

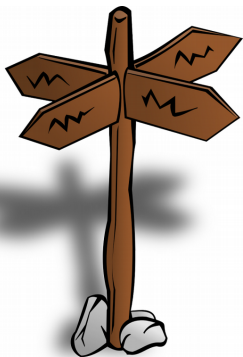
Aussagenlogik

Grundzüge digitaler Systeme

Vortrag von: Martin Riener

Aussagenlogik – Übersicht

- Aussagenlogik
- Aussagenlogische Funktionen
- Syntax und Semantik der Aussagenlogik
- Das Erfüllbarkeitsproblem
- Beispiel Dr. House
- Beispiel Gone Maggie gone



Klassische Aussagenlogik (Propositionallogik)

- zwei Wahrheitswerte: wahr/falsch, true/false, verum/falsum, 1/0, ein/aus, ...
- Aussagenvariablen, die wahr oder falsch sein können
- elementare Operatoren wie „und“, „oder“, „nicht“, ...
- keine Quantoren

Geht zurück auf die Antike

Grundlegend für

- Philosophie
- Mathematik
- Informatik



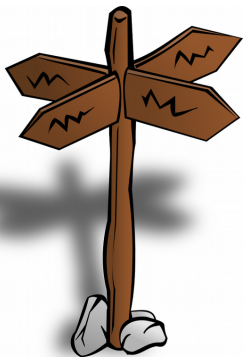
Clipart courtesy FCIT

Aristoteles

384–322 v.Chr.

Aussagenlogik – Übersicht

- Aussagenlogik
- Aussagenlogische Funktionen
- Syntax und Semantik der Aussagenlogik
- Das Erfüllbarkeitsproblem
- Beispiel Dr. House
- Beispiel Gone Maggie gone



Negation



Ich gehe **nicht** ins Kino.

Ist falsch, wenn ich ins Kino gehe, und wahr andernfalls.

not	
x	$\neg x$
1	0
0	1

Andere Bezeichnung: non

Symbole: $\neg x$, $-x$, $\sim x$, x' , $!x$, \bar{x} , Nx , ...

Logikgatter:  

Konjunktion


Der Himmel ist blau und die Sonne scheint.

Trifft nur zu, wenn jede der beiden Teilaussagen wahr ist.

and		
x	y	$x \wedge y$
1	1	1
1	0	0
0	1	0
0	0	0

Andere Bezeichnung: et

Symbole: $x \wedge y$, $x \cdot y$, xy , $x \& y$, K_{xy} , ...

Logikgatter: 

Disjunktion, Alternative



Ich trinke zum Essen Wein oder Bier (oder auch beides).

Nur falsch, wenn ich weder Wein noch Bier trinke.

		or
x	y	$x \vee y$
1	1	1
1	0	1
0	1	1
0	0	0

Andere Bezeichnung: vel

Symbole: $x \vee y$, $x + y$, $x \mid y$, Axy

Logikgatter:  

Ausschließende Disjunktion (Antivalenz)

Ich bin **entweder** gut drauf **oder** saugrantig,
etwas anderes gibt es bei mir nicht.



Trifft zu, wenn ich in genau einer der Stimmungslagen bin (die sich ausschließen).

		xor
x	y	$x \nleftrightarrow y$
1	1	0
1	0	1
0	1	1
0	0	0

Andere Formulierungen: x oder y

Andere Bezeichnungen: exor, aut

Symbole: $x \nleftrightarrow y$, $x \not\equiv y$, $x \oplus y$, $x \leftrightarrow y$, Jxy , ...

Logikgatter:  

Äquivalenz

Ich springe dann (und nur dann), wenn du es auch tust.



Trifft zu, wenn beide springen oder keiner.

		iff
x	y	$x \Leftrightarrow y$
1	1	1
1	0	0
0	1	0
0	0	1

Andere Formulierungen: x genau dann wenn y , x if and only if y ,
 x ist notwendig und hinreichend für y , x ist äquivalent zu y

Andere Bezeichnungen: eq, äq, xnor, nxor, ...

Symbole: $x \Leftrightarrow y$, $x \equiv y$, $x \leftrightarrow y$, E_{xy} , ...

Logikgatter:  

Implikation

Wenn/Falls ich ins Kino gehe, (dann) esse ich dort Popcorn.
Ich gehe nur dann ins Kino, wenn ich dort Popcorn esse.

Falsch, wenn ich im Kino kein Popcorn esse, und wahr, wenn doch.
Keine Festlegung betreffend Popcorn außerhalb des Kinos, daher wahr.

implies		
x	y	$x \Rightarrow y$
1	1	1
1	0	0
0	1	1
0	0	1


„Verum ex quodlibet“: $x \text{ implies } 1 = 1$

„Ex falso quodlibet“: $0 \text{ implies } y = 1$

Andere Formulierungen: aus x folgt y , x impliziert y , x hinreichend für y

Andere Bezeichnung: seq (sequi)

Symbole: $x \Rightarrow y$, $x \supset y$, $x \rightarrow y$, Cxy , ...

Logikgatter: 



Implikation (Umkehrung)

Ich esse (dann) Popcorn, wenn/falls ich ins Kino gehe.

		if
x	y	$x \Leftarrow y$
1	1	1
1	0	1
0	1	0
0	0	1

Andere Formulierungen: x folgt aus y , x wird von y impliziert,
 x ist notwendig für y

Symbole: $x \Leftarrow y$, $x \subset y$, $x \leftarrow y$, ...

Logikgatter:  

Negierte Konjunktion



Negierte Disjunktion

		nand	
x	y	$x \wedge y$	$x \uparrow y$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	1

Andere Bezeichnungen:

Sheffer-Strich, nd (J.Nicod)

Symbole: $x \uparrow y$, $x \mid y$, x/y , D_{xy} , ...



Logikgatter:  

		nor	
x	y	$x \vee y$	$x \downarrow y$
1	1	1	0
1	0	1	0
0	1	1	0
0	0	0	1

Andere Bezeichnungen:

Peirce-Pfeil, sh (H.M.Sheffer)

Symbole: $x \downarrow y$, X_{xy} , ...

Logikgatter:  

Wenn Feiertag ist oder der Vortragende krank ist,
findet die Vorlesung nicht statt.

Logische Struktur: „Wenn x oder y , dann nicht z .“

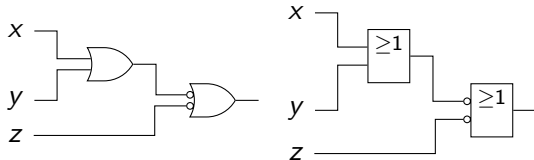
Logische Funktion: $(x \text{ or } y) \text{ implies not } z$ $\text{implies } (\text{or } (x, y), \text{not}(z))$

Logische Formel: $(x \vee y) \Rightarrow \neg z$

Prefix-Notation: $C A x y N z$

Algebraische Notation: $(x + y) \rightarrow -z$ $\bar{x} \bar{y} + \bar{z}$

Logischer Schaltkreis:



Implikation oder Äquivalenz?

Natürlichsprachliche Implikationen sind oft logische Äquivalenzen.

Wenn du mein Auto wäscht, bekommst du 10 Euro.

Und was, wenn ich es nicht tue?

Nur ein Logiker hält in diesem Fall 10 Euro für möglich.

Alle anderen interpretieren den Satz als:

Du bekommst 10 Euro dann und nur dann, wenn du das Auto wäscht.

Der positive Erfolg bei allen Lehrveranstaltungen und Prüfungen der Studieneingangs- und Orientierungsphase berechtigt zur Absolvierung der weiteren Lehrveranstaltungen und Prüfungen sowie zum Verfassen der im Curriculum vorgesehenen Bachelor- oder Diplomarbeiten.

Universitätsgesetz 2002, Stand Bgbl I Nr. 50/2024, § 66(2)

Logiker: Keine Einschränkung bei nicht bestandener STEOP.

Ministerium: Restliches Studium dann und nur dann, wenn STEOP.

Der Besitz eines Führerscheins berechtigt zum Lenken eines Autos.

Ohne Führerschein keine Berechtigung? (Äquivalenz)
Auch nicht auf Privatgelände? (Doch nur Implikation?)

In formalen Kontexten wird strikt zwischen Implikation und Äquivalenz unterschieden. „Implikation = halbe Äquivalenz“

Wenn eine Zahl durch 4 teilbar ist, ist sie gerade.

4-Teilbarkeit ist eine hinreichende Bedingung für Geradheit,
aber keine notwendige.

Äquivalenz führt zu einer falschen Aussage:

Eine Zahl ist durch 4 teilbar genau dann, wenn sie gerade ist.

2 ist eine gerade Zahl, aber nicht durch 4 teilbar.

Inklusive oder exklusive Disjunktion?

Natürlichsprachliche Disjunktionen sind meist ausschließend gemeint.

Falls du mich suchst: Ich bin zu Hause oder in der Arbeit.

Physikalisch kann ein Körper nicht an zwei Orten gleichzeitig sein.
Andererseits: Das Büro kann Teil der Wohnung sein.

„Tee oder Kaffee?“ – „Beides, bitte!“

Eher unüblich, aber der Gast ist König.

Ich besuche dich morgen oder übermorgen.

Ein Besuch an beiden Tagen wäre unerwartet.

Ich fahre entweder Auto oder höre Musik.
(Auf beides gleichzeitig kann ich mich nicht konzentrieren.)

Wirklich ein Beispiel für ausschließende Disjunktion?

Habe ich außerhalb des Autos tatsächlich keine ruhige Minute?

Die exklusive Disjunktion ist hier als Implikation gemeint (und wird auch so verstanden):

Wenn ich Auto fahre, höre ich nicht Musik.

Legt nicht fest, was ich außerhalb des Autos mache.

Rezept für Zweifelsfälle der aussagenlogischen Modellierung

- 1 Identifiziere die elementaren Aussagen.
- 2 Analysiere *alle* Wahrheitsbelegungen.
- 3 Wähle geeignete logische Funktionen (unbeirrt von Intuition und natürlicher Sprache).

z = Entweder „ich fahre Auto“ (x) oder „ich höre Musik“ (y).

x	y	z	$x \vee y$	$x \nleftrightarrow y$	$x \Rightarrow \neg y$	$x \uparrow y$
1	1	0	1	0	0	0
1	0	1	1	1	1	1
0	1	1	1	1	1	1
0	0	1	0	0	1	1

$x \Rightarrow \neg y$: Wenn ich Auto fahre, dann höre ich nicht Musik.

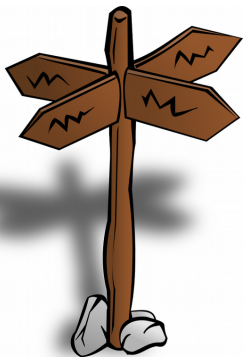
$x \uparrow y$: Es kommt nicht vor, dass ich Auto fahre und Musik höre.

Modellierung vs. Implementierung

- Modellierung:
 - möglichst einfach zu verstehen
 - nahe an der Intuition (viele Operatoren)
 - dafür komplexe Formelstruktur
- Implementierung:
 - möglichst einfach zu Verarbeiten
 - wenige Operatoren
 - vereinfachte Formeln
 - einfache Darstellung (Normalformen)

Aussagenlogik – Übersicht

- Aussagenlogik
- Aussagenlogische Funktionen
- Syntax und Semantik der Aussagenlogik
- Das Erfüllbarkeitsproblem
- Beispiel Dr. House
- Beispiel Gone Maggie gone



Syntax versus Semantik

- Bisher war das Symbol $=$ in Regeln wie $\neg(x \uparrow y) = (x \uparrow y) \uparrow (x \uparrow y)$ nicht genau definiert.
- Mathematik: zwei Funktionen $f, g : D \mapsto B$ sind gleich, wenn sie für die selben Argumente dasselbe Ergebnis liefern.
D.h., wenn $f(x) = g(x)$ für alle $x \in D$, dann gilt $f = g$.
- $\neg(x \uparrow y)$ und $(x \uparrow y) \uparrow (x \uparrow y)$ sind in diesem Sinn gleich.
- Mit diesem Gleichheitsbegriff können wir zB folgendes nicht ausdrücken:
 - Zählt man die Vorkommen, enthält $\neg(x \uparrow y)$ zwei, $(x \uparrow y) \uparrow (x \uparrow y)$ drei Operatoren.
 - Die Formel $\neg(x \uparrow y)$ ist nicht in disjunktiver Normalform, die Formel $\neg x \vee \neg y$ aber schon.
- Wir benötigen eine zweite Sichtweise, bei der wir diese Unterscheidung treffen können.

Syntax versus Semantik

Syntax:

- Zeichenfolge (String), mit der etwas notiert wird
- Regeln dafür, welche Zeichenfolgen zulässig sind

Semantik:

- Bedeutung einer Zeichenfolge
- Funktion, die jeder zulässigen Zeichenfolge eine Bedeutung zuordnet

Syntax und Semantik sind grundsätzlich voneinander unabhängig.
Die Bedeutung von Zeichen muss explizit vereinbart werden.

Syntax	Semantik
eins (deutsch)	das abstrakte Konzept der Zahl „1“
one (englisch)	
1 (mathematisch)	
Bug	Schiffsvorderteil (deutsch) Käfer, Programmfehler (englisch)

Induktive Definition unendlicher Mengen

Stufenweise Konstruktion der geraden Zahlen:

- 0 ist eine gerade Zahl: $G_0 = \{0\}$
- Addiert man zu geraden Zahlen 2, erhält man wieder gerade Zahlen:
$$G_1 = G_0 \cup \{n + 2 \mid n \in G_0\} = \{0, 2\}$$
$$G_2 = G_1 \cup \{n + 2 \mid n \in G_1\} = \{0, 2, 4\}$$
$$G_{i+1} = G_i \cup \{n + 2 \mid n \in G_i\} = \{0, 2, 4, \dots, 2(i + 1)\}$$
- Die geraden Zahlen sind alle so konstruierten Zahlen:
$$\mathbb{G} = \lim_{i \rightarrow \infty} G_i = \bigcup_{i \geq 0} G_i$$

Umständlich, aber konstruktiv: Beginnend mit G_0 lassen sich systematisch alle geraden Zahlen berechnen.

Beobachtung:

- $G_0 \subseteq \mathbb{G}$
- Wenn $n \in \mathbb{G}$, dann auch $n + 2 \in \mathbb{G}$.
- \mathbb{G} ist die kleinste Menge mit diesen beiden Eigenschaften.

Induktive Definition der geraden Zahlen

\mathbb{G} ist die kleinste Menge, für die gilt:

- $0 \in \mathbb{G}$
- Wenn $n \in \mathbb{G}$, dann auch $n + 2 \in \mathbb{G}$.

Kompakte Definition, aber nicht konstruktiv:

In den Bedingungen kommt die zu definierende Menge \mathbb{G} selbst vor.

Beide Methoden definieren dieselbe Menge.

(Nicht offensichtlich, Beweis erforderlich!)

Daher: „Use the best of both worlds.“

- Definiere die Menge induktiv.
- Konstruiere benötigte Elemente stufenweise.

Anmerkung: Der Zusatz „ist kleinste Menge“ ist wesentlich.

Die natürlichen Zahlen erfüllen ebenfalls beide Bedingungen, sind aber nicht die kleinste derartige Menge.

Induktive Definition – allgemeine Situation

$\mathcal{U} \dots$ Universum, Menge aller relevanten Elemente

$\mathcal{M}_0 \subseteq \mathcal{U} \dots$ Menge von Grundelementen

$f_1: \mathcal{U}^{n_1} \mapsto \mathcal{U}, f_2: \mathcal{U}^{n_2} \mapsto \mathcal{U}, \dots$ Konstruktionsfunktionen

Stufenweise Konstruktion der Menge \mathcal{M}

- $\mathcal{M}_{i+1} = \mathcal{M}_i \cup \{ f_1(x_1, \dots, x_{n_1}) \mid x_1, \dots, x_{n_1} \in \mathcal{M}_i \}$
 $\cup \{ f_2(x_1, \dots, x_{n_2}) \mid x_1, \dots, x_{n_2} \in \mathcal{M}_i \}$
 $\cup \dots$
- $\mathcal{M} = \lim_{i \rightarrow \infty} \mathcal{M}_i = \bigcup_{i \geq 0} \mathcal{M}_i$

Induktive Definition der Menge \mathcal{M}

\mathcal{M} ist die kleinste Menge, für die gilt:

- $\mathcal{M}_0 \subseteq \mathcal{M}$
- Wenn $x_1, \dots, x_{n_1} \in \mathcal{M}$, dann $f_1(x_1, \dots, x_{n_1}) \in \mathcal{M}$.
- Wenn $x_1, \dots, x_{n_2} \in \mathcal{M}$, dann $f_2(x_1, \dots, x_{n_2}) \in \mathcal{M}$.
- \dots

Aussagenlogik – Syntax

Ausdrücke wie $x \wedge y$ und $(x \uparrow y) \uparrow (x \uparrow y)$ repräsentieren die gleiche Funktion. Um Aussagen über ihre Form treffen zu können, benötigen wir eine Formelsprache.

$$\mathcal{V} = \{A, B, C, \dots, A_0, A_1, \dots\}$$

aussagenlogische Variablen

Syntax aussagenlogischer Formeln

Die Menge \mathcal{A} der aussagenlogischen Formeln ist die kleinste Menge, für die gilt:

(a1) $\mathcal{V} \subseteq \mathcal{A}$

Variablen sind Formeln.

(a2) $\{\top, \perp\} \subseteq \mathcal{A}$

\top und \perp sind Formeln.

(a3) $\neg F \in \mathcal{A}$, wenn $F \in \mathcal{A}$.

$\neg F$ ist eine Formel, falls F eine ist.

(a4) $(F * G) \in \mathcal{A}$, wenn $F, G \in \mathcal{A}$ und $*$ $\in \{\wedge, \uparrow, \vee, \downarrow, \Leftrightarrow, \nRightarrow, \Rightarrow, \Leftarrow\}$.

$(F * G)$ ist eine Formel, falls F und G welche sind und $*$ ein binäres Op.symbol ist.

- (a1) $\mathcal{V} \subseteq \mathcal{A}$
- (a2) $\{\top, \perp\} \subseteq \mathcal{A}$
- (a3) $\neg F \in \mathcal{A}$, wenn $F \in \mathcal{A}$.
- (a4) $(F * G) \in \mathcal{A}$, wenn $F, G \in \mathcal{A}$ und $*$ $\in \{\wedge, \uparrow, \vee, \downarrow, \Leftrightarrow, \nLeftrightarrow, \Rightarrow, \Leftarrow\}$.

$((A \uparrow B) \uparrow (A \uparrow B))$ ist eine aussagenlogische Formel, weil:

- 1 A und B sind Formeln. (a1)
- 2 $(A \uparrow B)$ ist eine Formel, (a4)
 - da A und B Formeln sind (Punkt 1)
 - und \uparrow ein binäres Operatorsymbol ist.
- 3 $((A \uparrow B) \uparrow (A \uparrow B))$ ist eine Formel, (a4)
 - da $(A \uparrow B)$ und $(A \uparrow B)$ Formeln sind (Punkt 2)
 - und \uparrow ein binäres Operatorsymbol ist.

(a1) $\mathcal{V} \subseteq \mathcal{A}$

(a2) $\{\top, \perp\} \subseteq \mathcal{A}$

(a3) $\neg F \in \mathcal{A}$, wenn $F \in \mathcal{A}$.

(a4) $(F * G) \in \mathcal{A}$, wenn $F, G \in \mathcal{A}$ und $*$ $\in \{\wedge, \uparrow, \vee, \downarrow, \Leftrightarrow, \nLeftrightarrow, \Rightarrow, \Leftarrow\}$.

$A \wedge B$ ist keine aussagenlogische Formel.

- \mathcal{A} ist die kleinste Menge mit den Eigenschaften (a1)–(a4), daher kann \wedge nur aufgrund von (a4) in einer Formel vorkommen.
- Dann muss es aber auch ein Klammernpaar geben.
- $A \wedge B$ enthält \wedge , aber keine Klammern – Widerspruch.

Formelsyntax: Beispiel einer *induktiven Definition*

\mathcal{A} ist die kleinste Menge, für die gilt:

$$(a1) \quad \mathcal{V} \subseteq \mathcal{A}$$

$$(a2) \quad \{\top, \perp\} \subseteq \mathcal{A}$$

$$(a3) \quad \neg F \in \mathcal{A}, \text{ wenn } F \in \mathcal{A}.$$

$$(a4) \quad (F * G) \in \mathcal{A}, \text{ wenn } F, G \in \mathcal{A} \text{ und } * \in \{\wedge, \uparrow, \vee, \downarrow, \Leftrightarrow, \nLeftrightarrow, \Rightarrow, \Leftarrow\}.$$

$\mathcal{U} \dots$ Menge aller Zeichenketten bestehend aus Variablen,
Operatorsymbolen und Klammern

$\mathcal{V} \cup \{ \text{„}\top\text{“}, \text{„}\perp\text{“} \} \dots$ Grundelemente

$$\left. \begin{array}{l} f_{\neg}(F) = \text{„}\neg\text{“ } F \\ f_{\wedge}(F, G) = \text{„}(\text{“ } F \text{ „}\wedge\text{“ } G \text{ „})\text{“} \\ f_{\uparrow}(F, G) = \text{„}(\text{“ } F \text{ „}\uparrow\text{“ } G \text{ „})\text{“} \\ \vdots \\ f_{\Leftarrow}(F, G) = \text{„}(\text{“ } F \text{ „}\Leftarrow\text{“ } G \text{ „})\text{“} \end{array} \right\} \dots \text{Konstruktionsfunktionen}$$

$((A \wedge \neg B) \Rightarrow \perp)$ – wahr oder falsch?

Hängt ab

- vom Wert der Variablen A und B und
- von der Bedeutung der Symbole \wedge , \neg , \Rightarrow und \perp .

Interpretationen

$\mathbb{B} = \{1, 0\}$... Wahrheitswerte

$I: \mathcal{V} \mapsto \mathbb{B}$... Wahrheitsbelegung, Interpretation

$\mathcal{I} = \{I \mid I: \mathcal{V} \mapsto \mathbb{B}\}$... Menge aller Interpretationen

$I(A) = I(C) = 1$ und $I(v) = 0$ sonst

„Die elementaren Aussagen A und C sind wahr, die übrigen sind falsch.“

Semantik aussagenlogischer Formeln

Der Wert einer Formel in einer Interpretation I wird festgelegt durch die Funktion $\text{val}: \mathcal{I} \times \mathcal{A} \mapsto \mathbb{B}$:

$$(v1) \quad \text{val}_I(A) = I(A) \text{ f\"ur } A \in \mathcal{V};$$

$$(v2) \quad \text{val}_I(\top) = 1 \text{ und } \text{val}_I(\perp) = 0;$$

$$(v3) \quad \text{val}_I(\neg F) = \neg \text{val}_I(F);$$

$$(v4) \quad \text{val}_I(F * G) = \text{val}_I(F) \circledast \text{val}_I(G),$$

wobei \circledast die logische Funktion zum Operator $*$ ist.

(v4) ist eine Abkürzung für:

$$\text{val}_I(F \wedge G) = \text{val}_I(F) \wedge \text{val}_I(G)$$

$$\text{val}_I(F \vee G) = \text{val}_I(F) \vee \text{val}_I(G)$$

$$\text{val}_I(F \Leftrightarrow G) = \text{val}_I(F) \Leftrightarrow \text{val}_I(G)$$

$$\text{val}_I(F \Rightarrow G) = \text{val}_I(F) \Rightarrow \text{val}_I(G)$$

\vdots

Logische (Boolesche) Funktionen – Wiederholung

true	false
1	0
\neg	\neg

x	not
1	0
0	1
\neg	

x	y	and ($f_{2.1}$)	nand ($f_{2.14}$)	or ($f_{2.7}$)	nor ($f_{2.8}$)	iff ($f_{2.9}$)	xor ($f_{2.6}$)	implies ($f_{2.11}$)	($f_{2.2}$)	if ($f_{2.13}$)	($f_{2.4}$)
1	1	1	0	1	0	1	0	1	0	1	0
1	0	0	1	1	0	0	1	0	1	1	0
0	1	0	1	1	0	0	1	1	0	0	1
0	0	0	1	0	1	1	0	1	0	1	0
		\wedge	\uparrow	\vee	\downarrow	\Leftrightarrow	\oplus	\Rightarrow	\nRightarrow	\Leftarrow	\nLeftarrow

Semantik aussagenlogischer Formeln

- Warum die farbliche Hervorhebung in $\text{val}_I((F \wedge G)) = \text{val}_I(F) \wedge \text{val}_I(G)$?
- $(F \wedge G)$ ist eine Formel, d.h., \wedge ist ein Symbol der Syntax.
- $\text{val}_I(F) \wedge \text{val}_I(G)$ ist die Anwendung einer mathematischen Funktion in der Semantik.
- Weil wir $f_{2.2}$ und \wedge als gleiche Funktion festgelegt haben, können wir auch $f_{2.2}(\text{val}_I(F), \text{val}_I(G))$ schreiben.
- $f_{2.2}(F, G)$ ist aber *keine* Formel – dazu müssten wir die Syntaxregeln der Aussagenlogik anpassen.
- Praxis: Syntax- und Semantik-Ebene oft vermischt.
Besser: unterschiedliche Bezeichnungen bei Verwechslungsgefahr (z.B. and, $f_{2.2}$)

Semantik aussagenlogischer Formeln (ohne Farben)

Der Wert einer Formel in einer Interpretation I wird festgelegt durch die Funktion $\text{val}: \mathcal{I} \times \mathcal{A} \mapsto \mathbb{B}$:

(v1) $\text{val}_I(A) = I(A)$ für $A \in \mathcal{V}$;

(v2) $\text{val}_I(\top) = 1$ und $\text{val}_I(\perp) = 0$;

(v3) $\text{val}_I(\neg F) = \text{not } \text{val}_I(F)$;

(v4) $\text{val}_I((F * G)) = \text{val}_I(F) \circledast \text{val}_I(G)$,
wobei \circledast die logische Funktion zum Operator $*$ ist.

(v4) ist eine Abkürzung für:

$$\text{val}_I((F \wedge G)) = \text{val}_I(F) \text{ and } \text{val}_I(G)$$

$$\text{val}_I((F \vee G)) = \text{val}_I(F) \text{ or } \text{val}_I(G)$$

$$\text{val}_I((F \Leftrightarrow G)) = \text{val}_I(F) \text{ iff } \text{val}_I(G)$$

$$\text{val}_I((F \Rightarrow G)) = \text{val}_I(F) \text{ implies } \text{val}_I(G)$$

\vdots

Beispiel: Auswertung einer Formel mittels val_I

- (v1) $\text{val}_I(A) = I(A)$ für $A \in \mathcal{V}$;
- (v2) $\text{val}_I(\top) = 1$ und $\text{val}_I(\perp) = 0$;
- (v3) $\text{val}_I(\neg F) = \text{not } \text{val}_I(F)$;
- (v4) $\text{val}_I((F * G)) = \text{val}_I(F) \circledast \text{val}_I(G)$,
wobei \circledast die logische Funktion zum Operator $*$ ist.

Wert von $((A \wedge \neg B) \Rightarrow \perp)$ für $I(A) = 1$ und $I(B) = 0$

$$\begin{aligned}\text{val}_I(((A \wedge \neg B) \Rightarrow \perp)) &= \text{val}_I((A \wedge \neg B)) \text{ implies } \text{val}_I(\perp) \\ &= (\text{val}_I(A) \text{ and } \text{val}_I(\neg B)) \text{ implies } 0 \\ &= (1 \text{ and not } \text{val}_I(B)) \text{ implies } 0 \\ &= (1 \text{ and not } 0) \text{ implies } 0 \\ &= (1 \text{ and } 1) \text{ implies } 0 \\ &= 1 \text{ implies } 0 = 0\end{aligned}$$

Wahrheitstabelle - Wiederholung

- Kompakte Berechnung der Formelwerte für alle Interpretationen
- Unter jedem Operator steht der Wert der entsprechenden Teilformel.

A	B	$((A \wedge \neg B) \Rightarrow \perp)$
---	---	---

1	1	1 0 0 1 1 0
---	---	--------------------

1	0	1 1 1 0 0 0
---	---	--------------------

0	1	0 0 0 1 1 0
---	---	--------------------

0	0	0 0 1 0 1 0
---	---	--------------------

bedeutet:

$I(A) = 1, I(B) = 1: \text{val}_I(\dots) = \dots = 1$

$I(A) = 1, I(B) = 0: \text{val}_I(\dots) = \dots = 0$

$I(A) = 0, I(B) = 1: \text{val}_I(\dots) = \dots = 1$

$I(A) = 0, I(B) = 0: \text{val}_I(\dots) = \dots = 1$

false
0
\perp

x	not
1	0
0	1
	\neg

x	y	and	implies
1	1	1	1
1	0	0	0
0	1	0	1
0	0	0	1
		\wedge	\Rightarrow

Rezept für Zweifelsfälle der aussagenlogischen Modellierung

- 1 Identifiziere die elementaren Aussagen.
- 2 Analysiere *alle* Wahrheitsbelegungen.
- 3 Wähle geeignete logische Funktionen
(unbeirrt von Intuition und natürlicher Sprache)

Klingt ja nicht schlecht, aber:

Wie kann man eine beliebige Funktion auf eine Kombination der bekannten logischen Grundfunktionen zurückführen?

Beziehungsweise:

Wie kann man eine beliebige Funktion mit den bekannten Operatoren als Formel darstellen?

Gesucht: Ein allgemeines Verfahren (ein Algorithmus), das zu einer gegebenen Funktion eine passende Formel liefert.

Algorithmus via DNF

- Stelle die Wahrheitstabelle für die Formel F auf.
- Übersetze jede Zeile, für die $\text{val}_I(F) = 1$ gilt, in eine Konjunktion von Literalen der jeweiligen Variablen.
 - Eine Variable A wird zum Literal A , falls $\text{val}_I(A) = 1$ gilt.
 - Eine Variable A wird zum Literal $\neg A$, falls $\text{val}_I(A) = 0$ gilt.
- Bilde die Disjunktion über die Formeln der einzelnen Zeilen.

Algorithmus via KNF

- Stelle die Wahrheitstabelle für die Formel F auf.
- Übersetze jede Zeile, für die $\text{val}_I(F) = 0$ gilt, in eine Disjunktion von Literalen der jeweiligen Variablen.
 - Eine Variable A wird zum Literal $\neg A$, falls $\text{val}_I(A) = 1$ gilt.
 - Eine Variable A wird zum Literal A , falls $\text{val}_I(A) = 0$ gilt.
- Bilde die Konjunktion über die Formeln der einzelnen Zeilen.

Beispiel: Kardinalitäten ausdrücken

Lara, Can, Sam und Jae wollen ein Zweierteam zum Fußball auswählen.
D.h. wir wollen genau zwei Personen aus vier auswählen.

L ... Lara ist im Team.

S ... Sam ist im Team.

C ... Can ist im Team.

J ... Jae ist im Team.

L	C	S	J	F	Formel	L	C	S	J	F	Formel
0	0	0	0	0		1	0	0	0	0	
0	0	0	1	0		1	0	0	1	1	$L \wedge \neg C \wedge \neg S \wedge J$
0	0	1	0	0		1	0	1	0	1	$L \wedge \neg C \wedge S \wedge \neg J$
0	0	1	1	1	$\neg L \wedge \neg C \wedge S \wedge J$	1	0	1	1	0	
0	1	0	0	0		1	1	0	0	1	$L \wedge C \wedge \neg S \wedge \neg J$
0	1	0	1	1	$\neg L \wedge C \wedge \neg S \wedge J$	1	1	0	1	0	
0	1	1	0	1	$\neg L \wedge C \wedge S \wedge \neg J$	1	1	1	0	0	
0	1	1	1	0		1	1	1	1	0	
$F = (\neg L \wedge \neg C \wedge S \wedge J) \vee (\neg L \wedge C \wedge \neg S \wedge J) \vee (\neg L \wedge C \wedge S \wedge \neg J) \vee$ $(L \wedge \neg C \wedge \neg S \wedge J) \vee (L \wedge \neg C \wedge S \wedge \neg J) \vee (L \wedge C \wedge \neg S \wedge \neg J)$											

Funktionale Vollständigkeit von not, and, or

- Aus der Wahrheitstabelle lässt sich zu jeder Booleschen Funktion eine Formel in DNF bzw. KNF ablesen.
- Beide Normalformen verwenden nur \neg , \wedge und \vee .

Folgerung:

$\{\neg, \wedge, \vee\}$ ist funktional vollständig.

Klassifikation von Formeln

Eine Formel F heißt

- *gültig*, wenn $\text{val}_I(F) = 1$ für alle $I \in \mathcal{I}$; „Tautologie“
- *erfüllbar*, wenn $\text{val}_I(F) = 1$ für mindestens ein $I \in \mathcal{I}$;
- *widerlegbar*, wenn $\text{val}_I(F) = 0$ für mindestens ein $I \in \mathcal{I}$;
- *unerfüllbar*, wenn $\text{val}_I(F) = 0$ für alle $I \in \mathcal{I}$. „Kontradiktion“

Folgerungen:

- Eine gültige Formel ist erfüllbar, aber weder widerlegbar noch unerfüllbar.
- Eine erfüllbare Formel kann gültig oder widerlegbar sein, aber nicht unerfüllbar.
- Eine widerlegbare Formel kann erfüllbar oder unerfüllbar sein, aber nicht gültig.
- Eine unerfüllbare Formel ist widerlegbar, aber weder gültig noch erfüllbar.
- F ist gültig/erfüllbar/widerlegbar/unerfüllbar genau dann, wenn $\neg F$ unerfüllbar/widerlegbar/erfüllbar/gültig ist.

$((A \wedge \neg B) \Rightarrow \perp)$ ist erfüllbar und widerlegbar.

A	B	$((A \wedge \neg B) \Rightarrow \perp)$			
1	1	1	0	0	1 0
1	0	1	1	1	0 0
0	1	0	0	0	1 0
0	0	0	0	1	0 0

Die Formel ist

- erfüllbar (daher nicht unerfüllbar),
- widerlegbar (daher nicht gültig).

$(A \vee \neg A)$ ist gültig und erfüllbar.

A	$(A \vee \neg A)$
1	1 1 0 1
0	0 1 1 0

Die Formel ist

- gültig (daher nicht widerlegbar),
- erfüllbar (daher nicht unerfüllbar).

$(A \wedge \neg A)$ ist unerfüllbar und widerlegbar.

A	$(A \wedge \neg A)$
1	1 0 0 1
0	0 0 1 0

Die Formel ist

- unerfüllbar (daher nicht erfüllbar),
- widerlegbar (daher nicht gültig).

Semantische Äquivalenz 1/2

Semantische Äquivalenz

Zwei Formeln F und G heißen *äquivalent*, geschrieben $F = G$, wenn $\text{val}_I(F) = \text{val}_I(G)$ für alle Interpretationen I gilt.

$\neg(A \wedge B)$ und $(\neg A \vee \neg B)$ sind äquivalent

A	B	$\neg(A \wedge B) = (\neg A \vee \neg B)$									
1	1	0	1	1	1	✓	0	1	0	0	1
1	0	1	1	0	0	✓	0	1	1	1	0
0	1	1	0	0	1	✓	1	0	1	0	1
0	0	1	0	0	0	✓	1	0	1	1	0

Semantische Äquivalenz 2/2

Äquivalenz bleibt bei der Ersetzung von Variablen durch Formeln erhalten.

$$\neg(A \wedge B) = (\neg A \vee \neg B) \quad [A \mapsto (C \vee D), B \mapsto \neg D]$$

Ersetzen einer Teilformel durch eine äquivalente liefert eine äquiv. Formel.

$$(A \Rightarrow \neg(A \wedge B)) \quad \neg(A \wedge B) = (\neg A \vee \neg B)$$

Semantische Äquivalenz 2/2

Äquivalenz bleibt bei der Ersetzung von Variablen durch Formeln erhalten.

$$\neg((C \vee D) \wedge \neg D) = (\neg(C \vee D) \vee \neg\neg D) \quad [A \mapsto (C \vee D), B \mapsto \neg D]$$

Ersetzen einer Teilformel durch eine äquivalente liefert eine äquiv. Formel.

$$(A \Rightarrow \neg(A \wedge B)) = (A \Rightarrow (\neg A \vee \neg B)) \quad \neg(A \wedge B) = (\neg A \vee \neg B)$$

$\langle \mathbb{B}, \text{and, or, not}, 0, 1 \rangle$ ist eine Boolesche Algebra

Das heißt, es gelten folgende Gleichungen.

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

$$A \wedge B = B \wedge A$$

$$A \wedge A = A$$

$$A \wedge \top = A$$

$$A \wedge \neg A = \perp$$

$$A \wedge (A \vee B) = A$$

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

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

$$(A \vee B) \vee C = A \vee (B \vee C)$$

$$A \vee B = B \vee A$$

$$A \vee A = A$$

$$A \vee \perp = A$$

$$A \vee \neg A = \top$$

$$A \vee (A \wedge B) = A$$

Assoziativität

Kommutativität

Idempotenz

Neutralität

Komplement

Absorption

Distributivität

Schreibvereinfachung:

- keine Außenklammern,
- keine Klammern bei geschachteltem \wedge oder \vee (Assoziativität!)

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

Weitere Äquivalenzen

Ersetzen von Junktoren durch \wedge , \vee und \neg

$$\begin{array}{ll} A \uparrow B = \neg A \vee \neg B & A \Leftrightarrow B = (\neg A \vee B) \wedge (A \vee \neg B) \\ A \downarrow B = \neg A \wedge \neg B & = (A \wedge B) \vee (\neg A \wedge \neg B) \\ A \Rightarrow B = \neg A \vee B & A \nLeftrightarrow B = (\neg A \vee \neg B) \wedge (A \vee B) \\ A \Leftarrow B = A \vee \neg B & = (A \wedge \neg B) \vee (\neg A \wedge B) \end{array}$$

Verschieben der Negation

$$\left. \begin{array}{l} \neg(A \wedge B) = \neg A \vee \neg B \\ \neg(A \vee B) = \neg A \wedge \neg B \end{array} \right\} \text{De Morgan Regeln} \quad \neg\neg A = A$$

Äquivalenzen für \top und \perp

$$\begin{array}{llll} A \wedge \top = A & A \wedge \perp = \perp & A \wedge \neg A = \perp & \neg \top = \perp \\ A \vee \perp = A & A \vee \top = \top & A \vee \neg A = \top & \neg \perp = \top \end{array}$$

$$\begin{aligned}
& (X \uparrow Y) \uparrow (T \uparrow Y) \\
&= (\neg X \vee \neg Y) \uparrow (\neg T \vee \neg Y) \\
&= \neg(\neg X \vee \neg Y) \vee \neg(\neg T \vee \neg Y) \\
&= (\neg\neg X \wedge \neg\neg Y) \vee (\neg\neg T \wedge \neg\neg Y) \\
&= (X \wedge Y) \vee (T \wedge Y) \\
&= (X \wedge Y) \vee Y \\
&= Y
\end{aligned}$$

$$A \uparrow B = \neg A \vee \neg B$$

$$A \uparrow B = \neg A \vee \neg B$$

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

$$\neg\neg A = A$$

$$A \wedge T = A, \text{ Komm. } \wedge$$

$$A \vee (A \wedge B) = A, \text{ Komm. } \wedge, \vee$$

Logische Konsequenz

$F_1, \dots, F_n \models I G$: „Aus $\text{val}_I(F_1) = \dots = \text{val}_I(F_n) = 1$ folgt $\text{val}_I(G) = 1$.“

„Falls in der Wahrheitsbelegung I alle Prämissen wahr sind,
dann ist auch die Konklusion wahr in I .“

$I(A)$	$I(B)$	$A, A \vee B \models_I B$			
1	1	1	1	✓	1
1	0	1	1	✗	0
0	1	0	1	✓	1
0	0	0	0	✓	0

Logische Konsequenz

$F_1, \dots, F_n \models G$: $F_1, \dots, F_n \models_I G$ gilt für alle Interpretationen I .

„Die Formel G ist eine logische Konsequenz der Formeln F_1, \dots, F_n .“

„Die Formel G folgt aus den Formeln F_1, \dots, F_n .“

Konvention: „ $\models G$ “ ($n = 0$) bedeutet „ G ist immer wahr (gültig).“

$A, A \vee B \models B$? Nein!

$I(A)$	$I(B)$	$A, A \vee B \models_I B$			
1	1	1	1	✓	1
1	0	1	1	✗	0
0	1	0	1	✓	1
0	0	0	0	✓	0

$I(A) = 1, I(B) = 0$:

Es gilt $\text{val}_I(A) = \text{val}_I(A \vee B) = 1$,
aber $\text{val}_I(B) \neq 1$!

I heißt Gegenbeispiel.

Man schreibt in dem Fall auch $A, A \vee B \not\models B$.

$A, A \Rightarrow B \models B$? Ja!

$I(A)$	$I(B)$	$A, A \Rightarrow B \models_I B$			
1	1	1	1	✓	1
1	0	1	0	✓	0
0	1	0	1	✓	1
0	0	0	1	✓	0

A	x
$A \Rightarrow B$	Wenn x , dann y .
B	y

Ist eine gültige Inferenzregel!

Kriterium für die Gültigkeit von Inferenzregeln

Immer wenn alle Prämissen wahr sind, ist auch die Konklusion wahr.

Abgrenzung Konsequenz von Implikation

- Konsequenz $A \models B$:

“Immer wenn A in einer Interpretation I wahr ist, ist auch B in I wahr (Interpretationen, in denen A falsch ist, werden nicht betrachtet).“

Konsequenz ist damit eine semantische Aussage über die Wahrheit von Formeln.

- Implikation $A \Rightarrow B$:

“Die Formel ist wahr, wenn A falsch ist oder A und B wahr sind (ansonsten ist sie falsch).“

Implikation verbindet zwei Formeln syntaktisch zu einer größeren Formel.

- $A \Rightarrow B$ teilt mit, um welche Formel es sich handelt,
 $\models A \Rightarrow B$ behauptet außerdem, dass die Formel gültig ist.

Äquivalenz, Konsequenz und Gültigkeit

Mit der logischen Konsequenz können wir auch symbolisch ausdrücken, dass eine Formel gültig / erfüllbar / widerlegbar / unerfüllbar ist:

$\models F$... F ist in allen Interpretationen wahr
... F ist gültig

$\not\models F$... F ist **nicht** in allen Interpretationen wahr
... F ist widerlegbar

$\models \neg F$... $\neg F$ ist in allen Interpretationen wahr
... F ist in allen Interpretationen falsch
... F ist unerfüllbar

$\not\models \neg F$... $\neg F$ ist **nicht** in allen Interpretationen wahr
... F ist **nicht** in allen Interpretationen falsch
... F ist erfüllbar

Äquivalenz, Konsequenz und Gültigkeit

Die Formeln F und G sind äquivalent ($F = G$) genau dann, wenn $F \Leftrightarrow G$ eine gültige Formel ist.

Deduktionstheorem

G folgt aus F_1, \dots, F_n genau dann, wenn $F_n \Rightarrow G$ aus F_1, \dots, F_{n-1} folgt.
 $F_1, \dots, F_n \models G$ genau dann, wenn $F_1, \dots, F_{n-1} \models F_n \Rightarrow G$.

Mehrfache Anwendung liefert:

$F_1, \dots, F_n \models G$ genau dann, wenn $F_1 \Rightarrow (F_2 \Rightarrow \dots (F_n \Rightarrow G) \dots)$ gültig.

Wegen $A \Rightarrow (B \Rightarrow C) = (A \wedge B) \Rightarrow C$ erhalten wir weiters:

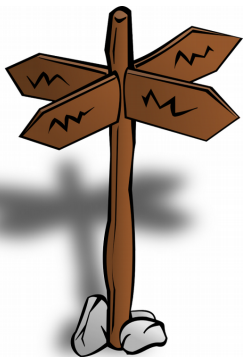
$F_1, \dots, F_n \models G$ genau dann, wenn $(F_1 \wedge \dots \wedge F_n) \Rightarrow G$ gültig.

Das heißt: Semantik ($=$ und \models) ausdrückbar in der Syntax (\Leftrightarrow und \Rightarrow).

Ist nicht in jeder Logik möglich!

Aussagenlogik – Übersicht

- Aussagenlogik
- Aussagenlogische Funktionen
- Syntax und Semantik der Aussagenlogik
- **Das Erfüllbarkeitsproblem**
- Beispiel Dr. House
- Beispiel Gone Maggie gone



Das Erfüllbarkeitsproblem der Aussagenlogik

Erfüllbarkeitsproblem (Satisfiability, SAT)

Gegeben: aussagenlogische Formel F

Frage: Ist F erfüllbar, d.h., gibt es ein $I \in \mathcal{I}$, sodass $\text{val}_I(F) = 1$?

Effiziente Verfahren zur Lösung von SAT sind wichtig in der Praxis:

- Viele praktische Aufgaben lassen sich als Probleme der Aussagenlogik formulieren, wie z.B.
 - Verifikation von Hard- und Software
 - Planungsaufgaben, Logistik-Probleme
- Die meisten aussagenlogischen Fragen lassen sich zu einem (Un)Erfüllbarkeitsproblem umformulieren:

$$G \text{ gültig} \iff \neg G \text{ unerfüllbar}$$

$$G \text{ widerlegbar} \iff \neg G \text{ erfüllbar}$$

$$G = H \iff G \not\equiv H \text{ unerfüllbar}$$

$$F_1, \dots, F_n \models G \iff F_1 \wedge \dots \wedge F_n \wedge \neg G \text{ unerfüllbar}$$

Methoden zur Lösung von SAT

Wahrheitstabelle:

- Berechne den Formelwert der Reihe nach für jede Interpretation. Antwort „ja“, sobald man den Wert 1 erhält; „nein“, wenn immer 0.
- Unbrauchbar, da **exponentiell**: $2^{\text{Variablenzahl}}$ Interpretationen!

Umwandlung in DNF:

- Wandle F in eine disjunktive Normalform um. Antwort „nein“, wenn man \perp erhält; „ja“ sonst.
- Unbrauchbar: F meistens in Fast-KNF. Distributivgesetz verlängert F **exponentiell**.

SAT-Solver: Programme, die SAT lösen.

- Verwenden fortgeschrittene algebraische/graphenorientierte/logische Methoden mit besonderen Datenstrukturen.
- Können SAT für Formeln mit Millionen von Variablen lösen.
- Stand der Technik bei der Verifikation von Prozessoren etc.
- Aber: **Exponentielle** Laufzeit für manche Formelarten!

Minisat: ein kleiner, effizienter SAT-Solver

- `www.minisat.se`: „a small, yet efficient, SAT solver“
- Eingabe: KNF Formel via Textdatei im DIMACS Format
- DIMACS Format:
 - Kopfzeile: `p cnf <v> <n>`
 - Alle anderen Zeilen: eine Disjunktion der KNF Formel
 - Variablen: X_1, \dots, X_n dargestellt durch Index
 - positiv: $i \dots X_i$, negativ: $-i \dots \neg X_i$
 - Disjunktion: $X_i \dots X_k \ 0$
- Beispiel: $(X_1 \vee X_2 \vee X_3) \wedge (\neg X_1 \vee \neg X_3)$

Input:	Output:
<code>p cnf 3 2</code>	CPU time: 0.001s
<code>1 2 3 0</code>	SAT -1 2 -3
<code>-1 -3 0</code>	

Interpretation: $I(X_1) = 0, I(X_2) = 1, I(X_3) = 0$ bzw. $\neg X_1 \wedge X_2 \wedge \neg X_3$

Konstruktion DNF/KNF – Wiederholung

Gegeben: Aussagenlogische Formel F

Gesucht: Äquivalente Formel in DNF/KNF

- 1 Ersetze alle Junktoren durch \wedge , \vee und \neg .

$$A \uparrow B = \neg A \vee \neg B \quad A \downarrow B = \neg A \wedge \neg B \quad A \Rightarrow B = \neg A \vee B \quad A \Leftarrow B = A \vee \neg B$$

$$A \Leftrightarrow B = (\neg A \vee B) \wedge (A \vee \neg B) = (A \wedge B) \vee (\neg A \wedge \neg B)$$

$$A \nabla B = (\neg A \vee \neg B) \wedge (A \vee B) = (A \wedge \neg B) \vee (\neg A \wedge B)$$

- 2 Verschiebe Negationen nach innen, eliminiere Doppelnegationen.

$$\neg(A \wedge B) = \neg A \vee \neg B \quad \neg(A \vee B) = \neg A \wedge \neg B \quad \neg\neg A = A$$

- 3 Wende das Distributivgesetz an.

DNF: Schiebe Disjunktionen nach außen mittels

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

KNF: Schiebe Konjunktionen nach außen mittels

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

- 4 Eliminiere \top und \perp .

$$A \wedge \top = A \quad A \wedge \perp = \perp \quad A \wedge \neg A = \perp \quad \neg \top = \perp$$

$$A \vee \perp = A \quad A \vee \top = \top \quad A \vee \neg A = \top \quad \neg \perp = \top$$

(Äquivalenzen werden hier von links nach rechts angewendet.)

Beispiel: komplexere Formel in Minisat

Ist $\neg(A \Rightarrow (B \vee C)) \wedge (A \Leftrightarrow B)$ erfüllbar?

KNF-Umwandlung

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

$$\neg(\neg A \vee (B \vee C)) \wedge ((\neg A \vee B) \wedge (A \vee \neg B)) \quad \text{Definition } \Rightarrow, \Leftrightarrow$$

$$(\neg\neg A \wedge \neg(B \vee C)) \wedge ((\neg A \vee B) \wedge (A \vee \neg B)) \quad \text{Doppelneg., de Morgan}$$

$$A \wedge \neg B \wedge \neg C \wedge (\neg A \vee B) \wedge (A \vee \neg B) \quad \text{de Morgan, Klammern weglassen}$$

DIMACS Datei

Input:

p cnf 3 5

1 0

-2 0

-3 0

-1 2 0

1 -2 0

Output:

CPU time: 0s

UNSAT

\$ 1.000.000,– Prämie für effizienten SAT-Solver

... oder für den Beweis, dass es diesen nicht geben kann.

Abzuholen beim *Clay Mathematics Institute* (www.claymath.org)
für das offene Millenniumsproblem „*P versus NP*“.

Weiters warten ewiger Ruhm, eine Universitätsstelle, ...

P: Klasse der Probleme, die sich effizient (polynomiell) lösen lassen.

NP: Klasse jener Probleme, deren Lösungen sich effizient (polynomiell) verifizieren lassen; die Suche nach der Lösung kann aber aufwändig sein.

P versus NP (Stephen Cook, 1971)

Gilt $P = NP$ oder $P \neq NP$ (gleichbedeutend mit $P \subsetneq NP$)?

NP-Vollständigkeit

Die schwierigsten Probleme in NP heißen *NP-vollständig*.
Ihr Kennzeichen:

Kann man *ein* NP-vollständiges Problem effizient lösen,
dann kann man *alle* Probleme in NP effizient lösen.

HAMILTON-KREIS ist NP-vollständig

Gegeben: Party-Gäste, von denen sich einige nicht mögen.

Frage: Kann man die Gruppe so um einen runden Tisch setzen, dass sich je zwei Sitznachbarn vertragen?

- Wenn alle sitzen, ist leicht zu prüfen, ob sich alle Nachbarn verstehen.
- Das Finden einer geeigneten Sitzordnung ist aber im Allgemeinen schwierig. Exponentiell?

SAT ist NP-vollständig

Gegeben: eine aussagenlogische Formel.

Frage: Ist die Formel erfüllbar?

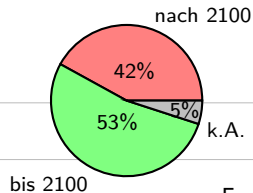
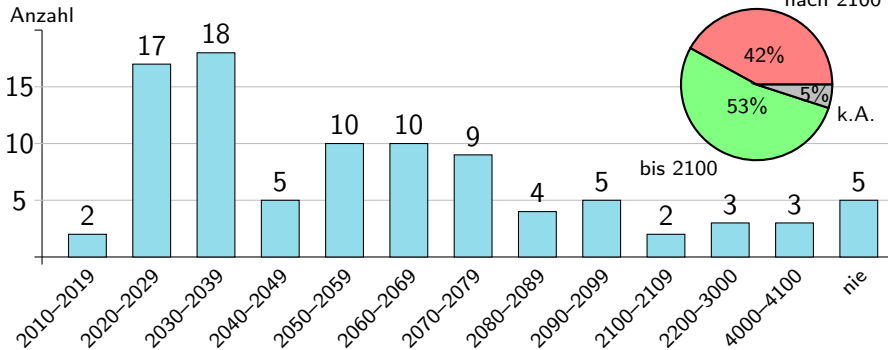
- Ist die Interpretation I gegeben, lässt sich $\text{val}_I(F) = 1$ leicht überprüfen.
- Das Finden der Interpretation ist aber schwierig. Exponentiell?

SAT polynomiell lösbar $\implies P = NP$

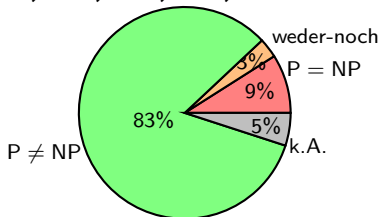
SAT nicht polynomiell lösbar $\implies P \neq NP$

Umfrage unter 152 Experten [W.I.Gasarch 2012]

Wann wird die Frage $P \stackrel{?}{=} NP$ gelöst werden?



Wie wird die Antwort lauten?



Falls Sie SAT nicht ausreichend inspiriert . . .

MINESWEEPER ist NP-vollständig

Gegeben: eine Minesweeper-Stellung

Frage: Ist die Stellung möglich?

Beispiel einer unmöglichen Stellung:

1	2	1	
1	1	1	
6			1

- „2“, aber 5 Bomben in der Umgebung
- „6“, aber nur drei Bomben möglich
- „1“, aber keine Bombe in der Umgebung

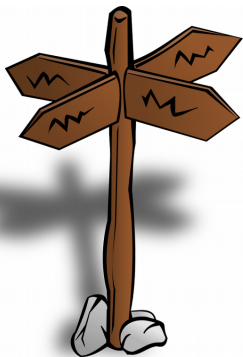
MINESWEEPER polynomiell lösbar $\implies P = NP$

MINESWEEPER nicht polynomiell lösbar $\implies P \neq NP$

Es sind mittlerweile hunderte von NP-vollständigen Problemen aus allen Bereichen der Informatik bekannt.

Aussagenlogik – Übersicht

- Aussagenlogik
- Aussagenlogische Funktionen
- Syntax und Semantik der Aussagenlogik
- Das Erfüllbarkeitsproblem
- Beispiel Dr. House
- Beispiel Gone Maggie gone



House

Max wird mit hohem Fieber und ausgeprägten Gliederschmerzen in das Spital eingeliefert. Dr. House diskutiert die Diagnose mit einer Kollegin.

House: „Wenn der Patient Fieber hat, handelt es sich um Grippe oder Erkältung.“

Cameron: „Wenn er keine starken Gliederschmerzen hat, dann hat er auch keine Grippe.“

House: „Jedenfalls weisen hohes Fieber und starke Gliederschmerzen immer auf Grippe hin.“

Cameron: “Er hat sicher nicht beide Krankheiten gleichzeitig.“

Wie lautet die Diagnose?

Wie lässt sie sich mit Hilfe der Aussagenlogik finden und begründen?

House – Wahl der Aussagenvariablen

Aussagenvariablen können nur Aussagen repräsentieren, die einen Wahrheitswert besitzen.

Einzelne Haupt-, Zeit- oder Eigenschaftswörter sind keine Aussagen!

Falsch: $A = \text{„krank“}$ oder $A = \text{„Fieber“}$.

Möglich: $A = \text{„Max ist krank“}$ oder $A = \text{„Der Patient hat Fieber“}$.

Max wird mit hohem Fieber und ausgeprägten Gliederschmerzen in das Spital eingeliefert.

„Max wird mit ... eingeliefert“ = A ?

„Max hat hohes Fieber“ = A ,

„Max hat ausgeprägte Gliederschmerzen“ = B und

„Max wird in das Spital eingeliefert“ = C ?

„Max hat hohes Fieber“ = „Max hat Fieber“ = A und

„Max hat ausgeprägte Gl.schmerzen“ = „Max hat Gl.schmerzen“ = B ?

House – Wahl der Aussagenvariablen

Dr. House diskutiert die Diagnose mit einer Kollegin.

„Dr. House diskutiert ... mit einer Kollegin“ = D ?

Wenn der Patient Fieber hat, handelt es sich um Grippe oder Erkältung.

„Der Patient hat Fieber“ = E ?

„Der Patient hat Fieber“ = „Max hat Fieber“ = A ?

Cameron: “Er hat sicher nicht beide Krankheiten gleichzeitig.”

„Cameron sagt, dass er nicht beide Krankheiten gleichzeitig hat.“ = F ?

„Max kann nicht beide Krankheiten gleichzeitig haben.“ = F ?

- *Elimination von Abkürzungen und Referenzen*
„Er hat beide Krankheiten“ = „P. hat Grippe“ + „P. hat Erkältung“
- *Generalisierung*: Zusammenfassen von gleichartigen Aussagen
- *Abstraktion*: Weglassen von Details
- *Konzentration auf das Wesentliche*: Identifikation der relevanten Teilaussagen

Aber:

- Was zusammengefasst wurde, kann nicht mehr getrennt analysiert werden.
- Was weggelassen wurde, kann nicht für die Argumentation verwendet werden.
- Was nicht zusammengefasst wurde, aber zusammengehört, muss durch zusätzliche Formeln in Beziehung gesetzt werden.

Was kann man zusammenfassen? Was weglassen? Was ist wesentlich?

House – Wahl der Aussagenvariablen

Max wird mit hohem Fieber und ausgeprägten Gliederschmerzen in das Spital eingeliefert. Dr. House diskutiert die Diagnose mit einer Kollegin.

House: „Wenn der Patient Fieber hat, handelt es sich um Grippe oder Erkältung.“

Cameron: „Wenn er keine starken Gliederschmerzen hat, dann hat er auch keine Grippe.“

House: „Jedenfalls weisen hohes Fieber und starke Gliederschmerzen immer auf Grippe hin.“

Cameron: “Er hat sicher nicht beide Krankheiten gleichzeitig.“

F ... „Max/Patient hat (hohes) Fieber.“

S ... „Max/Patient hat starke/ausgeprägte Gliederschmerzen.“

G ... „Max/Patient hat eine Grippe.“

E ... „Max/Patient hat eine Erkältung.“

House – aussagenlogische Modellierung

F ... „Max/Patient hat (hohes) Fieber.“

S ... „Max/Patient hat starke/ausgeprägte Gliederschmerzen.“

G ... „Max/Patient hat eine Grippe.“

E ... „Max/Patient hat eine Erkältung.“

Max wird mit hohem Fieber und ausgeprägten Gliederschmerzen in das Spital eingeliefert. Dr. House diskutiert die Diagnose mit einer Kollegin.

House: „Wenn der Patient Fieber hat, handelt es sich um Grippe oder Erkältung.“

Cameron: „Wenn er keine starken Gliederschmerzen hat, dann hat er auch keine Grippe.“

House: „Jedenfalls weisen hohes Fieber und starke Gliederschmerzen immer auf Grippe hin.“

Cameron: „Er hat sicher nicht beide Krankheiten gleichzeitig.“

$$F_1 := F \wedge S$$

$$F_2 := F \Rightarrow (G \vee E)$$

$$F_3 := \neg S \Rightarrow \neg G$$

$$F_4 := (F \wedge S) \Rightarrow G$$

$$F_5 := \neg(G \wedge E)$$

House – Diagnose

Finde alle Interpretationen I , in denen alle Formeln wahr sind.

Methode 1: Wahrheitstabelle

Vereinfachung: Prüfe nur Interpretationen, in denen $F_1 = F \wedge S$ wahr ist.

F	S	G	E	F_1	$F \Rightarrow (G \vee E)$	$\neg S \Rightarrow \neg G$	$(F \wedge S) \Rightarrow G$	$\neg(G \wedge E)$
1	1	0	0	1	0	1	0	1
1	1	0	1	1	1	1	0	1
1	1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1	0

$I(G) = 1, I(E) = 0 \Rightarrow$ Die Diagnose lautet auf „Grippe“.

Methode 2: Umwandlung in KNF, SAT-Solver aufrufen

$$\underbrace{F \wedge S}_{F_1} \wedge \underbrace{(\neg F \vee G \vee E)}_{F_2} \wedge \underbrace{(S \vee \neg G)}_{F_3} \wedge \underbrace{(\neg F \vee \neg S \vee G)}_{F_4} \wedge \underbrace{(\neg G \vee \neg E)}_{F_5}$$

SAT-Solver liefert „erfüllbar“ sowie die Interpretation I mit $I(F) = I(S) = I(G) = 1$ und $I(E) = 0$.

Weitere Lösungen durch Ausschluss der bereits gefundenen mit der zusätzlichen Formel $F_6 = \neg(F \wedge S \wedge G \wedge \neg E) = \neg F \vee \neg S \vee \neg G \vee E$

SAT-Solver liefert für $F_1 \wedge \dots \wedge F_5 \wedge F_6$ das Ergebnis „unerfüllbar“, es gibt also keine weiteren Lösungen.

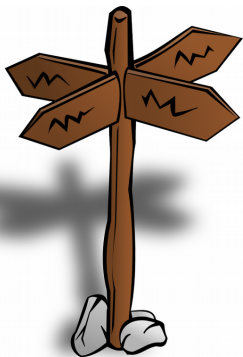
Methode 3: Umwandlung in DNF und Vereinfachung

$$\begin{aligned} & \overbrace{F \wedge S}^{F_1} \wedge \overbrace{(\neg F \vee G \vee E)}^{F_2} \wedge \overbrace{(S \vee \neg G)}^{F_3} \wedge \overbrace{(\neg F \vee \neg S \vee G)}^{F_4} \wedge \overbrace{(\neg G \vee \neg E)}^{F_5} \\ & ((\underbrace{(F \wedge S \wedge \neg F)}_{=\perp}) \vee (F \wedge S \wedge G) \vee (F \wedge S \wedge E)) \wedge \dots \\ & ((F \wedge S \wedge G) \vee (F \wedge S \wedge E)) \wedge (S \vee \neg G) \wedge \dots \\ & ((F \wedge S \wedge G) \vee (F \wedge S \wedge E) \vee \underbrace{(F \wedge S \wedge G \wedge \neg G)}_{=\perp} \vee \underbrace{(F \wedge S \wedge E \wedge \neg G)}_{\text{Absorption } F \wedge S \wedge E}) \wedge \dots \\ & ((F \wedge S \wedge G) \vee (F \wedge S \wedge E)) \wedge (\neg F \vee \neg S \vee G) \wedge \dots \\ & ((F \wedge S \wedge G \wedge G) \vee (F \wedge S \wedge E \wedge G)) \wedge \dots \\ & ((F \wedge S \wedge G) \vee \underbrace{(F \wedge S \wedge E \wedge G)}_{\text{Absorption } F \wedge S \wedge G}) \wedge \dots \\ & (F \wedge S \wedge G) \wedge (\neg G \vee \neg E) \\ & \underbrace{(F \wedge S \wedge G \wedge \neg G)}_{=\perp} \vee (F \wedge S \wedge G \wedge \neg E) \end{aligned}$$

$$F \wedge S \wedge G \wedge \neg E \quad \text{DNF mit Lösung } I(F) = I(S) = I(G) = 1 \text{ und } I(E) = 0$$

Aussagenlogik – Übersicht

- Aussagenlogik
- Aussagenlogische Funktionen
- Syntax und Semantik der Aussagenlogik
- Das Erfüllbarkeitsproblem
- Beispiel Dr. House
- Beispiel Gone Maggie gone



Gone Maggie gone



„The Simpsons“, Staffel 20, Folge 13

Homer will mit Maggie, dem Hund Knecht Ruprecht und einem Glas mit Giftpillen auf die andere Seite des Flusses.

The Simpsons – aussagenlogische Modellierung

If all you have is a hammer, everything looks like a nail.

$M_i \dots$ Maggie	}	\dots befindet sich zum Zeitpunkt i auf der anderen Seite des Flusses.
$K_i \dots$ Knecht Ruprecht		
$G_i \dots$ Gift		
$H_i \dots$ Homer		

- Zum Zeitpunkt i befinden sich alle auf dieser Flusseite.

$\text{AlleHier}(i) := \neg M_i \wedge \neg K_i \wedge \neg G_i \wedge \neg H_i$

- Zum Zeitpunkt i befinden sind alle auf der anderen Flusseite.

$\text{AlleDort}(i) := M_i \wedge K_i \wedge G_i \wedge H_i$

- Wenn sich Maggie und KR oder Maggie und das Gift am selben Flussufer befinden, muss Homer bei Maggie sein.

$\text{Sicher}(i) := ((M_i \Leftrightarrow K_i) \vee (M_i \Leftrightarrow G_i)) \Rightarrow (M_i \Leftrightarrow H_i)$

MH_i ... Maggie	}	... fährt mit Homer über den Fluss (zw. den Zeitpunkten $i - 1$ und i).
KH_i ... Knecht Ruprecht		
GH_i ... Gift		
HH_i ... Homer fährt alleine über den Fluss (zwischen $i - 1$ und i).		

- Genau eine Überfahrt zwischen den Zeitpunkten $i - 1$ und i .

Überfahrt(i) :=

$$(MH_i \wedge \neg KH_i \wedge \neg GH_i \wedge \neg HH_i) \vee (\neg MH_i \wedge KH_i \wedge \neg GH_i \wedge \neg HH_i) \vee (\neg MH_i \wedge \neg KH_i \wedge GH_i \wedge \neg HH_i) \vee (\neg MH_i \wedge \neg KH_i \wedge \neg GH_i \wedge HH_i)$$

- Definition der Überfahrten:

DefÜberfahrt(i) :=

$$\begin{aligned} & (MH_i \Rightarrow ((M_{i-1} \Leftrightarrow M_i) \wedge (K_{i-1} \Leftrightarrow K_i) \wedge (G_{i-1} \Leftrightarrow G_i) \wedge (H_{i-1} \Leftrightarrow H_i) \wedge (H_i \Leftrightarrow M_i))) \\ & \wedge (KH_i \Rightarrow ((M_{i-1} \Leftrightarrow M_i) \wedge (K_{i-1} \Leftrightarrow K_i) \wedge (G_{i-1} \Leftrightarrow G_i) \wedge (H_{i-1} \Leftrightarrow H_i) \wedge (H_i \Leftrightarrow K_i))) \\ & \wedge (GH_i \Rightarrow ((M_{i-1} \Leftrightarrow M_i) \wedge (K_{i-1} \Leftrightarrow K_i) \wedge (G_{i-1} \Leftrightarrow G_i) \wedge (H_{i-1} \Leftrightarrow H_i) \wedge (H_i \Leftrightarrow G_i))) \\ & \wedge (HH_i \Rightarrow ((M_{i-1} \Leftrightarrow M_i) \wedge (K_{i-1} \Leftrightarrow K_i) \wedge (G_{i-1} \Leftrightarrow G_i) \wedge (H_{i-1} \Leftrightarrow H_i))) \end{aligned}$$

Gesamtformel: Nach n Überfahrten sollen alle auf der anderen Seite sein.

$$\begin{aligned} \text{Simpsons}(n) := & \text{AlleHier}(0) \wedge \text{AlleDort}(n) \wedge \bigwedge_{i=0}^n \text{Sicher}(i) \\ & \wedge \bigwedge_{i=1}^n \text{Überfahrt}(i) \wedge \bigwedge_{i=1}^n \text{DefÜberfahrt}(i) \end{aligned}$$

Methode zum Lösen des Rätsels:

- 1 Errate die benötigte Zahl n der Überfahrten.
- 2 Finde eine erfüllende Interpretation für die Formel $\text{Simpsons}(n)$ (z.B. mit Hilfe eines SAT-Solvers).

Eine mögliche Lösung:

$$n = 7,$$

$$I(MH_1) = I(HH_2) = I(GH_3) = I(MH_4) = I(KH_5) = I(HH_6) = I(MH_7) = 1$$

Gone Maggie gone (Fortsetzung)



„The Simpsons“, Staffel 20, Folge 13

Eigenschaften aussagenlogischer Modellierungen

Vorteile:

- *deklarativ-statisch, nicht prozedural-dynamisch*

Welche Eigenschaften sollen gelten?

Nicht: Welche Schritte sind für Lösung erforderlich?

- *modular*

Neue Bedingungen werden durch zusätzliche Formeln berücksichtigt.

Nachteile:

- *Erraten von Parametern*

n muss durch Probieren gefunden werden

- *Große Zahl an Variablen und Formeln*

Dynamik muss durch indizierte Variablen simuliert werden.

- *Frame Problem*

Bei jeder Aktion muss auch definiert werden, was sich nicht ändert.

- *unintuitiv*

Bei der Modellierung von Abläufen denkt man an Zustände und Übergänge, nicht an statische Bedingungen.