Diskrete Strukturen in der Informatik

Aussagenlogik

PD Dr. Stefan Milius

WS 2015/2016

Überblick

Inhalt

1. Aussagen- und Prädikatenlogik
2. Naive Mengenlehre
3. Relationen und Funktionen
4. Kombinatorik und Stochastik
5. Algebraische Strukturen
6. Bäume und Graphen
7. Arithmetik

Überblick

Fähigkeiten

- Standardnotation lesen und schreiben
- Einführung mathematisches Denken
- Beweise lesen und analysieren
- (formale) Beweise führen

Vorlesungsziele

heutige Vorlesung

1. Einführung Aussagenlogik
2. Äquivalenz von komplexen Aussagen
3. Tautologien und Unerfüllbarkeit

Bitte Fragen direkt stellen!

Organisation

Organisation

Materialien

- Folien und Ankündigungen im OLAT-Kurs:

  W15.Inf.DiskreteStrukturen

- Literatur (Selbststudium und Vertiefung):

  CHRISTOPH MEINEL, MARTIN MUNDHENK
  Mathematische Grundlagen der Informatik
  Vieweg+Teubner, 5. Auflage, 2011

  ANGELIKA STEGER
  Diskrete Strukturen — Band 1
  Kombinatorik, Graphentheorie, Algebra
  Springer-Verlag, 2. Auflage, 2007

Organisation

Vorlesung

dienstags, 17:15–18:45 Uhr, Hörsaal 2

Übungen

- Übungsgruppen (jede Woche):

Wochentag	Zeit	Raum	Übungsleiter
Montag	11:15	SG 3-13	Hannes Strass
Dienstag	11:15	SG 3-13	Doreen Heusel
Dienstag	13:15	SG 3-13	Raj Dahya
Mittwoch	13:15	SG 3-14	Frank Loebe
Freitag	9:15	SG 2-14	Matthias Waack
Freitag	11:15	SG 3-14	Matthias Waack
Freitag	13:15	SG 3-13	Raj Dahya

- keine Übung: 12.–16.10., 18.11., 02.12.
  — bitte Alternativtermin in der gleichen Woche wählen

Organisation

Übungen

- Hausaufgabenkontrolle: Matti Berthold, Hannes Thalheim,
- Übungs- und Hausaufgabenblätter im OLAT
  $\rightarrow$ richtige Email-Adresse im OLAT hinterlegen!
- bitte für Übungsgruppe im AlmaWeb anmelden
  $\rightarrow$ Weiterleitung von Nachrichten an Email-Adresse einstellen!

Sprechstunden ...

... nach Vereinbarung mit den Übungsgruppenleitern / dem Dozenten.

Workload + Modulabschluss

Workload

2+2 SWS bzw. 5 ECTS
(Workload = 150 h, d.h. 60 h (Präsenz) + 90 h (eigenständig))

Modulabschluss

- erfolgreiches Lösen der Hausaufgaben !
- Abgabe der Hausaufgaben vor der Vorlesung
  (Abgabedatum steht auf dem Aufgabenblatt)
- $\geq$ 50% Punkte als Prüfungsvoraussetzung
- 60-/90-minütige benotete Abschlussklausur ergibt Modulnote
- maximal 15% Bonuspunkte durch Hausaufgaben

Danksagung

Die Folien basieren auf Folien von Dr. A. Maletti aus dem WS 2014/2015.

Ihm möchten wir hiermit herzlich danken!

Grundlagen der Logik

Inhalt

Aussagenlogik — Beispiel

StVO I, § 30(3) — Sonn- und Feiertagsfahrverbot [editiert]

An Sonn- und Feiertagen dürfen in der Zeit 0.00–22.00 Uhr Lastkraftwagen mit einer zulässigen Gesamtmasse über 7,5 t sowie Anhänger hinter Lastkraftwagen nicht verkehren. Dies gilt nicht für

1. [. . .] und/oder
2. die Beförderung von
   - a frischer Milch und frischen Milcherzeugnissen,
   - b frischem Fleisch und frischen Fleischerzeugnissen,
   - c frischen Fischen, lebenden Fischen und frischen Fischerzeugn.,
   - d leicht verderblichem Obst und Gemüse, und/oder
3. Leerfahrten im Zusammenhang mit Fahrten nach 2, und/oder
4. [. . .]

Aussagenlogik — Aussagen

§1.1 Definition (Aussage)

Eine Aussage ist eine Repräsentation eines Satzes,
der entweder wahr (1) oder falsch (0) ist

(genau ein Wahrheitswert, auch wenn evtl. unbekannt)

Beispiele

- *"L befördert frische Milch"* ist eine Aussage

  für einen geg. Lastkraftwagen L
- *"D ist ein Feiertag"* ist eine Aussage

  für ein geg. Datum D
- *"2 ist eine Primzahl"* ist eine wahre Aussage
- "$2 + 2 = 5$" ist eine falsche Aussage

Aussagenlogik — Aussagen

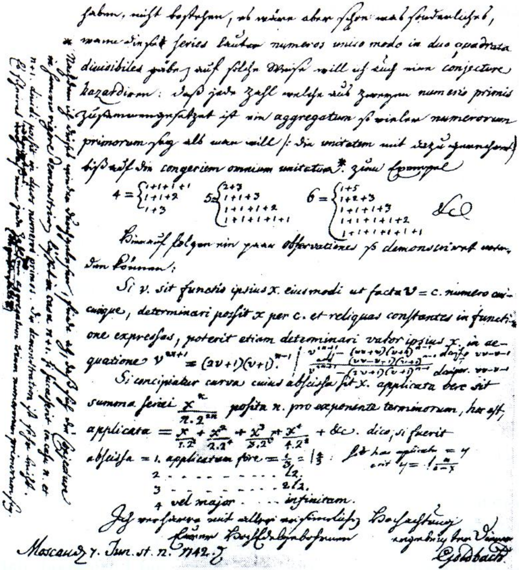
weiteres Beispiel: GOLDBACHs Vermutung (1742)

"Jede gerade natürliche Zahl $n > 2$ ist die Summe zweier Primzahlen"

ist eine Aussage — Wahrheitswert unbekannt

CHRISTIAN GOLDBACH (* 1690; † 1764)

- studierte Medizin und Jura in Königsberg
- erlernte später Mathematik
- Tutor von Zar PETER II



haben, nicht beystehen, ob wäre aber schon mal sonderlich, wann dergleichen series lauter numeros unico modo in duo quadrata divisibiles gäben, auf solche Weise will ich auch eine conjecture hazardiren: daß jede Zahl welche aus zweyen numeris primis zusammengesetzt ist ein aggregatum so vieler numerorum primorum sey als man will (die unitatem mit dazu gerechnet) bis auf die congeriem omnium unitatum*. zum Exempel

$$4 = \begin{cases} 1+1+1+1 \\ 1+1+2 \\ 1+3 \end{cases} \quad 5 = \begin{cases} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{cases} \quad 6 = \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1+3 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{cases} \quad \&c.$$

Hierauf folgen ein paar observationes so demonstrirt werden können:

Si v. sit functio ipsius x. eiusmodi ut facta v = c. numero cuicunque, determinari possit x per c. et reliquas constantes in functione expressas, poterit etiam determinari valor ipsius x. in aequatione ...

Si concipiatur curva cujus abscissa sit x. applicata vero sit summa seriei $\frac{x^n}{n.2^n}$ posita n. pro exponente terminorum, hoc est, applicata $= \frac{x}{1.2} + \frac{x^2}{2.2^2} + \frac{x^3}{3.2^3} + \frac{x^4}{4.2^4} + \&c.$ dico, si fuerit abscissa = 1. applicatam fore = l2.

Ich verharre mit aller ersinnlichen Hochachtung
Euer Hochedelgebohren
ergebenster Diener
Goldbach

Moscau d. 7. Jun. st. n. 1742.

Aussagenlogik — Aussagen

weiteres Beispiel: Selbstreferenz

"Dieser Satz ist falsch."

ist keine Aussage

kann weder wahr noch falsch sein!

Aussagenlogik — Junktoren

Gegenstand der Logik

- nicht die Wahrheitsbestimmung von Basis-Aussagen
  (dies ist Aufgabe der Fachgebiete)
- Formalisierung von (komplexen) Aussagenverknüpfungen
- Bewertung von Aussagenverknüpfungen
  basierend auf Wahrheitswerten der Teilaussagen
- Schlussregeln

Notation (Junktoren)

- (Basis-)Aussagen $A, B, C, \ldots$ aber auch "hatFisch"
- Negation $\neg A$ — nicht A
- Konjunktion $A \wedge B$ — A und B
- Disjunktion $A \vee B$ — A oder B
- Implikation $A \rightarrow B$ — wenn A, dann B

Aussagenlogik — Junktoren

Erklärungsversuch Notation

- Konjunktion $A \wedge B$ — A **und** B
  - entspricht $A \cap B$ (unten offen)
  - Elemente von $A \cap B$ müssen in A und B liegen
- Disjunktion $A \vee B$ — A **oder** B
  - entspricht $A \cup B$ (oben offen)
  - Elemente von $A \cup B$ müssen in A oder B liegen

§1.2 Interpretation

- Jede Aussage (auch jede Aussagenverknüpfung) ist entweder wahr (1) oder falsch (0)
- Wahrheit von Aussagenverknüpfungen ergibt sich aus Wahrheit der Teilaussagen gemäß folgender Tabelle

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

Aussagenlogik — Junktoren

Schwierigkeit: Implikation

- $A \to B$ besteht aus Vorbedingung A und Folgerung B
- $A \to B$ ist genau dann falsch, wenn die Vorbedingung A gilt, aber die Folgerung B nicht

Beispiel

- "Wenn es regnet, dann nehme ich den Schirm mit."
- Formalisierung: Regen $\to$ Schirm
- wenn es nicht regnet, dann kann ich den Schirm mitnehmen oder daheim lassen (Vorbedingung nicht erfüllt)
- wenn es regnet und ich den Schirm nicht mitnehme, dann gilt die Aussage Regen $\to$ Schirm nicht

Aussagenlogik — Syntax und Semantik

§1.3 Definition

- (aussagenlogische) Atome = Basis-Aussagen wie A, B etc.
- (aussagenlogische) Formeln = Aussagen mit Verknüpfungen

Notizen

- Wahrheit eines Atoms abhängig von fachlicher “Aussage”
- Wahrheit einer Formel ist nur abhängig von der Wahrheit ihrer Atome

Aussagenlogik — Wahrheitswertetabelle

Interesse

- wir sind an wahren Aussagen (sog. Theoremen) interessiert

→ Erkenntnisgewinn und Verständnis der Welt

Nachweis

- die Wahrheit einer Aussage muss erst nachgewiesen werden

→ Beweis

Wahrheitswertetabelle

- einfachste Beweismethode
- Nachweis der Wahrheit der Aussage
  unabh. von der Wahrheit ihrer Atome

Aussagenlogik — Wahrheitswertetabelle

Wahrheitswertetabelle

- Beweisschema für komplexe Aussagen
- tabellarische Auflistung aller Möglichkeiten
- funktioniert evtl. nicht bei Abhängigkeiten zwischen Aussagen

§1.4 Beispiel

- "Wenn A und B gelten, dann gilt A."
- dabei können A und B beliebig komplexe Aussagen sein
- Formalisierung: $(A \wedge B) \rightarrow A$
- Beweis durch Wahrheitswertetabelle:

A	B	$A \wedge B$	$(A \wedge B) \rightarrow A$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	1

Aussagenlogik — Wahrheitswertetabelle

§1.5 Beispiel

- "Eine natürliche Zahl, die nicht ungerade ist, ist gerade."
- Formalisierung: $\neg U \to G$
- Fachwissen: "Jede natürliche Zahl ist gerade oder ungerade."
- neue Formalisierung: $(U \vee G) \to (\neg U \to G)$

Beweis.

Beweis mit Wahrheitswertetabelle (mit Fachwissen):

U	G	$U \vee G$	$\neg U$	$\neg U \to G$	$(U \vee G) \to (\neg U \to G)$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	1	1
1	1	1	0	1	1

□

Aussagenlogik — Formalisierung

StVO I, § 30(3) — Sonn- und Feiertagsfahrverbot [editiert]

[. . .] Dies gilt nicht für

1. [. . .]
2. die Beförderung von
   - a frischer Milch und frischen Milcherzeugnissen,
   - b frischem Fleisch und frischen Fleischerzeugnissen,
   - c frischen Fischen, lebenden Fischen und frischen Fischerzeugn.,
   - d leicht verderblichem Obst und Gemüse,

[. . .]

Formalisierung

- $\neg((\text{hatMilch} \wedge \text{hatMilchE}) \wedge (\text{hatFleisch} \wedge \text{hatFleischE}) \wedge \cdots)$
- $\neg((\text{hatMilch} \vee \text{hatMilchE}) \wedge (\text{hatFleisch} \vee \text{hatFleischE}) \wedge \cdots)$
- $\neg((\text{hatMilch} \wedge \text{hatMilchE}) \vee (\text{hatFleisch} \wedge \text{hatFleischE}) \vee \cdots)$
- $\neg((\text{hatMilch} \vee \text{hatMilchE}) \vee (\text{hatFleisch} \vee \text{hatFleischE}) \vee \cdots)$

Aussagenlogik — Formalisierung

hM	hME	hF	hFE	hM $\wedge$ hME	hF $\wedge$ hFE	hM $\vee$ hME	hF $\vee$ hFE
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	0	0	1
0	0	1	1	0	1	0	1
0	1	0	0	0	0	1	0
0	1	0	1	0	0	1	1
0	1	1	0	0	0	1	1
0	1	1	1	0	1	1	1
1	0	0	0	0	0	1	0
1	0	0	1	0	0	1	1
1	0	1	0	0	0	1	1
1	0	1	1	0	1	1	1
1	1	0	0	1	0	1	0
1	1	0	1	1	0	1	1
1	1	1	0	1	0	1	1
1	1	1	1	1	1	1	1

Frage

Welche (weiteren) Beweistechniken kennen Sie?

Mögliche Antworten

- beidseitige Implikationen
- Implikationskette
- Ringschluss
- indirekter Beweis
- Kontraposition
- vollständige Induktion
- ...

Äquivalenz

Aussagenlogik — Äquivalenz

§1.6 Definition (Äquivalenz)

Zwei Aussagen A und B sind äquivalent (geschrieben: $A \leftrightarrow B$), genau dann wenn (gdw.) ihre Wahrheitswerte übereinstimmen

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
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 — Äquivalenz

Beispiele

- $U \vee G$ und $\neg U \rightarrow G$ sind äquivalent (siehe §1.5)
- $A \vee B$ und $A \rightarrow B$ sind nicht äquivalent (siehe §1.2)

äquivalente Formeln		Bezeichnung
$A \wedge B$	$B \wedge A$	Kommutativität von $\wedge$
$A \vee B$	$B \vee A$	Kommutativität von $\vee$
$(A \wedge B) \wedge C$	$A \wedge (B \wedge C)$	Assoziativität von $\wedge$
$(A \vee B) \vee C$	$A \vee (B \vee C)$	Assoziativität von $\vee$
$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$	Distributivität von $\wedge$
$A \vee (B \wedge C)$	$(A \vee B) \wedge (A \vee C)$	Distributivität von $\vee$
$A \wedge A$	A	Idempotenz von $\wedge$
$A \vee A$	A	Idempotenz von $\vee$
$\neg\neg A$	A	Involution $\neg$
$\neg(A \wedge B)$	$(\neg A) \vee (\neg B)$	deMorgan-Gesetz für $\wedge$
$\neg(A \vee B)$	$(\neg A) \wedge (\neg B)$	deMorgan-Gesetz für $\vee$

§1.7 Theorem

$F_1 = A \vee (B \wedge C)$ und $F_2 = (A \vee B) \wedge (A \vee C)$ sind äquivalent

Beweis.

Mit Wahrheitswertetabelle:

A	B	C	$B \wedge C$	F_1	$A \vee B$	$A \vee C$	F_2	$F_1 \leftrightarrow F_2$
0	0	0	0	0	0	0	0	1
0	0	1	0	0	0	1	0	1
0	1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1	1
1	0	1	0	1	1	1	1	1
1	1	0	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1

$\square$

Aussagenlogik — Äquivalenz

Vorsicht

$F_1 = (A \to B) \to C$ und $F_2 = A \to (B \to C)$
sind nicht äquivalent.

Beweis.

Mit Wahrheitswertetabelle:

A	B	C	$A \to B$	F_1	$B \to C$	F_2	$F_1 \leftrightarrow F_2$
0	0	0	1	$\boxed{0}$	1	$\boxed{1}$	$\boxed{0}$
...	...	...	...	...	...	...	

□

§1.8 Beweisprinzip: beidseitige Implikationen

- die Aussage $A \leftrightarrow B$ entspricht "$A \rightarrow B$ und $B \rightarrow A$" $(A \leftarrow B)$
- formal: $(A \leftrightarrow B) \leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$
- um $A \leftrightarrow B$ zu zeigen, reicht es $A \rightarrow B$ und $B \rightarrow A$ zu zeigen

Beweis dieser Aussage

$$F = (A \leftrightarrow B) \leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$$

A	B	$A \leftrightarrow B$	$A \rightarrow B$	$B \rightarrow A$	$(A \rightarrow B) \wedge (B \rightarrow A)$	F
0	0	1	1	1	1	1
0	1	0	1	0	0	1
1	0	0	0	1	0	1
1	1	1	1	1	1	1

Aussagenlogik — Äquivalenz

§1.9 Äquivalenzen für $\rightarrow$ und $\leftrightarrow$

- $A \rightarrow B$ und $\neg A \vee B$ sind äquivalent
- $A \leftrightarrow B$ und $(A \rightarrow B) \wedge (B \rightarrow A)$ sind äquivalent (siehe §1.8)

Beweis.

Mit Wahrheitswertetabelle:

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

□

§1.10 Substitutionsprinzip

äquivalente Formeln können füreinander substituiert werden

$\leadsto$ Beweisprinzip: Äquivalenzkette

§1.11 Theorem (Beweisprinzip: Kontraposition)

$A \to B$ und $\neg B \to \neg A$ sind äquivalent
(“wenn A, dann B” entspricht “wenn nicht B, dann nicht A”)

Beweis.

Folge äquivalenter Formeln: (Äquivalenzkette)

	$A \to B$	
gdw.	$\neg A \lor B$	§1.9
gdw.	$\neg A \lor \neg\neg B$	Inv. $\neg$
gdw.	$\neg\neg B \lor \neg A$	Komm. $\lor$
gdw.	$\neg B \to \neg A$	§1.9

□

§1.12 Theorem

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

Beweis.

Kontraposition von QuadratGerade $\to$ ZahlGerade:

$$\neg\text{ZahlGerade} \to \neg\text{QuadratGerade}$$

Falls n nicht gerade ist, dann gilt $n = 2k + 1$ für ein $k \in \mathbb{Z}$ und

$$n^2 = (2k+1)^2 = (2k)^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1 \ ,$$

womit n^2 wieder ungerade (nicht gerade) ist.

(nutzt auch Fachwissen und Implikationskette — siehe später) $\square$

Aussagenlogik — Vereinfachung

Beispiel

[. . .] Dies gilt

$$\neg((\text{hatMilch} \vee \text{hatMilchE}) \vee (\text{hatFleisch} \vee \text{hatFleischE}) \vee \cdots)$$

Vereinfachung

$$\begin{aligned}
& \neg((\text{hatMilch} \vee \text{hatMilchE}) \vee (\text{hatFleisch} \vee \text{hatFleischE})) \\
\text{gdw.} \quad & \neg(\text{hatMilch} \vee \text{hatMilchE}) \wedge \neg(\text{hatFleisch} \vee \text{hatFleischE}) \\
\text{gdw.} \quad & \neg\text{hatMilch} \wedge \neg\text{hatMilchE} \wedge \neg\text{hatFleisch} \wedge \neg\text{hatFleischE}
\end{aligned}$$

Aussagenlogik — Vereinfachung

Vereinfachung — weiteres Beispiel

$$
\begin{array}{ll}
 & (A \wedge B) \vee (A \wedge C) \wedge A \\
\text{gdw.} & A \wedge (B \vee C) \wedge A \\
\text{gdw.} & A \wedge A \wedge (B \vee C) \\
\text{gdw.} & A \wedge (B \vee C)
\end{array}
$$

Tautologien

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

§1.14 Theorem (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 □

Aussagenlogik — Schlusskette

§1.15 Theorem

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

(Transitivität von $\to$)

Beweis.

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

Fallunterscheidung:

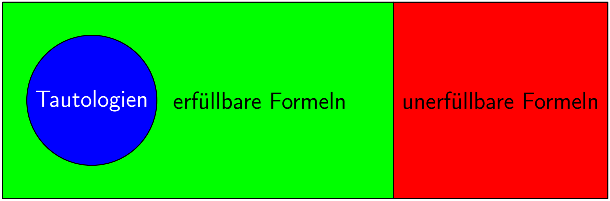
- Falls $\neg(A \to C)$ falsch ist, dann ist F wahr.
- Falls $\neg(A \to C)$ wahr ist, dann ist $A \to C$ falsch,
  daraus folgen: A wahr und C falsch
  - Sei B falsch. Dann ist $A \to B$ falsch und damit F' wahr
  - Sei B wahr. Dann ist $B \to C$ falsch und damit F' wahr

  Da F' wahr ist, ist auch F wahr $\square$

Aussagenlogik — Tautologien

Notizen

- Schlussregeln sollten immer Tautologien sein
  z.B. $(A \to B) \leftrightarrow (\neg B \to \neg A)$ — Kontraposition
- jede Tautologie ist erfüllbar
- Vorsicht mit der Negation:
  1. $\neg F$ ist unerfüllbar für jede Tautologie F
     ($\neg F$ ist für jede Belegung falsch)
  2. F kann erfüllbar sein, falls F keine Tautologie ist
     (F ist nicht für jede Belegung wahr)



Zusammenfassung

- Aussagenlogische Formeln und Interpretation
- Äquivalenz
- Tautologien und Erfüllbarkeit
- Grundlegende Beweistechniken

Erste Übungsserie wird demnächst im OLAT publiziert.