eine wahre Aussage, wenn **mindestens eine** der beiden Aussagen A oder B wahr ist.

Semantik der Kontravalenz

A	B	$(A \oplus B)$
f	f	f
f	w	w
w	f	w
w	w	f



D.h. $(A \oplus B)$ ist genau dann eine wahre Aussage, wenn **genau eine** der beiden Aussagen A oder B wahr ist.

Semantik der Implikation

Die Implikation hat die folgende Semantik:

A	B	$(A \rightarrow B)$
f	f	w
f	w	w
w	f	f
w	w	w



D.h. $(A \rightarrow B)$ ist genau dann wahr, wenn A **falsch** ist **oder** A und B **beide wahr** sind.

Semantik der Äquivalenz

A	B	$(A \leftrightarrow B)$
f	f	w
f	w	f
w	f	f
w	w	w



D.h. $(A \leftrightarrow B)$ ist genau dann wahr, wenn A und B **denselben Wahrheitswert** haben.

Semantik der aussagenlogischen Formeln

Der Wahrheitswert der Formeln hängt ab vom Wahrheitswert der **Variablen**.

Eine **Belegung** \mathcal{B} weist (endlich vielen) aussagenlogischen Variablen einen Wahrheitswert zu.

Belegung \mathcal{B} **für** F weist mindestens allen Variablen aus F einen Wahrheitswert zu.

$\mathcal{B}(F)$: „Wahrheitswert von F unter der Belegung \mathcal{B} “

- 1 Ersetze A durch $\mathcal{B}(A)$ in F .
- 2 Werte danach die Junktoren von innen nach außen aus.

Beispiel

Formel $F = ((A \wedge \neg B) \rightarrow \neg(C \rightarrow A))$.

Belegung $\mathcal{B}_1 = \{A \mapsto f, B \mapsto f, C \mapsto w\}$

Berechne $\mathcal{B}_1(F)$:

$$\begin{aligned}
 \mathcal{B}_1(F) &= \mathcal{B}_1((A \wedge \neg B) \rightarrow \neg(C \rightarrow A)) \\
 &= ((\mathcal{B}_1(A) \wedge \neg \mathcal{B}_1(B)) \rightarrow \neg(\mathcal{B}_1(C) \rightarrow \mathcal{B}_1(A))) \\
 &= ((f \wedge \neg f) \rightarrow \neg(w \rightarrow f)) \\
 &= ((f \wedge w) \rightarrow \neg(w \rightarrow f)) \\
 &= (f \rightarrow \neg(w \rightarrow f)) \\
 &= (f \rightarrow \neg f) \\
 &= (f \rightarrow w) \\
 &= w
 \end{aligned}$$

Wiederholung

		Negation	Konjunktion	Disjunktion	Kontravalenz	Implikation	Äquivalenz
A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \oplus B$	$A \rightarrow B$	$A \leftrightarrow B$
f	f	w	f	f	f	w	w
f	w		f	w	w	w	f
w	f	f	f	w	w	f	f
w	w		w	w	f	w	w

Wahrheitswert für alle Belegungen

Verwende eine Wahrheitstabelle:

- Spalten für alle Variablen
- Spalten für alle Teilformeln
- Zeilen für jede mögliche Belegung der Variablen
- Sukzessive Auswertung der Teilformeln, bis man bei der Gesamtformel ist.

Beispiel

Formel $(A \wedge \neg B) \rightarrow \neg(A \vee C)$

A	B	C	$\neg B$	$(A \wedge \neg B)$	$A \vee C$	$\neg(A \vee C)$	$(A \wedge \neg B) \rightarrow \neg(A \vee C)$
f	f	f	w	f	f	w	w
f	f	w	w	f	w	f	w
f	w	f	f	f	f	w	w
f	w	w	f	f	w	f	w
w	f	f	w	w	w	f	f
w	f	w	w	w	w	f	f
w	w	f	f	f	w	f	w
w	w	w	f	f	w	f	w

GESETZE DER AUSSAGENLOGIK

- Gesetze von de Morgan
- Gesetze der Booleschen Algebra
- Dualität
- Weitere Rechengesetze

Prioritäten, Klammerregeln

Problem: Unklar was $\neg A \vee B \wedge C$ meint:

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

Wir legen die Prioritäten fest als:

$$\neg > \wedge > \oplus > \vee > \rightarrow > \leftrightarrow$$

Höhere Priorität $>$ bedeutet „bindet die Operanden vorher“.

Beispiel: $\neg A \vee B \wedge C \rightarrow D \neg A \vee B \wedge C \rightarrow D(\neg A) \vee B \wedge C \rightarrow D(\neg A) \vee B \wedge C \rightarrow D(\neg A) \vee (B \wedge C) \rightarrow D$

Assoziativität: $A \vee B \vee C = (A \vee B) \vee C$ oder $\dots = A \vee (B \vee C)$? später...

Sätze

Definition (Tautologie)

Eine aussagenlogische Formel, die für jede Belegung wahr ist, nennt man eine **Tautologie** (oder **allgemeingültige Formel**)

Tautologien sind die **Sätze der Logik**.

Beispiel: $(A \wedge B) \rightarrow A$ ist eine Tautologie, denn

A	B	$A \wedge B$	$(A \wedge B) \rightarrow A$
f	f	f	w
f	w	f	w
w	f	f	w
w	w	w	w

Widerspruch

Definition (Widerspruch)

Eine aussagenlogische Formel, die für jede Belegung falsch ist, nennt man eine **Kontradiktion** (oder **Widerspruch**)

Beispiel:

$A \wedge \neg A$ ist eine Kontradiktion, denn

A	$\neg A$	$A \wedge \neg A$
f	w	f
w	f	f

Definition (Erfüllbarkeit und Widerlegbarkeit)

Sei F eine aussagenlogische Formel

- Wenn F für **mindestens eine Belegung wahr** ist, dann heißt F **erfüllbar**.
- Wenn F für **mindestens eine Belegung falsch** ist, dann heißt F **widerlegbar**

Beispiele:

- $(A \wedge B) \rightarrow A$ ist eine Tautologie, damit auch erfüllbar, aber nicht widerlegbar.
- $A \wedge \neg A$ eine Kontradiktion, damit auch widerlegbar, aber nicht erfüllbar.
- $A \wedge B$ ist erfüllbar und widerlegbar, denn

A	B	$A \wedge B$
f	f	f
w	w	w

Definition

Zwei Formeln F und G heißen **logisch äquivalent** geschrieben $F \equiv G$, wenn für jede Belegung \mathcal{B} gilt $\mathcal{B}(F) = \mathcal{B}(G)$.

Nachweis $F \equiv G$: Wahrheitstabelle mit allen Belegungen und mit Spalten für F und G .
Diese dann vergleichen

Beispiel: $A \rightarrow B \equiv \neg A \vee B$ gilt, denn:

A	B	$\neg A$	$A \rightarrow B$	$\neg A \vee B$
f	f	w	w	w
f	w	w	w	w
w	f	f	f	f
w	w	f	w	w

Satz

Zwei Formeln F und G sind genau dann logisch äquivalent, wenn $(F \leftrightarrow G)$ eine Tautologie ist.

Beweis (Skizze): Zwei Richtungen.

- „Wenn $F \equiv G$, dann ist $(F \leftrightarrow G)$ eine Tautologie.“
- „Wenn $(F \leftrightarrow G)$ eine Tautologie ist, dann gilt $F \equiv G$.“

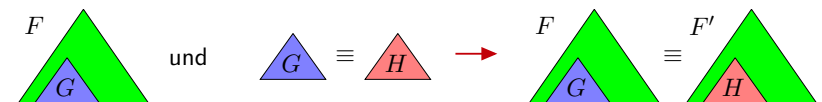
In beiden Fällen kann man über alle Belegungen argumentieren (siehe Skript).

Logische äquivalente (Teil-)Formeln darf man austauschen:

Satz

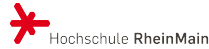
Sei F eine aussagenlogische Formel, die die Formel G als Teilformel enthält. Sei $G \equiv H$. Dann gilt $F \equiv F'$, wobei F' aus F entsteht, indem die Teilformel G durch H ersetzt wird.

Skizze dazu:



Beweis: Argumentiere über die Berechnung mit der Wahrheitstabelle.

Substitution von Variablen mit Formeln



Definition (Substitution)

Seien F, G_1, \dots, G_n Formeln und A_1, \dots, A_n aussagenlogische Variablen. Dann bezeichne $F[G_1/A_1, \dots, G_n/A_n]$ die Formel, die entsteht, indem jeweils für $1 \leq i \leq n$ alle Vorkommen von A_i in F durch die Formel G_i ersetzt werden.

Bemerkung: Die Substitution ist parallel durchzuführen, denn

$$F[G/A][H/B] \neq F[G/A, H/B] \text{ wenn } B \text{ in } G \text{ vorkommt}$$

Satz

Seien F, G, H aussagenlogische Formeln, A eine aussagenlogische Variable. Wenn $F \equiv G$ gilt, dann gilt auch $F[H/A] \equiv G[H/A]$

Gesetze von de Morgan



Satz von den Morgan

Seien F und G aussagenlogische Formeln. Dann gilt

$$\text{Erstes de Morgansches Gesetz: } \neg(F \wedge G) \equiv \neg F \vee \neg G$$

$$\text{Zweites de Morgansches Gesetz: } \neg(F \vee G) \equiv \neg F \wedge \neg G$$

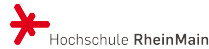
Beweis. Es genügt, die Teilformeln F und G wie aussagenlogische Variablen zu behandeln (wegen letztem Satz).

Wahrheitstabelle:

F	G	$(F \wedge G)$	$\neg(F \wedge G)$	$\neg F$	$\neg G$	$\neg F \vee \neg G$
f	f	f	w	w	w	w
f	w	f	w	w	f	w
w	f	f	w	f	w	w
w	w	w	f	f	f	f

Das zweite Gesetz lässt sich analog beweisen. □

Rechengesetze für \neg, \wedge, \vee



Satz (Rechengesetze für \wedge, \vee, \neg)

Für alle aussagenlogischen Formeln F, G, H gelten die folgenden Gesetze:

- Kommutativgesetz: $F \wedge G \equiv G \wedge F$ und $F \vee G \equiv G \vee F$
- Assoziativgesetz: $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ und $(F \vee G) \vee H \equiv F \vee (G \vee H)$
- Distributivgesetze: $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ und $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
- Existenz neutraler Elemente: $F \wedge w \equiv F$ und $F \vee f \equiv F$
- Existenz des Komplements: $F \wedge \neg F \equiv f$ und $F \vee \neg F \equiv w$

Alle Gesetze können mit Wahrheitstabellen bewiesen werden.

Wir machen es nur für das 1. Distributivgesetz

Beweis der 1. Distributivgesetz



F	G	H	$G \wedge H$	$F \vee (G \wedge H)$	$F \vee G$	$F \vee H$	$(F \vee G) \wedge (F \vee H)$
f	f	f	f	f	f	f	f
f	f	w	f	f	f	w	f
f	w	f	f	f	w	f	f
f	w	w	w	w	w	w	w
w	f	f	f	w	w	w	w
w	f	w	f	w	w	w	w
w	w	f	f	w	w	w	w
w	w	w	w	w	w	w	w

Satz

\oplus ist kommutativ und assoziativ.

Beweis. Übungsaufgabe

Da \vee, \wedge, \oplus assoziativ sind, lassen wir Klammern manchmal weg und schreiben $F \vee G \vee H, F \wedge G \wedge H$ bzw. $F \oplus G \oplus H$.

Eine Menge mit ausgezeichneten Elementen w, f und Operationen \wedge, \vee, \neg auf dieser Menge, für welche die

- Kommutativgesetze,
- Assoziativgesetze,
- Distributivgesetze,
- Existenz neutraler Elemente und
- Existenz des Komplements

gelten, nennt man **Boolesche Algebra** (benannt George Boole).

D.h. insbesondere $(\{f, w\}, \wedge, \vee, \neg)$ wie zuvor definiert, ist eine Boolesche Algebra. Es gibt auch weitere Boolesche Algebren.

Die Rechengesetze bestehen immer aus zwei symmetrischen Teilen:
Man erhält den einen Teil aus dem Anderen, indem man \wedge mit \vee sowie f mit w vertauscht.

Diese Eigenschaft der Booleschen Algebra nennt man **Dualität**

Ein Satz ist **dual** zu einem anderen Satz, wenn man ihn erhält, indem man \wedge mit \vee sowie f mit w vertauscht.

Satz (weitere Rechengesetze)

Für alle aussagenlogischen Formeln F und G gilt:

- Absorptionsgesetz: $F \wedge (F \vee G) \equiv F$ und $F \vee (F \wedge G) \equiv F$
- Idempotenzgesetz: $F \vee F \equiv F$ und $F \wedge F \equiv F$
- Involutionsgesetz (doppelte Negation): $\neg(\neg F) \equiv F$
- Extremalgesetz: $F \vee w \equiv w$ und $F \wedge f \equiv f$

Beweis. Involutionsgesetz und die Extremalgesetze können mit einer Wahrheitstabelle verifiziert werden.

$$\begin{aligned}
 1. \text{ Absorptionsgesetz: } & F \wedge (F \vee G) \\
 & \equiv (F \vee f) \wedge (F \vee G) \quad (\text{Existenz neutraler Elemente}) \\
 & \equiv (F \vee (f \wedge G)) \quad (\text{Distributivgesetz}) \\
 & \equiv (F \vee (G \wedge f)) \quad (\text{Kommutativgesetz}) \\
 & \equiv (F \vee f) \quad (\text{Extremalgesetz}) \\
 & \equiv f \quad (\text{Existenz neutraler Elemente})
 \end{aligned}$$

Aufgrund der Dualität können wir in allen Zwischenschritten \wedge mit \vee und f mit w vertauschen, was direkt das zweite Absorptionsgesetz zeigt.

Satz (weitere Rechengesetze)

Für alle aussagenlogischen Formeln F und G gilt:

- Idempotenzgesetze: $F \vee F \equiv F$ und $F \wedge F \equiv F$

Beweis des 1. Idempotenzgesetz:

$$\begin{aligned}
 &F \vee F \\
 &\equiv F \vee (F \wedge w) \quad (\text{Existenz neutraler Elemente}) \\
 &\equiv F \quad (\text{Absorptionsgesetz})
 \end{aligned}$$

Da das 1. Absorptionsgesetz dual zum 2. Absorptionsgesetz ist, folgt das 2. Idempotenzgesetz mittels der Dualität.

Wir vereinfachen die Formel $\neg(A \vee \neg B) \vee (A \wedge B)$

$$\begin{aligned}
 &\neg(A \vee \neg B) \vee (A \wedge B) \\
 &\equiv (\neg A \wedge \neg \neg B) \vee (A \wedge B) \quad (\text{De Morgansches Gesetz}) \\
 &\equiv (\neg A \wedge B) \vee (A \wedge B) \quad (\text{Involutionsgesetz}) \\
 &\equiv (B \wedge \neg A) \vee (B \wedge A) \quad (\text{Kommutativgesetz, 2 Mal}) \\
 &\equiv B \wedge (\neg A \vee A) \quad (\text{Distributivgesetz}) \\
 &\equiv B \wedge (A \vee \neg A) \quad (\text{Kommutativgesetz}) \\
 &\equiv B \wedge w \quad (\text{Komplement}) \\
 &\equiv B \quad (\text{Neutrale Elemente})
 \end{aligned}$$

VOLLSTÄNDIGKEIT VON JUNKTOREN

- Boolesche Funktionen
- Vollständige Menge von Junktoren

Boolesche Funktionen

Formel F mit Variablen A_1, \dots, A_n ist wie **Boolesche Funktion** $h(A_1, \dots, A_n)$

Umgekehrte Frage: Welche Boolesche Funktionen gibt es?

0-stellig: $h_1 = w$ und $h_2 = f$.

1-stellig: Vier Funktionen: Identität, konstant f , konstant w , Negation

2-stellig: ...

Satz

Für jede Boolesche Funktion h gibt es eine aussagenlogische Formel, die h berechnet.

Beweisidee:

- Gegeben: Wahrheitstabelle für h .
- Für jede „w“-Zeile: Bilde Konjunktion entsprechend der Belegung.
- Gesamtformel F : Disjunktion der Konjunktionen.
- $\mathcal{B}(F)$ ist genau dann wahr, wenn $h(\mathcal{B}(A_1), \dots, \mathcal{B}(A_n))$ wahr ist.

Passende Formel zur Booleschen Funktion: Beispiel

A	B	C	$h(A, B, C)$
f	f	f	w
f	f	w	f
f	w	f	w
f	w	w	f
w	f	f	w
w	f	w	w
w	w	f	f
w	w	w	w

$$\neg A \wedge \neg B \wedge \neg C$$

$$\neg A \wedge B \wedge \neg C$$

$$A \wedge \neg B \wedge \neg C$$

$$A \wedge \neg B \wedge C$$

$$A \wedge B \wedge C$$

$$F = (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee \neg B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (A \vee B \vee C)$$

Eine solche Disjunktion von Konjunktionen nennt man auch **Disjunktive Normalform**.

Vollständige Mengen an Junktoren

Definition (Vollständige Menge)

Eine Menge M von Junktoren heißt **vollständig**, wenn für jede aussagenlogische Formel eine logisch äquivalente Formel existiert, die nur die Junktoren aus M benutzt.

Beispiele:

- $\{w, f, \vee, \wedge\}$ nicht vollständig, denn z.B. für $\neg A$ keine logisch äquivalente Formel
- $\{\vee, \wedge, \neg\}$ vollständig, denn

$$w \equiv A \vee \neg A \quad f \equiv A \wedge \neg A \quad F \rightarrow G \equiv \neg F \vee G$$

$$F \leftrightarrow G \equiv F \rightarrow G \wedge G \rightarrow F \quad F \oplus G \equiv (F \vee G) \wedge \neg(F \wedge G)$$

- $\{\neg, \vee\}$ und $\{\neg, \wedge\}$ jeweils vollständig, denn

$$F \wedge G \equiv \neg(\neg F \vee \neg G) \quad F \vee G \equiv \neg(\neg F \wedge \neg G)$$

ANWENDUNGEN DER AUSSAGENLOGIK

- Digitale Schaltungen
- SAT-Solving

Anwendung der Aussagenlogik: Schaltungsentwurf

Schaltkreise sind aussagenlogische Formeln.

Beispiel: 2-aus-3-Schaltung: Die Wahrheitstabelle der gesuchten Funktion h :

A	B	C	$h(A, B, C)$
f	f	f	f
f	f	w	f
f	w	f	f
f	w	w	w
w	f	f	f
w	f	w	w
w	w	f	w
w	w	w	w

$$\text{Disjunktive NF } F := (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$$

Anwendung der Aussagenlogik: Schaltungsentwurf (2)

$$F := (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$$

kann man vereinfachen:

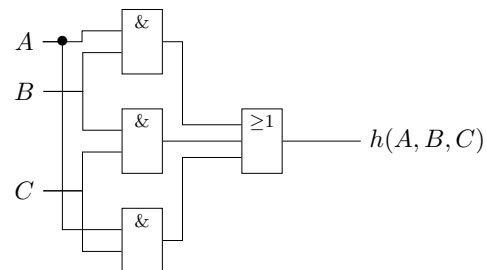
$$\begin{aligned} & (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C) \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee ((A \wedge B) \vee (\neg C \wedge C)) && \text{(Ausklammern von } A \wedge B) \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee ((A \wedge B) \wedge w) && \text{(Existenz des Komplements)} \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B) && \text{(Idempotenzgesetz)} \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge ((\neg B \wedge C) \vee B)) && \text{(Ausklammern von } A) \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge ((B \vee \neg B) \wedge (B \vee C))) && \text{(Ausmultiplizieren)} \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge (w \wedge (B \vee C))) && \text{(Existenz des Komplements)} \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge (B \vee C)) && \text{(Idempotenzgesetz)} \\ \equiv & (\neg A \wedge B \wedge C) \vee (A \wedge B) \vee (A \wedge C) && \text{(Ausmultiplizieren)} \\ \equiv & (C \wedge ((\neg A \wedge B) \vee A)) \vee (A \wedge B) && \text{(Ausklammern von } C) \\ \equiv & (C \wedge ((A \vee \neg A) \wedge (A \vee B))) \vee (A \wedge B) && \text{(Ausmultiplizieren)} \\ \equiv & (C \wedge (w \wedge (A \vee B))) \vee (A \wedge B) && \text{(Existenz des Komplements)} \\ \equiv & (C \wedge ((A \vee B))) \vee (A \wedge B) && \text{(Idempotenzgesetz)} \\ \equiv & (C \wedge A) \vee (C \wedge B) \vee (A \wedge B) && \text{(Ausmultiplizieren)} \end{aligned}$$

Es gibt dafür spezielle Verfahren (KV-Diagramme) und Tools z.B. wolframalpha.com.

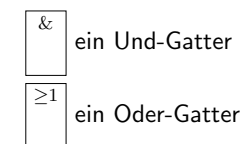
Anwendung der Aussagenlogik: Schaltungsentwurf (3)

$$F \equiv (A \wedge B) \vee (A \wedge C) \vee (B \wedge C)$$

Schaltkreis dazu



Dabei ist:



Anwendung der Aussagenlogik: SAT-Solving

- Idee: Kodiere Problem als aussagenlogische Formel
- Ziel: Finde erfüllende Belegung eine Formel (nennt man auch **Modell**)
- Erfüllende Belegung = Lösung des Problems / Rätsels etc.
- Softwarewerkzeug zum Finden des Modells: SAT-Solver (SAT = satisfiability)
- Wir betrachten als Beispiel ein Rätsel von Raymond Smullyan.

Wer ist der Pfefferdieb?

Es gibt drei Verdächtige: Den Hutmacher, den Schnapphasen und die Haselmaus.

- 1 Genau einer von ihnen ist der Dieb.
- 2 Unschuldige sagen immer die Wahrheit
- 3 Schnappphase: Der Hutmacher ist unschuldig.
- 4 Hutmacher: Die Haselmaus ist unschuldig

Rätsel kodieren mit Aussagenlogik:

Variablen H , S und M für Hutmacher / Schnappphase / Maus ist schuldig.

- Für 1.: $(H \vee M \vee S) \wedge \neg(H \wedge M) \wedge \neg(H \wedge S) \wedge \neg(M \wedge S)$
- Für 2. und 3.: $\neg S \rightarrow \neg H$
- Für 2. und 4.: $\neg H \rightarrow \neg M$

Gesamtformel:

$$(H \vee M \vee S) \wedge \neg(H \wedge M) \wedge \neg(H \wedge S) \wedge \neg(M \wedge S) \wedge (\neg S \rightarrow \neg H) \wedge (\neg H \rightarrow \neg M)$$

Modell berechnen mit SAT-Solver

Vereinfachen

$$\begin{aligned} & (H \vee M \vee S) \wedge \neg(H \wedge M) \wedge \neg(H \wedge S) \wedge \neg(M \wedge S) \wedge (\neg S \rightarrow \neg H) \wedge (\neg H \rightarrow \neg M) \\ \equiv & (H \vee M \vee S) \wedge \neg(H \wedge M) \wedge \neg(H \wedge S) \wedge \neg(M \wedge S) \wedge (S \vee \neg H) \wedge (\neg H \rightarrow \neg M) \\ \equiv & (H \vee M \vee S) \wedge \neg(H \wedge M) \wedge \neg(H \wedge S) \wedge \neg(M \wedge S) \wedge (S \vee \neg H) \wedge (H \vee \neg M) \\ \equiv & (H \vee M \vee S) \wedge (\neg H \vee \neg M) \wedge (\neg H \vee \neg S) \wedge (\neg M \vee \neg S) \wedge (S \vee \neg H) \wedge (H \vee \neg M) \end{aligned}$$

Dies ist eine **Konjunktive Normalform** (eine Disjunktion von Konjunktionen)

Eingabe für SAT-Solver im DIMACS-Format Ausgabe (z.B. msoos.github.io/cryptominisat_web)
(1 = H, 2 = M, 3 = S)

```
p cnf 3 6
1 2 3 0
-1 -3 0
-1 -2 0
-2 -3 0
-1 3 0
1 -2 0
```

```
SAT -1 -2 3
```

Erfüllende Belegung ist:

$\{H \mapsto f, M \mapsto f, S \mapsto w\}$

D.h. ?

FORMELN MIT QUANTOREN

- Aussageformen
- All- und Existenzquantoren
- Prädikatenlogische Formeln

Quantoren: Einführung

- Wir machen die Betrachtung nicht ganz formal
- Lernziel: Umgang mit Quantoren beherrschen
- Genaue Semantik ist Inhalt vertiefender Veranstaltungen

Objektvariablen und Aussageformen

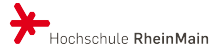
- Bisher: Aussagen wie „2 ist eine Primzahl“
- Es fehlt: Konstrukte wie „ x ist eine Primzahl“: Wahrheitsgehalt hängt von x ab!
- „ x ist eine Primzahl“ ist **keine** Aussage!
- **Aussageform**: Sätze mit Variablen für Objekte
- Setzt man Werte für die Variablen ein, erhält man Aussagen.

Aussageform „ x ist eine Primzahl“

- 2 für x einsetzen: Man erhält eine wahre Aussage
- 4 für x einsetzen: Man erhält eine falsche Aussage
- Grün für x einsetzen: Das ist nicht gewollt!
- Die Menge der Werte für x sollte einschränkbar sein.

Ein solche **Menge für Objektvariablen** nennt man **Universum**

Universumsbeispiele, Aussageform



- „ x ist eine Primzahl“ \rightarrow sinnvolles Universum für x : \mathbb{N}
- „ x ist eine Farbe der additiven Farbmischung“
 \rightarrow sinnvolles Universum für x : alle Farben
- „Man benötigt x Fußballspieler:innen pro Team, damit ein Spiel angepfiffen werden darf.“
 \rightarrow sinnvolles Universum: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Definition (Aussageform)

Seien x_1, \dots, x_n Variablen und U_1, \dots, U_n Universen. Dann ist eine **Aussageform** ein Satz mit Variablen x_1, \dots, x_n , sodass nach Ersetzen aller Variablen x_i durch Objekte $u_i \in U_i$ ein Satz entsteht der wahr oder falsch ist.

Prädikatensymbole



- In der Aussagenlogik: Variablen A, B, \dots für Aussagen
- Jetzt: **Variablen P, Q, \dots für Aussageformen**
- Um die Anzahl und Namen der Objektvariablen von P festzulegen: $P(x_1, \dots, x_n)$
 P ist dann **n -stellig**.
- P, Q, \dots nennt man auch **Prädikatensymbole**

Beispiel:

- $P_1(x) =$ „ x ist Primzahl“
- Verwende dann $P_1(x)$ in den Formeln
- $P_1(2)$ meint dann die Aussage „2 ist Primzahl“.

Beispiel mit 3-stelligem Prädikatensymbol:

- $Q(x, y, z) := x + y = z$
- $Q(1, 2, 3)$ ist eine wahre Aussage, $Q(2, 2, 3)$ ist eine falsche Aussage

Allaussagen



Allaussagen sind Aussagen über **alle Elemente eines Universums**.

Beispiele:

- Alle Primzahlen > 10 sind ungerade.
Für alle x aus \mathbb{N} gilt: Wenn $x > 10$ und x Primzahl, dann ist x ungerade.
- In jedem Dreieck beträgt die Summe der Winkel 180 Grad.
Für alle x aus der Menge der Dreiecke gilt: Winkelsumme von x ist 180 Grad.
- Jede der Zahlen 15, 27, 69 ist ungerade.
Für alle x aus $\{15, 27, 69\}$ gilt: x ist ungerade.

Solche Allaussagen können stets in die Form

Für alle x aus einem Universum U gilt \dots

gebracht werden.

Allquantor



„Für alle x aus einem Universum U gilt $P(x)$ “

wird mit neuer Syntax (dem **Allquantor \forall**) ausgedrückt als

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



Semantik des Allquantors

$\forall x \in U : P(x)$ ist genau dann wahr,
wenn $P(u)$ für jedes $u \in U$ eine wahre Aussage ist.

Beachte: $\forall x \in U : P(x)$ ist wieder eine Aussage (wenn es keine anderen Variablen als x gibt)!

- $\forall x \in \mathbb{R} : x^2 \geq 0$ (w)
- $\forall x \in \{17, 39, 47\} : \text{ungerade}(x)$ (w)
- $\forall x \in \mathbb{N} : \text{Wenn } x \text{ Primzahl, dann ist } x \text{ ungerade}$ (f)
- $\forall x \in \{2, 3, 4, 5\} : \text{gerade}(x)$ (f)

Satz

Sei $U = \{u_1, \dots, u_n\}$ ein **endliches** Universum. Dann gilt
 $\forall u \in U : P(u) \equiv P(u_1) \wedge \dots \wedge P(u_n)$.

Beispiel:

$$\begin{aligned} & \forall x \in \{2, 3, 4, 5\} : \text{gerade}(x) \\ \equiv & \text{gerade}(2) \wedge \text{gerade}(3) \wedge \text{gerade}(4) \wedge \text{gerade}(5) \end{aligned}$$

Existenzaussagen fordern, dass **mindestens ein Element eines Universums** eine gewisse Eigenschaft hat.

Beispiele für Existenzaussagen sind:

- Es gibt eine gerade Primzahl.
Es gibt ein $x \in \mathbb{N}$, für das gilt: x ist gerade Primzahl
- Sei $U = \{1, 3, 5, 7, 8\}$. Dann gibt es ein $x \in U$, für das gilt: x ist gerade.
Es gibt ein $x \in \{1, 3, 5, 7, 8\}$, für das gilt: x ist gerade

Solche Existenzaussagen können stets in die Form

Es gibt ein x aus einem Universum U , für das gilt

gebracht werden.

Es gibt ein x aus einem Universum U , für das gilt: $P(x)$

wird mit neuer Syntax (dem **Existenzquantor** \exists) ausgedrückt als

$$\exists x \in U : P(x)$$

Semantik des Existenzquantors

$\exists x \in U : P(x)$ ist genau dann wahr,
wenn $P(u)$ für mindestens ein $u \in U$ eine wahre Aussage ist.

Beachte: $\exists x \in U : P(x)$ ist wieder eine Aussage (wenn es keine anderen Variablen als x gibt)!

Beispiele

- $\exists x \in \mathbb{R} : x^2 = 2$ (w)
- $\exists x \in \{2, 4, 5, 9\} : \text{gerade}(x)$ (w)
- $\exists x \in \mathbb{N} : x^2 = 2$ (f)
- $\exists x \in \{3, 5, 7, 9\} : \text{gerade}(x)$ (f)

Existenzquantor bei endlichem Universum

Satz

Sei $U = \{u_1, \dots, u_n\}$ ein **endliches** Universum. Dann gilt
 $\exists u \in U : P(u) \equiv P(u_1) \vee \dots \vee P(u_n)$.

Beispiel:

$$\begin{aligned} & \exists x \in \{2, 3, 4, 5\} : \text{gerade}(x) \\ \equiv & \text{gerade}(2) \vee \text{gerade}(3) \vee \text{gerade}(4) \vee \text{gerade}(5) \end{aligned}$$

Syntax der prädikatenlogischen Formeln

Zusammenfassend definieren wir:

Definition (Prädikatenlogische Formeln)

Atomare Aussagen sind prädikatenlogische Formeln.

Wenn P n -stelliges Prädikat, dann ist $P(x_1, \dots, x_n)$ eine prädikatenlogische Formel.

Wenn F und G prädikatenlogische Formeln und U ein Universum, dann sind

$$(\neg F), (F \wedge G), (F \vee G), (F \oplus G), (F \rightarrow G), (F \leftrightarrow G), \forall x \in U : F, \exists x \in U : F$$

prädikatenlogische Formeln.

Bemerkung Auch 0-stellige Prädikate sind erlaubt. Wenn nur solche vorkommen (und keine Quantoren), dann haben wir wieder eine aussagenlogische Formel

Für den Wahrheitswert eine Formel betrachten wir nur **geschlossene** Formeln, d.h. alle x sind unter einem Quantor $\exists x \dots$ oder $\forall x \dots$

Beispiele

- Wenn zwei Zahlen nicht größer oder kleiner zueinander sind, dann müssen sie gleich sein:

$$\forall x \in \mathbb{N} : \forall y \in \mathbb{N} : (\neg(x < y) \wedge \neg(y < x)) \rightarrow x = y$$

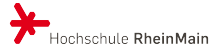
- Für jede natürliche Zahl, gibt es eine größere natürliche Zahl, die Primzahl ist

$$\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : x < y \wedge y \text{ ist Primzahl}$$

Wenn das Universum U klar ist, dann lassen wir es manchmal weg und schreiben

$$\begin{aligned} & \forall x : F \text{ statt } \forall x \in U : F \\ & (\text{bzw. } \exists x : F \text{ statt } \exists x \in U : F) \end{aligned}$$

Negation von All- und Existenzaussagen



Satz

- $\neg \forall x \in U : P(x) \equiv \exists x \in U : \neg P(x)$
- $\neg \exists x \in U : P(x) \equiv \forall x \in U : \neg P(x)$.

Beispiele für das Schieben der Negation:

- Negation von „Alle Menschen sind schlau“ ist:
„Es gibt (mindestens) einen nicht schlauen Menschen“
- Negation von „Es gibt eine schwere Klausur“ ist:
„Alle Klausuren sind nicht schwer“.
- $\neg(\exists x \in \mathbb{N} : x^2 = 2) \equiv \forall x \in \mathbb{N} : x^2 \neq 2$
- $\neg(\forall x \in \mathbb{R} : x^2 \neq 2) \equiv \exists x \in \mathbb{R} : x^2 = 2$

Quantorregeln



Satz

Es gilt

- $(\forall x \in U : P(x)) \wedge (\forall x \in U : Q(x)) \equiv (\forall x \in U : (P(x) \wedge Q(x)))$
- $(\exists x \in U : P(x)) \vee (\exists x \in U : Q(x)) \equiv (\exists x \in U : (P(x) \vee Q(x)))$

Beispiele:

- „Alle Autos haben ein Lenkrad und alle Autos haben mindestens drei Räder“ ist äquivalent zu
„Alle Autos haben ein Lenkrad und mindestens drei Räder.“
- $(\exists x \in \mathbb{N} : x > 10) \vee (\exists x \in \mathbb{N} : x < 5) \equiv (\exists x \in \mathbb{N} : x > 10 \vee x < 5)$.

Falsche Verschiebungen



Beachte:

- $\forall x \in U : (P(x) \vee Q(x))$ **ist nicht gleich zu** $(\forall x \in U : P(x)) \vee (\forall x \in U : Q(x))$
- $\exists x \in U : (P(x) \wedge Q(x))$ **ist nicht gleich zu** $(\exists x \in U : P(x)) \wedge (\exists x \in U : Q(x))$

Beispiele:

- „Für alle Primzahlen p gilt: p ist ungerade oder $p = 2$ “ ist **wahr**, aber
„(Alle Primzahlen sind ungerade) oder (Alle Primzahlen sind gleich zu 2)“
ist **falsch**.
- „Es gibt ein Auto mit drei Rädern und es gibt ein Auto mit vier Rädern“
ist **nicht gleich zu**
„Es gibt ein Auto mit drei und mit vier Rädern“.

Vertauschungsregeln



Satz

Für Universen U_1, U_2 und Formeln F gelten die folgenden Äquivalenzen:

- $\forall x \in U_1 : \forall y \in U_2 : F \equiv \forall y \in U_2 : \forall x \in U_1 : F$
- $\exists x \in U_1 : \exists y \in U_2 : F \equiv \exists y \in U_2 : \exists x \in U_1 : F$

Beispiel: $\forall x \in \mathbb{R} : \forall y \in \mathbb{R} : x \geq y \vee x < y \equiv \forall y \in \mathbb{R} : \forall x \in \mathbb{R} : x \geq y \vee x < y$

Gilt **nicht** für unterschiedliche Quantoren:

- $\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : x^2 = y$ ist **wahr**, aber $\exists y \in \mathbb{N} : \forall x \in \mathbb{N} : x^2 = y$ ist **falsch**
- „Es gibt einen Studierenden, der alle Aufgaben in der Klausur lösen kann.“
ist **nicht äquivalent zu**
„Jede Aufgabe der Klausur kann durch irgendeinen Studierenden gelöst werden.“

Schlussbemerkung



In vielen sprachlichen und mathematischen Sätzen wird oft implizit allquantifiziert
wird, ohne dass der Quantor genannt wird.

Beispiel:

„Die erste binomische Formel lautet:
Für reellwertige a, b gilt $(a + b)^2 = a^2 + b^2 + 2ab$ “

Implizit ist gemeint, dass diese Gleichung für alle $a, b \in \mathbb{R}$ gilt.