

# Formale Grundlagen der Informatik 1

## Kapitel 14

### Folgerbarkeit, Äquivalenzen und Normalformen

Frank Heitmann  
heitmann@informatik.uni-hamburg.de

24. Mai 2016

# Syntax

## Definition (Syntax der Aussagenlogik)

Mit  $AS_{AL}$  sei die Menge der *Aussagensymbol* der Aussagenlogik bezeichnet. Wir notieren diese üblicherweise als  $A_1, A_2, A_3, \dots$  oder  $A, B, C, \dots$

Die Menge  $\mathcal{L}_{AL}$  der Formeln der Aussagenlogik definieren wir mittels

- 1 Jedes  $A \in AS_{AL}$  ist eine (atomare) Formel.
- 2 Ist  $F$  eine Formel, so ist auch  $\neg F$  eine (komplexe) Formel.
- 3 Sind  $F$  und  $G$  Formeln, so sind auch  $(F \vee G)$ ,  $(F \wedge G)$ ,  $(F \Rightarrow G)$  und  $(F \Leftrightarrow G)$  (komplexe) Formeln.
- 4 Es gibt keine anderen Formeln, als die, die durch *endliche Anwendungen* der Schritte 1-3 erzeugt werden.

# Semantik

## Definition (Semantik der Aussagenlogik)

Eine **Belegung** ist eine Funktion  $\mathcal{A}_{AS} : AS_{AL} \rightarrow \{0, 1\}$ , die jedem Aussagesymbol einen Wahrheitswert zuordnet.

Zu dieser wird rekursiv eine Funktion,  $\mathcal{A} : \mathcal{L}_{AL} \rightarrow \{0, 1\}$  definiert, die alle Formeln bewertet (wird ebenfalls Belegung genannt). Für jedes  $A \in AS_{AL}$  ist  $\mathcal{A}(A) = \mathcal{A}_{AS}(A)$  und für alle Formeln  $F, G \in \mathcal{L}_{AL}$  sei

- $\mathcal{A}(\neg F) = 1$  genau dann, wenn  $\mathcal{A}(F) = 0$
- $\mathcal{A}((F \vee G)) = 1$  gdw.  $\mathcal{A}(F) = 1$  oder  $\mathcal{A}(G) = 1$
- $\mathcal{A}((F \wedge G)) = 1$  gdw.  $\mathcal{A}(F) = 1$  und  $\mathcal{A}(G) = 1$
- $\mathcal{A}((F \Rightarrow G)) = 1$  gdw.  $\mathcal{A}(F) = 0$  oder  $\mathcal{A}(G) = 1$
- $\mathcal{A}((F \Leftrightarrow G)) = 1$  gdw.  $\mathcal{A}(F) = \mathcal{A}(G)$

# Semantik - Wahrheitstafeln

**Wahrheitstafeln** geben für die atomaren Formeln alle möglichen Belegungen an und für die anderen Formeln die entsprechenden Bewertungen. Sie stellen die Definition von eben übersichtlich dar.

$A$	$B$	$\neg A$	$A \vee B$	$A \wedge B$	$A \Rightarrow B$	$A \Leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	1	0	1	0
1	0	0	1	0	0	0
1	1	0	1	1	1	1

## Wichtige Anmerkung

Hier und auf den nachfolgenden Folien verwenden wir bereits Klammerersparnisregeln. Wir führen diese später auch noch genauer ein. Insb. lassen wir äussere Klammern weg.

# Semantik - Wahrheitstafeln - Vorgehen

## Vorgehen

Will man zu einer komplexen Formeln  $F$  eine Wahrheitstafel aufbauen, so

- notiert man links in der Tafel alle (verschiedenen) Aussagensymbole, die in  $F$  auftreten und
- geht diese zeilenweise von “alle auf 0 setzen” bis “alle auf 1 setzen” durch (am besten indem man binär durchzählt).
- Dann zerlegt man  $F$  am Hauptoperator und notiert die beiden oder im Falle der Negation die eine Teilformel in der Tafel. Mit dieser/n Formel/n macht man dann weiter und zerlegt sie wieder am Hauptoperator.
- Dann bestimmt man für jede der (Teil-)Formeln den Wahrheitswert ausgehend von den bereits berechneten Werten der Teilformeln.
- Zuletzt ergibt sich der Wahrheitswerteverlauf von  $F$

## Wahrheitstafel - Beispiel

## Beispiel

Ein Beispiel für die Formel  $F := C \Leftrightarrow ((A \wedge B) \Rightarrow (\neg A \vee B))$

$A$	$B$	$C$	$\neg A$	$A \wedge B$	$\neg A \vee B$	$(A \wedge B) \Rightarrow (\neg A \vee B)$	$F$
0	0	0	1	0	1	1	0
0	0	1	1	0	1	1	1
0	1	0	1	0	1	1	0
0	1	1	1	0	1	1	1
1	0	0	0	0	0	1	0
1	0	1	0	0	0	1	1
1	1	0	0	1	1	1	0
1	1	1	0	1	1	1	1

# Kategorien

## Definition

- Eine Belegung heißt **passend** zu einer Formel  $F$ , wenn sie jedem Aussagesymbol in  $F$  einen Wahrheitswert zuweist.
- Eine Belegung  $\mathcal{A}$  mit  $\mathcal{A}(F) = 1$  nennt man ein **Modell** für  $F$  oder eine *erfüllende Belegung* von  $F$ . Ist  $\mathcal{A}(F) = 0$ , so ist  $\mathcal{A}$  eine *falsifizierende Belegung* von  $F$ .
- Ist ferner  $M$  eine (evtl. sogar unendliche) Formelmenge. So nennt man eine Belegung  $\mathcal{A}$ , die alle Formeln  $F$  aus  $M$  wahr macht, ebenfalls ein *Modell* für  $M$  und schreibt dafür bisweilen auch kurz  $\mathcal{A}(M) = 1$ .
- Zudem ist jede Belegung Modell der leeren Menge. Die leere Menge ist also erfüllbar.

# Kategorien

## Definition

- Besitzt  $F$  mindestens eine erfüllende Belegung (ein Modell)  $\mathcal{A}$ , so heißt  $F$  **erfüllbare** Formel. Notation:  $\mathcal{A} \models F$
- Besitzt  $F$  mindestens eine falsifizierende Belegung  $\mathcal{A}$ , so heißt  $F$  **falsifizierbare** Formel. Notation:  $\mathcal{A} \not\models F$
- Besitzt  $F$  mindestens eine erfüllende und mindestens eine falsifizierende Belegung so heißt  $F$  **kontingente** Formel.
- Besitzt  $F$  kein Modell, so heißt  $F$  **unerfüllbare** Formel oder **Kontradiktion**. Notation:  $F \models$
- Ist  $F$  unter jeder möglichen Belegung „wahr“, so heißt  $F$  **(allgemein-)gültig** oder **Tautologie**. Notation:  $\models F$

# Fragen

Ist die folgende Wahrheitstafel korrekt?

$A$	$B$	$\neg B$	$A \Leftrightarrow B$	$A \Rightarrow B$	$\neg B \Rightarrow A$
0	0	1	1	1	0
0	1	0	0	1	1
1	0	1	0	0	1
1	1	0	1	1	0

- ① Ja!
- ② Nein!
- ③ Nein! Fehler in ...
- ④ Ich seh' da nur 0en und 1en ...

# Fragen

Sei  $K$  eine Kontradiktion,  $T$  eine Tautologie und  $F$  eine kontingente Formel, was ist dann

$$(K \vee F) \wedge T$$

- 1 Unerfüllbar!
- 2 Allgemeingültig!
- 3 Kontingent!
- 4 Weiß ich nicht ...

# Fragen

Sei  $K$  eine Kontradiktion,  $T$  eine Tautologie und  $F$  eine kontingente Formel, was ist dann

$$(K \wedge F) \vee T$$

- ① Unerfüllbar!
- ② Allgemeingültig!
- ③ Kontingent!
- ④ Weiß ich nicht ...

# Zur Nachbereitung

## Zur Nachbereitung

- 1 Fehler in der letzten Spalte, letzten Zeile
- 2 Kontingenz
- 3 Allgemeingültig

# Folgerung

## Definition (Folgerung)

Eine Formel  $F$  **folgt** genau dann aus einer Formelmenge  $M$ , wenn jede Belegung, die Modell für  $M$  ist, auch Modell für  $F$  ist.

Notation:  $M \models F$ .

## Anmerkung

Im Falle einer einelementigen Menge  $M = \{G\}$  notiert man auch  $G \models F$  und sagt,  $F$  **folgt** aus  $G$ .

# Folgerung: Beispiel 1

## Definition (Folgerung)

Eine Formel  $F$  **folgt** genau dann aus einer Formelmenge  $M$ , wenn jede Belegung, die Modell für  $M$  ist, auch Modell für  $F$  ist.

Beweis von  $A \wedge B \models A \vee B$  mit Wahrheitstafel:

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

Jede Belegung, die Modell für  $A \wedge B$  ist (nur die vierte Zeile) ist auch Modell für  $A \vee B$ , daher gilt  $A \wedge B \models A \vee B$ . (Das  $A \vee B$  auch woanders wahr ist, ist egal!)

## Folgerung: Beispiel 2

Beweis von  $\{A \Rightarrow B, B \Rightarrow C\} \models A \Rightarrow C$  mit Wahrheitstafel:

$A$	$B$	$C$	$A \Rightarrow B$	$B \Rightarrow C$	$A \Rightarrow C$
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	1	0
1	0	1	0	1	1
1	1	0	1	0	0
1	1	1	1	1	1

Jede Belegung, die Modell für  $A \Rightarrow B$  **und** Modell für  $B \Rightarrow C$  ist (erste, zweite, vierte und achte Zeile) ist auch Modell für  $A \Rightarrow C$ , also gilt die Folgerbarkeitsbeziehung.

## Folgerung: Beispiel 3

Beweis von  $A \wedge B \wedge C \wedge D \models C \vee \neg D$  ohne Wahrheitstafel:

Sei  $\mathcal{A}$  ein Modell für  $A \wedge B \wedge C \wedge D$ . Nach der semantischen Definition von  $\wedge$  muss dann  $\mathcal{A}(A) = \mathcal{A}(B) = \mathcal{A}(C) = \mathcal{A}(D) = 1$  gelten womit wegen  $\mathcal{A}(C) = 1$  und der Definition der Semantik von  $\vee$  auch  $\mathcal{A}(C \vee \neg D) = 1$  gilt. Folglich ist jedes Modell von  $A \wedge B \wedge C \wedge D$  auch Modell von  $C \vee \neg D$ .

# Äquivalenz

## Definition (Äquivalenz)

Zwei Formeln  $F$  und  $G$  heißen **äquivalent** genau dann, wenn jede Belegung beiden Formeln den gleichen Wahrheitswert zuweist, wenn also  $\mathcal{A}(F) = \mathcal{A}(G)$  für jede Belegung  $\mathcal{A}$  gilt.

Notation:  $F \equiv G$ .

## Anmerkung

- 1 Alternativ: Zwei Formeln sind genau dann äquivalent, wenn sie dieselben Modelle besitzen, also  $\mathcal{A}(F) = 1$  gdw.  $\mathcal{A}(G) = 1$  gilt.
- 2 Äquivalente Formeln haben denselben Wahrheitswerteverlauf!

## Äquivalenz: Beispiel 1

Beweis von  $A \Leftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$  mit Wahrheitstafel:

$A$	$B$	$A \Leftrightarrow B$	$A \wedge B$	$\neg A \wedge \neg B$	$(A \wedge B) \vee (\neg A \wedge \neg B)$
0	0	1	0	1	1
0	1	0	0	0	0
1	0	0	0	0	0
1	1	1	1	0	1

In der dritten und letzten Spalte sieht man, dass  $A \Leftrightarrow B$  und  $(A \wedge B) \vee (\neg A \wedge \neg B)$  den gleichen Wahrheitswerteverlauf haben. Damit sind die beiden Formeln äquivalent.

## Äquivalenz: Beispiel 2

Widerlegung von  $A \wedge B \equiv A \vee B$  durch Angabe eines Gegenbeispiels:

$A \wedge B$  und  $A \vee B$  sind nicht äquivalent, da z.B.  $\mathcal{A}$  mit  $\mathcal{A}(A) = 0$  und  $\mathcal{A}(B) = 1$  zwar ein Modell von  $A \vee B$  nicht aber eines von  $A \wedge B$  ist. Damit haben die beiden Formeln nicht die gleichen Modelle und sind damit nicht äquivalent.

### Wichtige Anmerkung

Ebenso widerlegt man Folgerbarkeitsbeziehungen  $F \models G$  durch Angabe eines Gegenbeispiels also durch Angabe einer Belegung  $\mathcal{A}$ , die Modell für  $F$  ist, aber nicht für  $G$ .

# Wichtige Äquivalenzen

Kommutativität:	$(F \wedge G) \equiv (G \wedge F)$	$(F \vee G) \equiv (G \vee F)$
Assoziativität:	$(F \wedge (G \wedge H)) \equiv ((F \wedge G) \wedge H)$	$(F \vee (G \vee H)) \equiv ((F \vee G) \vee H)$
Distributivität:	$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H))$	$(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H))$
Doppelnegation:	$\neg\neg F \equiv F$	
de Morgans Regeln:	$\neg(F \wedge G) \equiv (\neg F \vee \neg G)$	$\neg(F \vee G) \equiv (\neg F \wedge \neg G)$
Elimination von $\Leftrightarrow$ :	$(F \Leftrightarrow G) \equiv (F \Rightarrow G) \wedge (G \Rightarrow F)$	$(F \Leftrightarrow G) \equiv (F \wedge G) \vee (\neg F \wedge \neg G)$
Elimination von $\Rightarrow$ :	$(F \Rightarrow G) \equiv (\neg F \vee G)$	

# Weitere wichtige Äquivalenzen

$$\begin{aligned} \text{Absorption:} \quad & (F \wedge (F \vee G)) \equiv F \\ & (F \vee (F \wedge G)) \equiv F \end{aligned}$$

$$\begin{aligned} \text{Idempotenz:} \quad & (F \wedge F) \equiv F \\ & (F \vee F) \equiv F \end{aligned}$$

$$\begin{aligned} \text{Tautologieregeln} \quad & (F \wedge \top) \equiv F \\ & (F \vee \top) \equiv \top \end{aligned}$$

$$\begin{aligned} \text{Kontradiktionsregeln:} \quad & (F \wedge \perp) \equiv \perp \\ & (F \vee \perp) \equiv F \end{aligned}$$

$$\begin{aligned} \text{Komplement:} \quad & (F \wedge \neg F) \equiv \perp \\ & (F \vee \neg F) \equiv \top \end{aligned}$$

# Anmerkung

## Wichtige Anmerkung

- 1 Auf der letzten Folien waren  $\perp$  und  $\top$  Konstanten. Man müsste sie streng formal als neue syntaktische Konstrukte einführen. Sie sind dann atomare Formeln, die immer zu 0 (bei  $\perp$ ) bzw. immer zu 1 (bei  $\top$ ) ausgewertet werden.
- 2 Alle obigen Äquivalenzen kann man z.B. mit Wahrheitstafeln schnell beweisen.

# Klammerersparnisregeln

Aufgrund der Äquivalenzen können wir uns auf folgende Regeln zur Klammerersparnis einigen:

- 1 Die äußersten Klammern entfallen:  $A \vee B$  statt  $(A \vee B)$
- 2 Bei mehrfacher Konjunktion oder Disjunktion entfällt die mehrfache Klammerung:  
$$((A \vee B) \vee C) \equiv (A \vee (B \vee C)) \equiv A \vee B \vee C$$
- 3 Weiterhin **nicht** erlaubt sind  $A \Rightarrow B \Rightarrow C$  oder  $A \vee B \wedge C$

## Bemerkung

In einigen Büchern findet man auch die Regel, dass  $\neg$  am stärksten bindet, dann  $\wedge$  und  $\vee$  und als dritte  $\Rightarrow$  und  $\Leftrightarrow$ . Damit wäre dann z.B. auch  $A \wedge B \Rightarrow C$  möglich. Wir wollen dies i.A. aber nicht benutzen. Eine Ausnahme sind Hornformeln in Implikationsschreibweise, zu denen wir später noch kommen.

# Folgerung und Äquivalenz (Wdh.)

## Definition (Folgerung)

Eine Formel  $F$  **folgt** genau dann aus einer Formelmenge  $M$ , wenn jede Belegung, die Modell für  $M$  ist, auch Modell für  $F$  ist.

Notation:  $M \models F$  bzw.  $G \models F$ , wenn  $M = \{G\}$ .

## Definition (Äquivalenz)

Zwei Formeln  $F$  und  $G$  heißen **äquivalent** genau dann, wenn jede Belegung beiden Formeln den gleichen Wahrheitswert zuweist, wenn also  $\mathcal{A}(F) = \mathcal{A}(G)$  für jede Belegung  $\mathcal{A}$  gilt.

Notation:  $F \equiv G$ .

# Fragen

Wenn  $F \equiv G$  und  $\models G$  gilt, dann gilt auch  $\models F$

- 1 Ja!
- 2 Nein!
- 3 Weiß ich nicht ...

# Fragen

Wenn  $F \models$  und  $G \models$  gilt, dann gilt  $F \equiv G$

- 1 Ja!
- 2 Nein!
- 3 Weiß ich nicht ...

# Einige Sätze

## Satz

- 1 Wenn  $F \equiv G$  und  $\models G$  gilt, dann gilt auch  $\models F$
- 2 Wenn  $F \equiv G$  und  $G \models$  gilt, dann gilt auch  $F \models$
- 3 Wenn  $\models F$  und  $\models G$  gilt, dann gilt  $F \equiv G$
- 4 Wenn  $F \models$  und  $G \models$  gilt, dann gilt  $F \equiv G$

## Beweis.

1. und 4. nachfolgend. 2. und 3. in den Präsenzaufgaben.

# Einige Sätze

## Satz

*Wenn  $F \equiv G$  und  $\models G$  gilt, dann gilt auch  $\models F$ .*

## Beweis.

Sie  $\mathcal{A}$  eine zu  $F$  und  $G$  passende Belegung. Da  $G$  eine Tautologie ist, gilt  $\mathcal{A}(G) = 1$ . Da ferner  $F \equiv G$  gilt, gilt  $\mathcal{A}(F) = \mathcal{A}(G)$ , also auch  $\mathcal{A}(F) = 1$ . Damit ist jede Belegung Modell für  $F$  und folglich  $F$  eine Tautologie. □

# Einige Sätze

## Satz

Wenn  $F \models$  und  $G \models$  gilt, dann gilt  $F \equiv G$

## Beweis.

Wir zeigen, dass  $\mathcal{A}(F) = \mathcal{A}(G)$  für jede Belegung  $\mathcal{A}$  gilt. Sei dazu  $\mathcal{A}$  eine zu  $F$  und  $G$  passende Belegung. Da sowohl  $F$  als auch  $G$  Kontradiktionen sind, gilt stets  $\mathcal{A}(F) = \mathcal{A}(G) = 0$  womit bereits alles gezeigt ist. □

# Sätze mit Folgerbarkeit

## Satz

$F \equiv G$  genau dann, wenn  $F \models G$  und  $G \models F$

## Beweis.

Sei  $F \equiv G$  und sei  $\mathcal{A}$  ein Modell für  $F$ . Wegen  $F \equiv G$  ist  $\mathcal{A}$  auch ein Modell für  $G$  und damit gilt  $F \models G$ . Analog gilt auch  $G \models F$ . Gelte nun andersherum  $F \models G$  und  $G \models F$  und sei  $\mathcal{A}$  ein Modell für  $F$ . Wegen  $F \models G$  gilt dann auch  $\mathcal{A}(G) = 1$ . Ist  $\mathcal{A}'$  ein Modell für  $G$ , dann ist  $\mathcal{A}'$  wegen  $G \models F$  auch ein Modell für  $F$ . Damit haben  $F$  und  $G$  genau dieselben Modelle und folglich gilt  $F \equiv G$ . □

# Drei wichtige Sätze

## Satz

- 1  $F \equiv G$  genau dann, wenn  $\models F \Leftrightarrow G$
- 2  $F \models G$  genau dann, wenn  $\models F \Rightarrow G$
- 3  $F \models G$  genau dann, wenn  $F \wedge \neg G \models$

## Beweis.

1. ist Präsenzaufgabe. Zu 2: Gelte  $F \models G$  und sei  $\mathcal{A}$  eine zu  $F$  und  $G$  passende Belegung. Ist  $\mathcal{A}(F) = 0$ , so ist  $\mathcal{A}(F \Rightarrow G) = 1$  aufgrund der Definition der Semantik von  $\Rightarrow$ . Ist  $\mathcal{A}(F) = 1$ , so ist wegen  $F \models G$  auch  $\mathcal{A}(G) = 1$  und damit wieder  $\mathcal{A}(F \Rightarrow G) = 1$  und folglich gilt  $\models F \Rightarrow G$ .

Sei umgekehrt  $\models F \Rightarrow G$  und sei  $\mathcal{A}$  ein Modell für  $F$ . Wegen der Definition der Semantik von  $\Rightarrow$  folgt aus  $\mathcal{A}(F \Rightarrow G) = 1$  (es gilt ja  $\models F \Rightarrow G$ ) sofort  $\mathcal{A}(G) = 1$  und damit ist jedes Modell von  $F$  auch Modell von  $G$  und wir sind fertig.  $\square$

# Drei wichtige Sätze

## Satz

- 1  $F \equiv G$  genau dann, wenn  $\models F \Leftrightarrow G$
- 2  $F \models G$  genau dann, wenn  $\models F \Rightarrow G$
- 3  $F \models G$  genau dann, wenn  $F \wedge \neg G \not\models$

## Beweis.

3. folgt aus 2. sofort aus der Äquivalenz  $F \Rightarrow G \equiv \neg F \vee G$  und da die Negation einer Tautologie eine Kontradiktion ist (und umgekehrt) und da  $\neg(\neg F \vee G) \equiv F \wedge \neg G$ . □

# Verallgemeinerung

Die Aussagen

- 1  $F \models G$  genau dann, wenn  $\models F \Rightarrow G$
- 2  $F \models G$  genau dann, wenn  $F \wedge \neg G \models$

können verallgemeinert werden. Sei  $M$  eine beliebige Formelmenge, dann gilt:

- 1  $M \cup \{F\} \models G$  genau dann, wenn  $M \models F \Rightarrow G$
- 2  $M \models G$  genau dann, wenn  $M \cup \{\neg G\}$  unerfüllbar ist.

Dabei ist eine Formelmenge unerfüllbar, wenn es keine Belegung gibt, die alle Formeln der Menge wahr macht.

# Alle Sätze im Überblick

## Satz

- 1 Wenn  $F \equiv G$  und  $\models G$  gilt, dann gilt auch  $\models F$
- 2 Wenn  $F \equiv G$  und  $G \models$  gilt, dann gilt auch  $F \models$
- 3 Wenn  $\models F$  und  $\models G$  gilt, dann gilt  $F \equiv G$
- 4 Wenn  $F \models$  und  $G \models$  gilt, dann gilt  $F \equiv G$
- 5  $F \equiv G$  genau dann, wenn  $F \models G$  und  $G \models F$
- 6  $F \equiv G$  genau dann, wenn  $\models F \Leftrightarrow G$
- 7  $F \models G$  genau dann, wenn  $\models F \Rightarrow G$
- 8  $F \models G$  genau dann, wenn  $F \wedge \neg G \models$
- 9  $M \cup \{F\} \models G$  genau dann, wenn  $M \models F \Rightarrow G$
- 10  $M \models G$  genau dann, wenn  $M \cup \{\neg G\}$  unerfüllbar ist.

# Normalformen

Wir wollen jetzt

- die Äquivalenzen nutzen, um Teilformeln zu ersetzen und
- so zu einer Normalform kommen

Die Normalform hat verschiedene Vorteile:

- Einfach strukturiert (daher gut für Beweis, Algorithmen, ...)
- Eigenschaften lassen sich bisweilen leichter ablesen/ermitteln.

# Ersetzungen

Unser Ziel ist es zunächst Teilformeln ersetzen zu dürfen, also aus

$$A \wedge (B \Rightarrow C)$$

z.B.

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

zu machen. Die Rechtfertigung dafür wird die Äquivalenz  $B \Rightarrow C \equiv \neg B \vee C$  sein. Dass wir dies tatsächlich in Teilformeln so ersetzen dürfen, sagt uns das *Ersetzbarkeitstheorem*.

# Ersetzbarkeitstheorem

## Satz (Ersetzbarkeitstheorem)

*Seien  $F$  und  $G$  äquivalente Formeln und sei  $H$  eine Formel mit (mindestens) einem Vorkommen der Formel  $F$  als Teilformel. Gehe  $H'$  aus  $H$  hervor, indem ein Vorkommen von  $F$  (in  $H$ ) durch  $G$  ersetzt wird. Dann sind  $H$  und  $H'$  äquivalent.*

Ersetzt man also eine Teilformel  $F$  einer Formel  $H$  durch eine äquivalente Formel, so ist die entstehende Formel  $H'$  zur ursprünglichen  $H$  äquivalent.

Der Satz ist die Rechtfertigung für die Schreibweise  
 $A \wedge (B \Rightarrow C) \equiv A \wedge (\neg B \vee C)$ .

Der Beweis erfolgt nun mittels struktureller Induktion...

# Beweis des Ersetzbarkeitstheorems

## Beweis

**Induktionsanfang.** Sei  $H$  eine atomare Formel und gehe  $H'$  durch Ersetzen von  $F$  durch  $G$  aus  $H$  hervor. Dann muss  $H = F$  und  $H' = G$  gelten und aus  $F \equiv G$  folgt dann sofort  $H = F \equiv G = H'$  also  $H \equiv H'$ .

**Induktionsannahme.** Wir nehmen an, dass  $H_1$  und  $H_2$  Formeln sind, für die gilt: Für jede Formel  $H'_1$  bzw.  $H'_2$ , die durch Ersetzung von  $F$  durch  $G$  aus  $H_1$  bzw.  $H_2$  hervorgegangen ist, gilt  $H_1 \equiv H'_1$  bzw.  $H_2 \equiv H'_2$ .

# Beweis des Ersetzbarkeitstheorems

**Induktionsschritt.** Ist  $F = H$ , so verfahren wir wie im Induktionsanfang und sind fertig. Nachfolgend genügt es also den Fall zu betrachten, dass  $F$  eine echte Teilformel von  $H$  ist.

Fall  $H = \neg H_1$ . Dann ist  $F$  eine Teilformel von  $H_1$  und es gibt  $H'_1$ , das aus  $H_1$  durch Ersetzen von  $F$  durch  $G$  entsteht und so, dass  $H' = \neg H'_1$  gilt. Nach Induktionsannahme gilt  $H_1 \equiv H'_1$ . Sei nun  $\mathcal{A}$  eine beliebige Belegung. Dann ist  $\mathcal{A}(H'_1) = \mathcal{A}(H_1)$  wegen  $H_1 \equiv H'_1$  und wegen der Definition der Semantik von  $\neg$  ist dann auch  $\mathcal{A}(\neg H'_1) = \mathcal{A}(\neg H_1)$  also auch  $\mathcal{A}(H) = \mathcal{A}(H')$  und damit  $H \equiv H'$ .

# Beweis des Ersetzbarkeitstheorems

**Induktionsschritt (Fortsetzung).** Fall  $H = H_1 \vee H_2$ .

Angenommen  $F$  ist eine Teilformel von  $H_1$  (der andere Fall ist analog). Dann gibt es wieder ein  $H'_1$ , das aus  $H_1$  durch Ersetzen von  $F$  durch  $G$  entsteht und so, dass  $H' = H'_1 \vee H_2$  gilt. Nach Induktionsannahme gilt  $H_1 \equiv H'_1$ . Sei nun  $\mathcal{A}$  eine beliebige Belegung. Dann ist  $\mathcal{A}(H'_1) = \mathcal{A}(H_1)$  wegen  $H_1 \equiv H'_1$  und ähnlich wie eben folgt wegen der Definition der Semantik von  $\vee$  dann  $\mathcal{A}(H') = \mathcal{A}(H'_1 \vee H_2) = \mathcal{A}(H_1 \vee H_2) = \mathcal{A}(H)$  und damit  $H' \equiv H$ . Die anderen Fälle gehen ganz analog, was den Beweis abschließt.

## Anmerkung

Wichtig ist hier, dass  $\mathcal{A}(H'_1 \vee H_2) = \mathcal{A}(H_1 \vee H_2)$  gilt. Dies folgt aus der Definition von  $\vee$  und wegen  $\mathcal{A}(H'_1) = \mathcal{A}(H_1)$ . Man überlegt sich, was passiert, wenn die einzelnen Teilformeln zu 0 oder 1 ausgewertet werden und dass tatsächlich immer das gleiche rauskommt.

# Beweis des Ersetzbarkeitstheorems

## Anmerkung

Um es genau auszuführen: Mit  $\mathcal{A}(H'_1) = \mathcal{A}(H_1)$  ist

$$\mathcal{A}(H'_1 \vee H_2) = \mathcal{A}(H_1 \vee H_2)$$

denn, wenn  $\mathcal{A}(H'_1) = 1$  gilt, dann ist

$$\mathcal{A}(H'_1 \vee H_2) = \mathcal{A}(H'_1) = 1 = \mathcal{A}(H_1) = \mathcal{A}(H_1 \vee H_2)$$

(insb. da hier der Wert von  $\mathcal{A}(H_2)$  irrelevant ist) und wenn  $\mathcal{A}(H'_1) = 0$  gilt, dann ist

$$\mathcal{A}(H'_1 \vee H_2) = \mathcal{A}(H_2) = \mathcal{A}(H_1 \vee H_2)$$

(letzteres insb. da  $\mathcal{A}(H_1) = \mathcal{A}(H'_1) = 0$  gilt).

# Äquivalenzumformungen

## Ergebnis

Wir dürfen nun dank des Ersetzbarkeitstheorems Teilformeln durch andere Formeln ersetzen, sofern diese zu der gewählten Teilformel äquivalent sind.

$$\neg A \Rightarrow \neg\neg B \equiv \neg A \Rightarrow B \equiv \neg\neg A \vee B \equiv A \vee B$$

# Normalformen - Motivation

Wir wollen nun eine **Normalform** für aussagenlogische Formeln einführen, d.h. eine Form

- in die wir jede aussagenlogische Formel durch Äquivalenzumformungen bringen können und
- die eine praktische Form hat (z.B. für Berechnungen)

Dazu erst ein paar Begriffe ...

# Normalformen - Begriffe

## Definition

- 1 Ein **Literal** ist eine atomare Formel oder eine negierte atomare Formel.
- 2 Ein **positives Literal** ist eine atomare Formel, ein **negatives Literal** eine negierte atomare Formel.
- 3 Zwei Literale heißen **komplementär**, wenn sie positives und negatives Literal der gleichen atomaren Formel sind. Bspw. ist  $A$  das komplementäre Literal zu  $\neg A$  und umgekehrt.
- 4 Literale und Disjunktionen von Literalen werden als **Klauseln** bezeichnet.
- 5 Literale und Konjunktionen von Literalen werden als **duale Klauseln** bezeichnet.

# Normalformen - Begriffe 2

## Definition

- 1 Eine Formel  $F$  ist in **konjunktiver Normalform** (KNF), wenn sie eine Konjunktion von Klauseln ist, also eine Konjunktion von Disjunktionen von Literalen, z.B.

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

- 2 Eine Formel  $F$  ist in **disjunktiver Normalform** (DNF), wenn sie eine Disjunktion von dualen Klauseln ist, also eine Disjunktion von Konjunktionen von Literalen, z.B.

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

# Eigenschaften der KNF und DNF

## Merkhilfe

KNF:  $(\neg A \vee B \vee \neg C) \wedge B \wedge (\neg C \vee \neg B)$

DNF:  $(A \wedge B) \vee (\neg A \wedge \neg C) \vee (B \wedge \neg A \wedge C)$

## Satz

- 1 Eine KNF ist gültig gdw. alle ihre Klauseln gültig sind gdw. in allen Klauseln mindestens ein Paar komplementäre Literale vorkommt.
- 2 Eine DNF ist unerfüllbar gdw. alle ihre dualen Klauseln unerfüllbar sind gdw. in allen dualen Klauseln mindestens ein Paar komplementäre Literale vorkommt.
- 3 Ein Erfüllbarkeitstest für DNFs ist effizient implementierbar (Laufzeit ist in  $P$ ). (Für KNFs gilt dies wahrscheinlich nicht! SAT ist NP-vollständig.)

# KNF und DNF

## Satz

*Zu jeder Formel  $F$  gibt es (mindestens) eine konjunktive Normalform und (mindestens) eine disjunktive Normalform, d.h. es gibt Formeln  $K$  in konjunktiver Normalform und  $D$  in disjunktiver Normalform mit  $F \equiv K \equiv D$ .*

# Verfahren für die Erstellung von KNF und DNF

- 1 Ersetze alle Teilformeln der Form
  - $(G \Leftrightarrow H)$  durch  $(\neg G \vee H) \wedge (\neg H \vee G)$  [Elimination von  $\Leftrightarrow$ ]
  - $(G \Rightarrow H)$  durch  $(\neg G \vee H)$  [Elimination von  $\Rightarrow$ ]
- 2 Ersetze alle Teilformeln der Form
  - $\neg\neg G$  durch  $G$  [Doppelte Negation]
  - $\neg(G \wedge H)$  durch  $(\neg G \vee \neg H)$  [de Morgan]
  - $\neg(G \vee H)$  durch  $(\neg G \wedge \neg H)$  [de Morgan]
- 3 Um die KNF zu bilden ersetze alle Teilformeln der Form
  - $(F \vee (G \wedge H))$  durch  $((F \vee G) \wedge (F \vee H))$  [Distributivität]
  - $((F \wedge G) \vee H)$  durch  $((F \vee H) \wedge (G \vee H))$  [Distributivität]
- 4 Um die DNF zu bilden ersetze alle Teilformeln der Form
  - $(F \wedge (G \vee H))$  durch  $((F \wedge G) \vee (F \wedge H))$  [Distributivität]
  - $((F \vee G) \wedge H)$  durch  $((F \wedge H) \vee (G \wedge H))$  [Distributivität]

## Beispiel

$$(A \wedge (B \Rightarrow C)) \Rightarrow D$$

$$\equiv (A \wedge (\neg B \vee C)) \Rightarrow D$$

$$\equiv \neg(A \wedge (\neg B \vee C)) \vee D$$

$$\equiv (\neg A \vee \neg(\neg B \vee C)) \vee D$$

$$\equiv (\neg A \vee (\neg\neg B \wedge \neg C)) \vee D$$

$$\equiv (\neg A \vee (B \wedge \neg C)) \vee D$$

$$\equiv ((\neg A \vee B) \wedge (\neg A \vee \neg C)) \vee D$$

$$\equiv ((\neg A \vee B) \vee D) \wedge ((\neg A \vee \neg C) \vee D)$$

$$\equiv (\neg A \vee B \vee D) \wedge (\neg A \vee \neg C \vee D)$$

Elimination von  $\Rightarrow$ Elimination von  $\Rightarrow$ 

de Morgan

de Morgan

Doppelte Negation

Distributivität

Distributivität

Klammern

# Zusammenfassung

Heute haben wir

- Folgerbarkeit und Äquivalenz eingeführt
  - Nachweis mit Wahrheitstafeln
  - Nachweis ohne Wahrheitstafeln
  - Gegenbeispiel (mit und ohne Wahrheitstafeln)
- etliche Sätze zur Folgerbarkeit und Äquivalenz gesehen
- das Ersetzbarkeitstheorem eingeführt und mit struktureller Induktion bewiesen
- Literal, Klausel, duale Klausel, DNF und KNF definiert
- gesehen, wie ein KNF und DNF hergestellt werden kann

Nächstes Mal:

- Beweisen wir formal die Existenz von KNF und DNF
- lernen noch ein zweites Verfahren zur Herstellung der KNF und DNF kennen
- ...