Formale Grundlagen der Informatik

WiSe 2014/15

Universität Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

1. Rechnen: Gesetze und Regeln

2. Modellieren und Formalisieren: Keine Angst vor Formalismen

3. Was ist hier schon logisch? Zum formalen Umgang mit der Logik

4. Warum stimmt das eigentlich ? Beweisverfahren

5. Herangehen an Aufgaben aus Informatik und Mathematik

Ziele der heutigen Veranstaltung

- Verstärktes Aufzeigen,
  was Mathematikunterricht an der Universität bedeuten kann.

- Unterbrechen Sie mich bitte, wenn Sie eine Folie nicht verstanden haben.

- ... sonst haben Sie Schwierigkeiten, “dem Rest” zu folgen.

- Weiteres (wichtiges) Ziel: Rekapitulation der “Grundlagen der elementaren Logik” aus dem Sommersemester

Logik für Informatiker

- Schaltkreislogik
- Also: Nähe zur elektrotechnischen Umsetzung
- Aber auch: Universelle mathematische Verkehrssprache
- Denkschule

Logik: Wahr oder falsch?

Eine *Aussage* ist ein sprachliches Konstrukt, das wahr oder falsch sein kann.

Manchmal ist es leicht, den Wahrheitsgehalt einer Aussage herauszufinden:

1. Paris ist die Hauptstadt von Frankreich.
2. Mäuse sind bekannt dafür, Kängurus zu jagen.

Die erste Aussage ist *offenkundig* wahr, die zweite ist falsch.
Die *Offenkundigkeit* hängt von unserem Weltwissen ab, wir wollen hiervon im Folgenden abstrahieren.
Beobachte: Die beiden Aussagen lassen sich nicht (syntaktisch) in Teilaussagen zerlegen, sie sind vielmehr *atomar*.

Mathematische Aussagen

Wir betrachten die folgenden atomaren Aussagen:

- 2 ist Teiler von 12.
- 3 ist Teiler von 12.
- 4 ist Teiler von 12.
- 5 ist Teiler von 12.
- 6 ist Teiler von 12.
- 7 ist Teiler von 12.

Zwei dieser atomaren Aussagen sind falsch, die übrigen sind wahr.
Von den folgenden zusammengesetzten Aussagen ist nur eine falsch.

- 2 ist Teiler von 12 **oder** 5 ist Teiler von 12.
- 2 ist Teiler von 12 **und** 5 ist Teiler von 12.
- 2 **und** 3 sind Teiler von 12.
- **Falls** 2 Teiler von 12 ist, **dann** ist 4 Teiler von 12.
- **Falls** 5 Teiler von 12 ist, **dann** ist 2 Teiler von 12.
- 2 ist Teiler von 12 **oder** **sowohl** 5 **als auch** 6 sind Teiler von 12.

Vorsicht Umgangssprache

Die folgenden zwei zusammengesetzten Aussagen meinen offenbar dasselbe:

- 5 ist Teiler von 12 **und** 2 ist Teiler von 12.
- 2 ist Teiler von 12 **und** 5 ist Teiler von 12.

Umgangssprachlich ist das aber bei der “UND-Verknüpfung” der folgenden beiden atomaren Aussagen nicht der Fall:

- Otto wird krank.
- Der Arzt verordnet Otto Medizin.

Das UND hat in der Allgemeinsprache auch noch einen zeitlichen Aspekt. Dieser wird in der Aussagenlogik vernachlässigt.

Grundüberlegungen zur formalen Logik

Wir gehen davon aus, es gäbe eine Menge $\mathfrak{A}$ von *atomaren Formel*n.

Über einen Teil $\mathfrak{D} \subseteq \mathfrak{A}$ dieser Formeln “wissen wir Bescheid”, d.h., wir können eine Abbildung $\beta : \mathfrak{D} \to \{0, 1\}$ angeben mit der Bedeutung:

- $\beta(a) = 0$, falls a falsch ist;
- $\beta(a) = 1$, falls a wahr ist.

$\mathfrak{D}$ ist also eine Menge definierter Aussagen, und β ist eine *Belegungsfunktion*.
$\mathfrak{A} \setminus \mathfrak{D}$: *logische Variablen* oder *Unbestimmte*.
Wir wollen dann *zusammengesetzte Aussagen* untersuchen.
Wir beschreiben nun, was das formal bedeutet.

Formalitäten: Die Syntax der Aussagenlogik

(Aussagenlogische) Formeln werden durch einen induktiven Prozess definiert:

- Jede atomare Formel ist eine Formel.
  Formaler: Ist $F \in \mathfrak{A}$, so ist F eine Formel.
- Ist F eine Formel, so auch $\neg F$. *Negation von* F
- Sind F und G Formeln, so auch $(F \wedge G)$. *Konjunktion von* F *und* G

Eine Formel, die als Teil einer Formel in F auftritt, heißt *Teilformel* von F.
$\mathfrak{F}$ bezeichne die Gesamtheit aller aussagenlogischen Formeln (bzgl. $\mathfrak{A}$).

Beispiel: Sind A, B, C Formeln, so auch $F = \neg((\neg(A \wedge B) \wedge C) \wedge \neg C)$.
$(A \wedge B)$ ist eine Teilformel von F. $(A \wedge B) \wedge C$ ist keine Teilformel von F, ebensowenig $(B \wedge A)$.
Aufgabe: Wie sieht die Menge aller Teilformeln von F aus?
Muss eine Teilformel notgedrungen als Formel im induktiven Aufbau einer Formel auftreten?

Übliche Abkürzungen

Wir werden im Folgenden zwei weitere Elemente von Formeln als Abkürzungen bekannter Formeln kennenlernen.

- $(F \vee G)$ steht für $\neg(\neg F \wedge \neg G)$. *Disjunktion von* F *und* G
- $(F \rightarrow G)$ steht für $(\neg F \vee G)$. *Implikation*
- $(F \leftrightarrow G)$ steht für $((F \rightarrow G) \wedge (G \rightarrow F))$. *Äquivalenz*

Die Objekte $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ heißen auch *Junktoren*.
Sie dienen dazu, Teilformeln zu verbinden.
Aufgabe: Wofür steht $(F \leftrightarrow G)$ gemäß unserer ursprünglichen Formeldefinition?

Wir haben bislang nicht festgelegt, was diese Objekte bedeuten sollen.
Die Semantik der Aussagenlogik betrachten wir im Folgenden.

Wozu Formeln formal?

- Wir können einfach feststellen, ob eine Folge von Zeichen eine aussagenlogische Formel darstellt.
- Wir können dies auch programmieren.
- Daher kann ein Computer etwas mit Formeln als Eingabe anfangen.
- Ganz ähnlich kann man z.B. arithmetische Formeln (Ausdrücke, Terme) maschinell verarbeiten.
- Mehr dazu in Veranstaltungen wie “Automaten und Formale Sprachen” oder “Compilerbau”.

Die Semantik der Aussagenlogik: Was sollen die Formeln bedeuten?

$\{0, 1\}$ ist die Menge der *Wahrheitswerte*.
Ggb.: Menge $\mathfrak{A}$ atomarer Formeln, $\mathfrak{F}$ von Formeln (über den atomaren Formeln $\mathfrak{A}$);
Teilmenge $\mathfrak{D} \subseteq \mathfrak{A}$ mit Belegungsfunktion $\beta : \mathfrak{D} \to \{0, 1\}$.
$\mathfrak{E}$ bezeichne die aus $\mathfrak{D}$ aufbaubaren Formeln, also diejenigen Formeln aus $\mathfrak{F}$, die nur Elemente aus $\mathfrak{D}$ als atomare Formeln enthalten.
Wir erweitern β induktiv zu einer Belegungsfunktion $\widehat{\beta} : \mathfrak{E} \to \{0, 1\}$ wie folgt:

Ist $F \in \mathfrak{E}$ atomar, so setze $\widehat{\beta}(F) := \beta(F)$.
Andernfalls unterscheide zwei Fälle:

(a) $F = \neg G$. Setze $\widehat{\beta}(F) := \begin{cases} 0, & \widehat{\beta}(G) = 1 \\ 1, & \widehat{\beta}(G) = 0 \end{cases}$

(b) $F = (G \wedge H)$. Setze $\widehat{\beta}(F) := \begin{cases} 1, & \widehat{\beta}(G) = 1 \text{ und } \widehat{\beta}(H) = 1 \\ 0, & \text{sonst.} \end{cases}$

Nach dieser sauberen Definition werden wir auch für $\widehat{\beta}$ vereinfachend β schreiben.

Ein Beispiel

Es sei $\mathfrak{D} = \{p, q\}$ vorgegeben mit $\beta(p) = 1$ und $\beta(q) = 0$.
Betrachte die Formel $F = ((p \to q) \vee p)$. Was liefert $\beta(F)$?
1. Rückführen auf die ursprüngliche Definition:
F steht für $((\neg p \vee q) \vee p)$ oder $\neg(\neg\neg(\neg\neg p \wedge \neg q) \wedge \neg p)$.
2. Benutze die induktive Definition als rekursive Berechnungsvorschrift:
Um $\beta(F)$ zu berechnen, benötigen wir nach (a) $\beta(F')$ für $F' = (\neg\neg(\neg\neg p \wedge \neg q) \wedge \neg p)$.
Dazu bestimme wegen (b): $\beta(G')$ und $\beta(H')$ mit $G' = \neg\neg(\neg\neg p \wedge \neg q)$ und $H' = \neg p$.
Mit (a) und wegen $\beta(p) = 1$ folgt: $\beta(H') = 0$.
Die Definition der Semantik der Konjunktion zeigt, dass dann (unabh. von $\beta(G')$) $\beta(F') = 0$ gilt.
Wegen (a) folgt also: $\beta(F) = 1$.

Aufgabe: Berechnen Sie $\beta(G')$ (was wir uns ja “gespart” hatten).
In der Aufgabe auf Seite 10 hatten Sie im Grunde die Formel $J = (p \leftrightarrow q)$ “zurückgeführt”.
Berechnen Sie mit obiger Belegungsfunktion $\beta(J)$.

Semantische Begriffe

Ist F eine Formel, so bezeichne $\mathfrak{A}(F)$ die in F vorkommenden atomaren Formeln. Mit $\mathfrak{D} \subseteq \mathfrak{A}$ heißt $\beta : \mathfrak{D} \to \{0, 1\}$ *passend* zu F, falls $\mathfrak{A}(F) \subseteq \mathfrak{D}$. Ist β eine zu F passende Belegungsfunktion, so heißt β ein *Modell* für F, falls $\beta(F) = 1$. Man schreibt dann auch: $\beta \models F$. Zwei Formeln F und G heißen *(semantisch) äquivalent* gdw. für jede Belegungsfunktion β, die sowohl für F als auch für G passend ist, gilt: $\beta(F) = \beta(G)$. Man schreibt dafür auch: $F \equiv G$.

Satz: (*Idempotenz*) Für jede Formel F gilt: $F \equiv (F \wedge F)$.

Beweis: Da $\mathfrak{A}(F) = \mathfrak{A}((F \wedge F))$, können wir uns auf Belegungsfunktionen β mit $\mathfrak{D} = \mathfrak{A}(F)$ beschränken. Sei β solch eine passende Belegungsfunktion.

Gilt $\beta(F) = 1$, so ist nach Def. der Semantik der Konjunktion $\beta((F \wedge F)) = 1$.

Gilt $\beta(F) = 0$, so ist nach Def. der Semantik der Konjunktion $\beta((F \wedge F)) = 0$. $\square$

Rechenregeln für Junktoren

Lemma: (*Absorption*) $F \equiv (F \wedge (F \vee G))$.

Beweis: Nach Definition der Disjunktion gilt:

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

Sei nun β eine zu F und zu $H := (F \wedge \neg(\neg F \wedge \neg G))$ passende Belegung.

Fall 1.: Ist $\beta(F) = 1$, so gilt $\beta(\neg F) = 0$ und daher $\beta((\neg F \wedge \neg G)) = 0$, unabh. von $\beta(G)$.

Mithin ist $\beta(\neg(\neg F \wedge \neg G)) = 1$ und somit $\beta(H) = 1$.

Fall 2.: Ist $\beta(F) = 0$, so gilt $\beta(H) = 0$ unabh. von $\beta(\neg(\neg F \wedge \neg G))$.

Kein anderer Fall kann eintreten. $\square$

Die Art der soeben durchgeführten Fallunterscheidung kann man systematisieren durch die Betrachtung von *Wahrheitstafeln*.
Beobachte hierbei, dass nur die Belegung der in den Formeln vorkommenden atomaren Aussagen von Interesse für den Wahrheitsgehalt einer Formel ist.
Enthält also eine Formel n solche verschiedenen atomaren Aussagen, so sind 2^n viele Fälle zu unterscheiden.

Wahrheitstafeln für die Grund-Junktoren

- Negation:

$\beta(F)$	$\beta(\neg F)$
0	1
1	0

- Konjunktion:

$\beta(F)$	$\beta(G)$	$\beta(F \wedge G)$
0	0	0
0	1	0
1	0	0
1	1	1

Die Verwandtschaft zur Schaltkreislogik ist offenbar.

http://www.dietrichgrude.de/informatik/schaltlogik.htm

Wahrheitstafeln für abgeleitete Junktoren

- Disjunktion:

$\beta(F)$	$\beta(G)$	$\beta(F \vee G)$
0	0	0
0	1	1
1	0	1
1	1	1

, denn

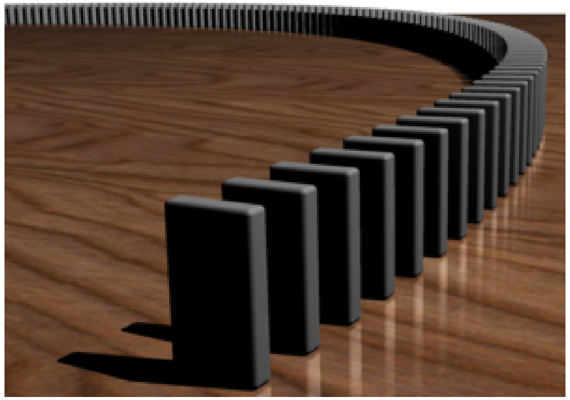
$\beta(F)$	$\beta(G)$	$\beta(\neg F)$	$\beta(\neg G)$	$\beta((\neg F \wedge \neg G))$	$\beta(\neg(\neg F \wedge \neg G))$
0	0	1	1	1	0
0	1	1	0	0	1
1	0	0	1	0	1
1	1	0	0	0	1

Aufgabe: Leiten Sie entsprechend die Wahrheitstafeln für $\rightarrow$ und $\leftrightarrow$ her.

Weitere Rechenregeln—Jetzt sind Sie dran!

Aufgabe: Beweisen Sie entsprechend die folgenden Sachverhalte:
Satz: (*Doppelte Negation*) Für jede Formel F gilt: $F \equiv \neg\neg F$.
Satz: (*Kommutativität*) Für alle Formeln F, G gilt: $(G \wedge F) \equiv (F \wedge G)$.

Zum Beweis können Sie entweder mit den Definitionen direkt argumentieren oder einen Wahrheitstafelbeweis führen.
Machen Sie sich klar, dass beide Beweisarten einander entsprechen.

Induktion veranschaulicht: Der Dominoeffekt: 

Die Aufstellung gewährleistet:
Wenn der k-te Dominostein in der Reihe fällt, so auch der $k + 1$-te.
Dies gewährleistet den Induktionsschritt.

Induktionsanfang: Jetzt fällt der erste Dominostein.

Folgerung: Schließlich werden alle Steine umgefallen sein.
Denn: zuerst fällt der erste, dann der zweite, dann der dritte, usf.

Eine logische Induktion

Lemma: Es sei n eine natürliche Zahl. Es sei F eine aussagenlogische Formel. Dann gilt für die Formeln

$$G_n := \underbrace{\neg \cdots \neg}_{n-\text{mal}} F \; :$$

(1) n ist gerade gdw. $F \equiv G_n$. (2) n ist ungerade gdw. $\neg F \equiv G_n$.

Beweis: Wir führen einen Beweis mit Hilfe der vollständigen Induktion.

Induktionsanfang: Für $n = 0$ und $n = 1$ gelten die Aussagen trivial.

Induktionshypothese (-voraussetzung): Wir nehmen an, die Aussage gilt für alle $n \leq m$.

Induktionsbehauptung: Die Aussage gilt für $n = m + 1$.

Betrachte daher $n = m + 1$. Klar: $n > 1$. Also gilt: $n - 2 \geq 0$ und $n - 2 < m$.

Außerdem ist n gerade gdw. $n - 2$ gerade.

Nach Definition gilt: $G_n = \neg\neg G_{n-2}$.

Nach dem Gesetz der doppelten Negation gilt: $G_n \equiv G_{n-2}$.

Nach Induktionsvoraussetzung (angewendet auf $n - 2 = m - 1$) folgt die Behauptung. $\square$

Die semantische Äquivalenz ist transitiv

Satz: Es seien F, G, H Formeln.
Gilt sowohl $F \equiv G$ als auch $G \equiv H$, dann gilt auch $F \equiv H$.

Beweis: Angenommen, sowohl $F \equiv G$ als auch $G \equiv H$ gelten.

Diskutiere eine beliebige, zu F und H passende Belegungsfunktion β.

β ist (zumindest) auf $D_{F,H} := \mathfrak{A}(F) \cup \mathfrak{A}(H)$ definiert. Setze $D_G := \mathfrak{G} \setminus D_{F,H}$.

Definiere nun $\overline{\beta}(p) := \begin{cases} \beta(p), & \text{falls } p \in D_{F,H} \\ 1, & \text{falls } p \in D_G \end{cases}$

Klar: $\overline{\beta}$ passt sowohl zu F als auch zu G als auch zu H.

Da $F \equiv G$ und $G \equiv H$, gilt ferner: $\overline{\beta}(F) = \overline{\beta}(G)$ und $\overline{\beta}(G) = \overline{\beta}(H)$.

Also ist $\overline{\beta}(F) = \overline{\beta}(H)$.

Diese Gleichheit wird nur durch die Belegung der atomaren Formeln in $D_{F,H}$ bedingt.

Daher gilt auch: $\beta(F) = \beta(H)$. Da β beliebig war, folgt $F \equiv H$. $\square$

De Morgansche Gesetze

Satz: Es seien F und G Formeln. Dann gilt:

$$\begin{aligned} \neg(F \wedge G) &\equiv (\neg F \vee \neg G) \\ \neg(F \vee G) &\equiv (\neg F \wedge \neg G) \end{aligned}$$

<u>Beweis:</u> Betrachte die Def. der Disjunktion sowie die Doppelte Negation:

$$\begin{aligned} \neg(F \wedge G) \equiv \neg(\neg\neg F \wedge \neg\neg G) &= (\neg F \vee \neg G) \\ \neg(F \vee G) = \neg\neg(\neg F \wedge \neg G) &\equiv (\neg F \wedge \neg G) \end{aligned}$$

$\square$

Weitere Übung: Geben Sie alternativ einen Beweis über Wahrheitstafeln an.

Assoziativität der Konjunktion

Satz: Es seien F, G, H Formeln. Dann gilt: $((F \wedge G) \wedge H) \equiv (F \wedge (G \wedge H))$.

Beweis: Wir führen einen Wahrheitstafelbeweis (vollständige Fallunterscheidung):

$\beta(F)$	$\beta(G)$	$\beta(H)$	$\beta((F \wedge G))$	$\beta(((F \wedge G) \wedge H))$	$\beta((G \wedge H))$	$\beta((F \wedge (G \wedge H)))$
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	0	1	0
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	1	0	0	0
1	1	1	1	1	1	1

$\square$

Hilfsüberlegung zum Ersetzbarkeitsstheorem

Lemma: Es seien F, G Formeln. Dann gilt $F \equiv G$ gdw. $\neg F \equiv \neg G$.

Beweis: Zunächst beobachte, dass D eine zu F und G passende Menge elementarer Formeln ist gdw. D zu $\neg F$ und zu $\neg G$ passt.

Sei β eine zu F und G (und somit zu $\neg F$ und $\neg G$) passende Belegung.

Gilt $\beta(F) = \beta(G)$, so gilt $\beta(\neg F) = \beta(\neg G)$ und umgekehrt (Def. der Semantik der Negation).

Daher gilt die Behauptung. $\square$

Das Ersetzbarkeitsstheorem

Satz: Es seien F, G, H Formeln. Es sei $F \equiv G$ und F sei eine Teilformel von H.
H' entstehe durch Ersetzen von einem Vorkommen von F durch G.
Dann gilt: $H \equiv H'$.

Beweis: Wir führen einen Induktionsbeweis über die Anzahl n der Junktoren in H.

Induktionsanfang: $n = 0$. D.h., H enthält gar keine Junktoren. Also ist H atomar. Daher muss $H = F$ sein. Daher gilt: $H' = G$. Nach Voraussetzung gilt: $F \equiv G$, also ist $H \equiv H'$.

Induktionsvoraussetzung: Die Aussage gilt für alle Junktorenanzahlen $n \leq m$.

Induktionsbehauptung: Dann gilt die Aussage für $n = m + 1 > 0$.

Gilt $H = F$, so folgt die Behauptung mit derselben Argumentation wie im Induktionsanfang.

Der Beweis vom Ersetzbarkeitsstheorem (Forts.)

Wir sind im Induktionsschritt.
Andernfalls gilt, da H nicht atomar: $H = \neg H_1$ oder $H = (H_1 \wedge H_2)$.
Beachte: H_1 und H_2 enthalten höchstens m Junktoren und F ist Teilformel von H_1 (oder von H_2).
Falls $H = \neg H_1$, so gilt für die aus H_1 durch Ersetzen von einem Vorkommen von F durch G entstehende Formel H_1' nach Induktionsvoraussetzung: $H_1 \equiv H_1'$. Wegen des vorigen Lemmas folgt: $H \equiv H'$ mit $H' = \neg H_1'$.
Sei nun $H = (H_1 \wedge H_2)$. Betrachte den Fall, dass ein Vorkommen von F in H_1 durch G ersetzt wird und so die Formel H_1' aus H_1 entsteht.
(Eine Ersetzung eines Vorkommens von F in H_2 kann man entsprechend diskutieren.)
Dann gilt nach Induktionsvoraussetzung: $H_1' \equiv H_1$. Betrachte $H' = (H_1' \wedge H_2)$.

Aufgabe: Zeige abschließend, dass $H' \equiv H$. $\square$

Ergänzungen zum Ersetzbarkeitsstheorem (zur Übung)

Satz: Es seien $F_1, \ldots, F_n$ Formeln. Angenommen, es gilt:

$$F_1 \equiv F_2, F_2 \equiv F_3, \ldots, F_{n-1} \equiv F_n.$$

Dann gilt: $F_i \equiv F_j$ für alle $1 \leq i < j \leq n$. (*verallg. Transitivität der Äquivalenz*)

Hinweis: Induktionsbeweis.

Satz: Es seien F, G, H Formeln. Es sei $F \equiv G$ und F sei eine Teilformel von H. H' entstehe durch Ersetzen von einem oder mehreren Vorkommen von F durch G. Dann gilt: $H \equiv H'$.

Hinweis: Induktionsbeweis mit Ersetzbarkeitsstheorem und dem vorigen Satz.

Satz: Es seien F und G äquivalente Formeln mit den Junktoren $\wedge$, $\vee$ und $\neg$. F' entstehe aus F (und entsprechend entstehe G' aus G) durch konsequentes Ersetzen von $\wedge$ durch $\vee$ und umgekehrt. Dann gilt: $F' \equiv G'$. (*Dualitätssatz*)

Hinweis: Induktionsbeweis.

Wie kann man die Gesetze anwenden?

Aus dem Dualitätssatz folgt sofort:

- Das Kommutativitätsgesetz der Disjunktion.
- Das Assoziativitätsgesetz der Disjunktion.
- Ein zweites Absorptionsgesetz: $F \equiv (F \vee (F \wedge G))$.
- Es gelten zweierlei Distributivgesetze:

$$\begin{array}{rcl} ((F \vee G) \wedge H) & \equiv & ((F \wedge H) \vee (G \wedge H)) \\ ((F \wedge G) \vee H) & \equiv & ((F \vee H) \wedge (G \vee H)) \end{array}$$

  Es genügt, eines der Gesetze durch Wahrheitstafelbeweis nachzuweisen (Dualität).

Logik-Algebra: Rechengesetze im Überblick

Satz: $(a \wedge b) \rightarrow a$; $(a \wedge b) \rightarrow b$; $a \rightarrow (a \vee b)$ sind Tautologien (s.u.).

Satz: $a \vee a \equiv a \wedge a \equiv a$.

Satz: $a \vee b \equiv b \vee a$; $a \wedge b \equiv b \wedge a$. (Kommutativität)

Satz: $(a \vee b) \vee c \equiv a \vee (b \vee c)$; $(a \wedge b) \wedge c \equiv a \wedge (b \wedge c)$. (Assoziativität)

Satz: $(a \vee b) \wedge c \equiv (a \wedge c) \vee (b \wedge c)$; $(a \wedge b) \vee c \equiv (a \vee c) \wedge (b \vee c)$. (Distributivität)

Aufgabe: Machen Sie sich sämtliche Aussagen an “möglichst allgemeinen” Beispielen klar.

Boolesche Algebra

- Vergleichen Sie die Rechengesetze aus der Logik-Algebra mit denen der Mengenalgebra.
- Diese sehen “ganz genauso aus”. $\cap$ “entspricht” $\wedge$; $\cup$ “entspricht” $\vee$.
- Das ist kein Zufall.
- Man kann allgemeiner “Boolesche Algebren” betrachten.
- Man kann Mengen über Eigenschaften beschreiben.
  Beispiel: $X := \{n \in \mathbb{N} : 2|n\}$, $Y := \{n \in \mathbb{N} : 3|n\}$, $Z := \{n \in \mathbb{N} : 6|n\}$.
  Es gilt: $Z = X \cap Y = \{n \in \mathbb{N} : (2|n) \wedge (3|n)\}$.

Unerfüllbarkeit bzw. Tautologie

Eine Formel F heißt eine *Tautologie*, falls jede zu F passende Belegungsfunktion ein Modell für F ist.

Eine Formel F heißt *unerfüllbar*, falls F kein Modell besitzt.

Satz: Eine Formel F ist genau dann gültig, wenn $\neg F$ unerfüllbar ist.

Beweis: F ist Tautologie gdw.

jede zu F (und somit zu $\neg F$) passende Belegungsfunktion ein Modell für F ist gdw.

keine zu $\neg F$ passende Belegungsfunktion ist ein Modell für $\neg F$ gdw.

$\neg F$ hat kein Modell gdw. $\neg F$ ist unerfüllbar. $\square$

Beispiel: $(F \wedge \neg F)$ ist für jede Formel F unerfüllbar.

Mehr zur Übung Es seien F und G Formeln.

- Ist F eine Tautologie, so gilt:

$$\begin{aligned} F &\equiv (F \vee G) \\ G &\equiv (F \wedge G) \end{aligned}$$

- Ist F unerfüllbar, so gilt:

$$\begin{aligned} G &\equiv (F \vee G) \\ F &\equiv (F \wedge G) \end{aligned}$$

Eine Anwendung

Es seien A, B, C Formeln.
Dann gilt: $((A \vee (B \vee C)) \wedge (C \vee \neg A)) \equiv ((B \wedge \neg A) \vee C)$.

<u>Beweis:</u> Wir benutzen unsere hergeleiteten Regeln.

$$
\begin{aligned}
((A \vee (B \vee C)) \wedge (C \vee \neg A)) &\overset{\text{AG/ET}}{\equiv} (((A \vee B) \vee C) \wedge (C \vee \neg A)) \\
&\overset{\text{KG/ET}}{\equiv} ((C \vee (A \vee B)) \wedge (C \vee \neg A)) \\
&\overset{\text{DG}}{\equiv} (C \vee ((A \vee B) \wedge \neg A)) \\
&\overset{\text{DG/ET}}{\equiv} (C \vee ((A \wedge \neg A) \vee (B \wedge \neg A))) \\
&\overset{\text{unerf./ET}}{\equiv} (C \vee (B \wedge \neg A)) \\
&\overset{\text{KG}}{\equiv} ((B \wedge \neg A) \vee C)
\end{aligned}
$$

Die Behauptung folgt mit der verallgemeinerten Transitivität der Äquivalenz. □

Aufgabe: Überprüfen Sie auf Äquivalenz: $(A \to (B \to C))$ und $((A \to B) \to C)$.

Mehr aus der Logik

- Formale Logik ist eine der Grundlagen der Informatik.
- Es gibt zwei Zugänge zu Beweisen über logische Sachverhalte:
  - Semantische Ebene: Argumentiere über Belegungen.
  - Syntaktische Ebene: Kalküle / Algorithmen zum Nachweis der Wahrheit von Formeln.
    Das klappt (erstaunlicherweise) für die Aussagenlogik.
    Es gibt Algorithmen zum “Nachrechnen” der Gültigkeit von Formeln der Aussagenlogik.
- Erweiterungen durch Quantoren $\forall$ (für alle) und $\exists$ (es gibt).
  Damit lässt sich viel mehr ausdrücken.
  Allerdings gibt es keine Algorithmen zur Beantwortung der Gültigkeitsfrage für Formeln.

Was sollte zumindest hängenbleiben?

Wie liest man Formeln, die mit logischen Symbolen gespickt sind?

- $x \wedge y$: x gilt und y gilt;
- $\neg x$: x gilt nicht
- $x \vee y$: x gilt oder (auch) y;
- $x \rightarrow y$: wenn x gilt, so gilt auch y;
- $x \leftrightarrow y$: x gilt genau dann, wenn y gilt.
- $\forall x$: für alle x gilt;
- $\exists x$: für ein x gilt.

Die “Hausaufgaben” sind in die Foliensammlung integriert.

Sie finden Sie auf den Folien Seite 9, Seite 10, Seite 13, Seite 17, Seite 18, (Seite 26), Seite 27, Seite 29, Seite 32, Seite 33.

Kurz zur Literatur:
Das meiste von der Veranstaltung heute finden Sie in:
Uwe Schöning: Logik für Informatiker. Spektrum Lehrbuch.