3.0 VU Formale Modellierung

Gernot Salzer

Forschungsbereich Theory and Logic
Institut für Logic and Computation

12.3.2019

Was Sie letztes Mal hörten

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen

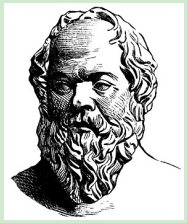
Organisatorisches

1. tiss.tuwien.ac.at
2. tuwel.tuwien.ac.at
3. „Infos zu Ablauf und Organisation“ (in TUWEL)

Was Sie letztes Mal hörten

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen
   - 3.3. Syntax und Semantik der Aussagenlogik
   - 3.4. Von der Funktion zur Formel
   - 3.5. Normalformen
   - 3.6. Das Erfüllbarkeitsproblem
   - 3.7. House
   - 3.8. Dualität von Funktionen, Operatoren und Formeln
   - 3.9. Gone Maggie gone

Die Logik untersucht allgemeine Prinzipien korrekten Schließens.



Alle Menschen sind sterblich.
Sokrates ist ein Mensch.
} Prämissen, Annahmen

Sokrates ist sterblich. — Konklusion, Folgerung

Inferenzregel

Alle x sind y.
z ist ein x.
---
z ist y.

x ... Mensch
y ... sterblich
z ... Sokrates

Kriterium für die Gültigkeit von Inferenzregeln

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

Unzulässige Inferenzen

Alle Menschen sind sterblich.
Sokrates ist sterblich.

Sokrates ist ein Mensch.

Sokrates ist ein Mensch.
Sokrates ist sterblich.

Alle Menschen sind sterblich.

Alle Menschen sind sterblich.			Alle x sind y.
Sokrates ist sterblich.		Inferenzregel:	z ist y.
Sokrates ist ein Mensch.			z ist ein x.

- Diese Regel erfüllt nicht das Kriterium.
- Gegenbeispiel: $x =$ Fußball, $y =$ rund, $z =$ Sonne

Alle Fußbälle sind rund.	wahr
Die Sonne ist rund.	wahr
Die Sonne ist ein Fußball.	falsch

- Die Inferenzregel ist daher nicht gültig,
  obwohl sie gelegentlich zu wahren Konklusionen führt.
  Aber eben nicht immer!

Unterscheidung von Logiken

... nach Wahrheitswerten:

- Zweiwertige Logik: wahr/falsch
- Mehrwertige Logiken: wahr/falsch/unbekannt/widersprüchlich, ...
- Fuzzy logic: [0,1] (alle reellen Zahlen zwischen 0 und 1)

... nach Quantoren:

- Aussagenlogik: keine Quantoren
- Quantifizierte Aussagenlogik: Quantoren über Aussagenvariablen
- Prädikatenlogik: Quantoren über Individuenvariablen
- Logiken höherer Stufen: Quantoren über Funktionen und Prädikate

... nach den Ausdrucksmöglichkeiten:

- Elementare Logik: und, oder, nicht, für alle, ...
- Zeitlogiken: im nächsten Moment, für immer, irgendwann später, ...
- Modallogiken: „ich glaube/weiß, dass“, „es ist möglich/notwendig, dass“, ...

... nach wahren/beweisbaren Formeln, nach Kalkülen, ...

Was Sie letztes Mal hörten

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen

Aussagenlogische Funktionen – Überblick

true	false
1	0
$\top$	$\bot$

x	not
1	0
0	1
	$\neg$

x	y	and	nand	or	nor	iff	xor	implies	if		
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
		$\wedge$	$\uparrow$	$\vee$	$\downarrow$	$\equiv$	$\not\equiv$	$\supset$	$\not\supset$	$\subset$	$\not\subset$

Eine Menge von Funktionen heißt vollständig (für eine Funktionsklasse), wenn damit alle Funktionen (der Klasse) ausgedrückt werden können.

$\{\text{not}, \text{and}, \text{or}\}$ ist vollständig für die aussagenlogischen Funktionen.

Begründung siehe später.

Die Mengen $\{\text{not}, \text{and}\}$, $\{\text{nand}\}$, $\{\text{not}, \text{or}\}$, $\{\text{nor}\}$, $\{\text{not}, \text{implies}\}$ und $\{\text{implies}, \text{false}\}$ sind ebenfalls funktional vollständig.

Was Sie heute erwartet

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen
   - 3.3. Syntax und Semantik der Aussagenlogik
   - 3.4. Von der Funktion zur Formel
   - 3.5. Normalformen
   - 3.6. Das Erfüllbarkeitsproblem
   - 3.7. House
   - 3.8. Dualität von Funktionen, Operatoren und Formeln
   - 3.9. Gone Maggie gone

Syntax versus Semantik

Syntax:

- Zeichenfolge, 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) one (englisch) 1 (mathematisch)	das abstrakte Konzept der Zahl „1“
Bug	Schiffsvorderteil (deutsch) Käfer, Programmfehler (englisch)

and, nand ... mathematische Funktionen

$$\left.\begin{array}{l} x \text{ and } y \\ (x \text{ nand } y) \text{ nand } (x \text{ nand } y) \end{array}\right\} \ldots \text{ ununterscheidbar, identische Funktion:}$$

x	y	x and y	$(x$ nand $y)$ nand $(x$ nand $y)$
1	1	1	1
1	0	0	0
0	1	0	0
0	0	0	0

Für Aussagen über die Form der Ausdrücke brauchen wir eine Formelsprache.

$$\left.\begin{array}{l} x \wedge y \\ (x \uparrow y) \uparrow (x \uparrow y) \end{array}\right\} \ldots \text{ unterschiedliche Zeichenketten mit } \begin{array}{c} 3 \\ 11 \end{array} \text{ Symbolen}$$

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:
  $G_1 = G_0 \cup \{ n+2 \mid n \in G_0 \} = \{0, 2\}$
  $G_2 = G_1 \cup \{ n+2 \mid n \in G_1 \} = \{0, 2, 4\}$
  $G_{i+1} = G_i \cup \{ n+2 \mid n \in G_i \} = \{0, 2, 4, \ldots, 2(i+1)\}$
- Die geraden Zahlen sind alle so konstruierten Zahlen:
  $\mathbb{G} = \lim_{i \to \infty} G_i = \bigcup_{i \geq 0} G_i$

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.

Beiden 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

$\mathcal{U}$ ... Universum, Menge aller relevanten Elemente
$\mathcal{M}_0 \subseteq \mathcal{U}$ ... Menge von Grundelementen
$f_1 : \mathcal{U}^{n_1} \mapsto \mathcal{U}$, $f_2 : \mathcal{U}^{n_2} \mapsto \mathcal{U}$, ... Konstruktionsfunktionen

Stufenweise Konstruktion der Menge $\mathcal{M}$

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

Induktive Definition der Menge $\mathcal{M}$

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

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

Aussagenlogik – Syntax

Ausdrücke wie x and y und $(x \text{ nand } y) \text{ nand } (x \text{ nand } y)$ sind ununterscheidbar (gleiche Funktion!). Um Aussagen über ihre Form treffen zu können, benötigen wir eine Formelsprache.

$\mathcal{V} = \{A, B, C, \ldots, A_0, A_1, \ldots\}$ 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) $\{\top, \bot\} \subseteq \mathcal{A}$ $\top$ und $\bot$ 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 $* \in \{\wedge, \uparrow, \vee, \downarrow, \equiv, \not\equiv, \supset, \subset\}$.
$(F * G)$ ist eine Formel, falls F und G welche sind und $*$ ein binäres Op.symbol ist.

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

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

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

(a4) $(F * G) \in \mathcal{A}$, wenn $F, G \in \mathcal{A}$ und $* \in \{\wedge, \uparrow, \vee, \downarrow, \equiv, \not\equiv, \supset, \subset\}$.

$((A \uparrow B) \uparrow (A \uparrow B))$ 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) $\{\top, \bot\} \subseteq \mathcal{A}$

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

(a4) $(F * G) \in \mathcal{A}$, wenn $F, G \in \mathcal{A}$ und $* \in \{\wedge, \uparrow, \vee, \downarrow, \equiv, \not\equiv, \supset, \subset\}$.

$A \wedge B$ 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) $\mathcal{V} \subseteq \mathcal{A}$

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

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

(a4) $(F * G) \in \mathcal{A}$, wenn $F, G \in \mathcal{A}$ und $* \in \{\wedge, \uparrow, \vee, \downarrow, \equiv, \not\equiv, \supset, \subset\}$.

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

$\mathcal{V} \cup \{„\top“, „\bot“\}$ ... Grundelemente

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

Aussagenlogik – Semantik

$((A \wedge \neg B) \supset \bot)$ – wahr oder falsch?

Hängt ab

- vom Wert der Variablen A und B und
- von der Bedeutung der Symbole $\wedge$, $\neg$, $\supset$ und $\bot$.

Interpretationen

$\mathbb{B} = \{1, 0\}$ ... Wahrheitswerte
$I \colon \mathcal{V} \mapsto \mathbb{B}$ ... Wahrheitsbelegung, Interpretation
$\mathcal{I} = \{\, I \mid I \colon \mathcal{V} \mapsto \mathbb{B} \,\}$ ... 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 $\mathrm{val} : \mathcal{I} \times \mathcal{A} \mapsto \mathbb{B}$:

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

(v2) $\mathrm{val}_I(\top) = 1$ und $\mathrm{val}_I(\bot) = 0$;

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

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

(v4) ist eine Abkürzung für:

$$\begin{aligned}
\mathrm{val}_I(\,(F \wedge G)\,) &= \mathrm{val}_I(F)\ \mathrm{and}\ \mathrm{val}_I(G)\\
\mathrm{val}_I(\,(F \vee G)\,) &= \mathrm{val}_I(F)\ \mathrm{or}\ \mathrm{val}_I(G)\\
\mathrm{val}_I(\,(F \equiv G)\,) &= \mathrm{val}_I(F)\ \mathrm{iff}\ \mathrm{val}_I(G)\\
\mathrm{val}_I(\,(F \supset G)\,) &= \mathrm{val}_I(F)\ \mathrm{implies}\ \mathrm{val}_I(G)\\
&\vdots
\end{aligned}$$

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

(v2) $\mathrm{val}_I(\top) = 1$ und $\mathrm{val}_I(\bot) = 0$;

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

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

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

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

Wahrheitstafel

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

A	B	$((A \wedge \neg B) \supset \bot)$
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:

$I(A) = 1$, $I(B) = 1$: $\mathrm{val}_I(\cdots) = \cdots = 1$

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

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

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

false
0
$\bot$

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
		$\wedge$	$\supset$

Eine Formel F heißt

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

$((A \wedge \neg B) \supset \bot)$ ist erfüllbar und widerlegbar.

A	B	$((A \wedge \neg B) \supset \bot)$
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

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

Zwei Formeln F und G heißen äquivalent, geschrieben $F = G$, wenn $\mathrm{val}_I(F) = \mathrm{val}_I(G)$ 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

Äquivalenz bleibt bei der Ersetzung von Variablen durch Formeln erhalten.

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

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

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

Semantische Äquivalenz

Zwei Formeln F und G heißen äquivalent, geschrieben $F = G$, wenn $\mathrm{val}_I(F) = \mathrm{val}_I(G)$ 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

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.

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

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

Das heißt, es gelten folgende Gleichungen.

$(A \wedge B) \wedge C = A \wedge (B \wedge C)$	$(A \vee B) \vee C = A \vee (B \vee C)$	Assoziativität
$A \wedge B = B \wedge A$	$A \vee B = B \vee A$	Kommutativität
$A \wedge A = A$	$A \vee A = A$	Idempotenz
$A \wedge \top = A$	$A \vee \bot = A$	Neutralität
$A \wedge \neg A = \bot$	$A \vee \neg A = \top$	Komplement
$A \wedge (A \vee B) = A$	$A \vee (A \wedge B) = A$	Absorption
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$		Distributivität
$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$		

Schreibvereinfachung: keine Außenklammern, keine Klammern bei geschachteltem $\wedge$ oder $\vee$ (Assoziativität!)

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

$\langle 2^M, \cap, \cup, \overline{\ }, \emptyset, M \rangle$ ... Beispiel einer anderen Booleschen Algebra
2^M ... Menge aller Teilmengen der Menge M, Potenzmenge
$\overline{X}$ ... Komplement der Menge X bzgl. M

Weitere Äquivalenzen

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

$$A \uparrow B = \neg A \vee \neg B \qquad A \equiv B = (\neg A \vee B) \wedge (A \vee \neg B)$$
$$A \downarrow B = \neg A \wedge \neg B \qquad = (A \wedge B) \vee (\neg A \wedge \neg B)$$
$$A \supset B = \neg A \vee B \qquad A \not\equiv B = (\neg A \vee \neg B) \wedge (A \vee B)$$
$$A \subset B = A \vee \neg B \qquad = (A \wedge \neg B) \vee (\neg A \wedge B)$$

Verschieben der Negation

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

Äquivalenzen für $\top$ und $\bot$

$$A \wedge \top = A \qquad A \wedge \bot = \bot \qquad A \wedge \neg A = \bot \qquad \neg\top = \bot$$
$$A \vee \bot = A \qquad A \vee \top = \top \qquad A \vee \neg A = \top \qquad \neg\bot = \top$$

$$
\begin{aligned}
& (X \uparrow Y) \uparrow (\top \uparrow Y) && A \uparrow B = \neg A \vee \neg B \\
= {} & (\neg X \vee \neg Y) \uparrow (\neg \top \vee \neg Y) && A \uparrow B = \neg A \vee \neg B \\
= {} & \neg(\neg X \vee \neg Y) \vee \neg(\neg \top \vee \neg Y) && \neg(A \vee B) = \neg A \wedge \neg B \\
= {} & (\neg\neg X \wedge \neg\neg Y) \vee (\neg\neg \top \wedge \neg\neg Y) && \neg\neg A = A \\
= {} & (X \wedge Y) \vee (\top \wedge Y) && A \wedge \top = A, \text{ Komm. } \wedge \\
= {} & (X \wedge Y) \vee Y && A \vee (A \wedge B) = A, \text{ Komm. } \wedge, \vee \\
= {} & Y
\end{aligned}
$$

Logische Konsequenz

$F_1, \ldots, F_n \models_I G$: „Aus $\mathrm{val}_I(F_1) = \cdots = \mathrm{val}_I(F_n) = 1$ folgt $\mathrm{val}_I(G) = 1$.“

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

$I(A)$	$I(B)$	A	$A \vee B$		B
1	1	1	1	✓	1
1	0	1	1	↯	0
0	1	0	1	✓	1
0	0	0	0	✓	0

Logische Konsequenz

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

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

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

Konvention: „$\models G$“ $(n = 0)$ bedeutet „G ist 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 $\mathrm{val}_I(A) = \mathrm{val}_I(A \vee B) = 1$,
aber $\mathrm{val}_I(B) \neq 1$!

I heißt Gegenbeispiel.

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

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

$$\frac{A \qquad A \supset B}{B} \qquad \frac{x \qquad \text{Wenn } x\text{, dann } y.}{y}$$

Ist eine gültige Inferenzregel!

Kriterium für die Gültigkeit von Inferenzregeln

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

Äquivalenz, Konsequenz und Gültigkeit

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

Deduktionstheorem

G folgt aus $F_1, \ldots, F_n$ genau dann, wenn $F_n \supset G$ aus $F_1, \ldots, F_{n-1}$ folgt.

$F_1, \ldots, F_n \models G$ genau dann, wenn $F_1, \ldots, F_{n-1} \models F_n \supset G$.

Mehrfache Anwendung liefert:

$F_1, \ldots, F_n \models G$ genau dann, wenn $F_1 \supset (F_2 \supset \cdots (F_n \supset G) \cdots)$ gültig.

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

$F_1, \ldots, F_n \models G$ genau dann, wenn $(F_1 \wedge \cdots \wedge F_n) \supset G$ gültig.

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

Ist nicht in jeder Logik möglich!

Was Sie heute erwartet

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen
   - 3.3. Syntax und Semantik der Aussagenlogik
   - 3.4. Von der Funktion zur Formel
   - 3.5. Normalformen
   - 3.6. Das Erfüllbarkeitsproblem
   - 3.7. House
   - 3.8. Dualität von Funktionen, Operatoren und Formeln
   - 3.9. Gone Maggie gone

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.

Von der Funktion zur Formel

Gegeben: Funktion $f : \mathbb{B}^n \mapsto \mathbb{B}$ (z.B. als Wahrheitstafel)
Gesucht: Formel, die f darstellt

A	B	C	$F[A, B, C]$?
x	y	z	$f(x, y, z)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Von der Funktion zur Formel

Gegeben: Funktion $f : \mathbb{B}^n \mapsto \mathbb{B}$ (z.B. als Wahrheitstafel)
Gesucht: Formel, die f darstellt

A	B	C	$F[A,B,C] := (A \wedge B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C)$			
x	y	z	$f(x,y,z)$			
1	1	1	1	1	0	0
1	1	0	0	0	0	0
1	0	1	0	0	0	0
1	0	0	1	0	1	0
0	1	1	1	0	0	1
0	1	0	0	0	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

DNF_f ... „Disjunktive Normalform zur Funktion f“

Von der Funktion zur Formel

Gegeben: Funktion $f : \mathbb{B}^n \mapsto \mathbb{B}$ (z.B. als Wahrheitstafel)
Gesucht: Formel, die f darstellt

A	B	C	$F[A, B, C]$?
x	y	z	$f(x, y, z)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

Von der Funktion zur Formel

Gegeben: Funktion $f : \mathbb{B}^n \mapsto \mathbb{B}$ (z.B. als Wahrheitstafel)
Gesucht: Formel, die f darstellt

A	B	C	$F[A,B,C] := (\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge \cdots$				
x	y	z	$f(x,y,z)$				
1	1	1	1	1	1	1	1 1
1	1	0	0	0	1	1	1 1
1	0	1	0	1	0	1	1 1
1	0	0	1	1	1	1	1 1
0	1	1	1	1	1	1	1 1
0	1	0	0	1	1	0	1 1
0	0	1	0	1	1	1	0 1
0	0	0	0	1	1	1	1 0

KNF_f ... „Konjunktive Normalform zur Funktion f“

Von der Funktion $f : \mathbb{B}^n \mapsto \mathbb{B}$ zur Formel DNF_f

Notation: $\bigwedge\{F, G, H, \dots\} = F \wedge G \wedge H \wedge \cdots \qquad \bigwedge\{\} = \top$

$\bigvee\{F, G, H, \dots\} = F \vee G \vee H \vee \cdots \qquad \bigvee\{\} = \bot$

Charakteristisches Konjunkt für $\vec{b} = (b_1, \dots, b_n) \in \mathbb{B}^n$:

$K_{\vec{b}} = \bigwedge\{ A_i \mid b_i = 1,\ i = 1..n \} \wedge \bigwedge\{ \neg A_i \mid b_i = 0,\ i = 1..n \}$

$\vec{b} = (1, 0, 1, 1) \quad \Longrightarrow \quad K_{\vec{b}} = A_1 \wedge \neg A_2 \wedge A_3 \wedge A_4$

$I_{\vec{b}}$ ... Interpretation definiert durch $I_{\vec{b}}(A_i) = b_i$

$K_{\vec{b}}$ hat den Wert 1 für $I_{\vec{b}}$, und 0 für alle anderen Interpretationen.

$I_{\vec{b}}$: $A_1 \mapsto 1,\ A_2 \mapsto 0,\ A_3 \mapsto 1,\ A_4 \mapsto 1 \quad \Longrightarrow \quad \mathrm{val}_{I_{\vec{b}}}(K_{\vec{b}}) = 1$

Disjunktive Normalform für $f : \mathbb{B}^n \mapsto \mathbb{B}$

$\mathrm{DNF}_f = \bigvee\{ K_{\vec{b}} \mid f(\vec{b}) = 1,\ \vec{b} \in \mathbb{B}^n \}$ repräsentiert die Funktion f, d.h.:

$\mathrm{val}_{I_{\vec{b}}}(\mathrm{DNF}_f) = f(\vec{b})$ für alle $\vec{b} \in \mathbb{B}^n$.

Von der Funktion $f : \mathbb{B}^n \mapsto \mathbb{B}$ zur Formel KNF_f

Notation: $\bigwedge\{F, G, H, \dots\} = F \wedge G \wedge H \wedge \cdots \qquad \bigwedge\{\} = \top$

$\bigvee\{F, G, H, \dots\} = F \vee G \vee H \vee \cdots \qquad \bigvee\{\} = \bot$

Charakteristisches Disjunkt für $\vec{b} = (b_1, \dots, b_n) \in \mathbb{B}^n$:

$D_{\vec{b}} = \bigvee\{ A_i \mid b_i = 0,\ i = 1..n \} \vee \bigvee\{ \neg A_i \mid b_i = 1,\ i = 1..n \}$

$\vec{b} = (1, 0, 1, 1) \quad \Longrightarrow \quad D_{\vec{b}} = \neg A_1 \vee A_2 \vee \neg A_3 \vee \neg A_4$

$I_{\vec{b}}$ ... Interpretation definiert durch $I_{\vec{b}}(A_i) = b_i$

$D_{\vec{b}}$ hat den Wert 0 für $I_{\vec{b}}$, und 1 für alle anderen Interpretationen.

$I_{\vec{b}}$: $A_1 \mapsto 1,\ A_2 \mapsto 0,\ A_3 \mapsto 1,\ A_4 \mapsto 1 \quad \Longrightarrow \quad \mathrm{val}_{I_{\vec{b}}}(D_{\vec{b}}) = 0$

Konjunktive Normalform für $f : \mathbb{B}^n \mapsto \mathbb{B}$

$\mathrm{KNF}_f = \bigwedge\{ D_{\vec{b}} \mid f(\vec{b}) = 0,\ \vec{b} \in \mathbb{B}^n \}$ repräsentiert die Funktion f, d.h.:

$\mathrm{val}_{I_{\vec{b}}}(\mathrm{KNF}_f) = f(\vec{b})$ für alle $\vec{b} \in \mathbb{B}^n$.

A_1	A_2	A_3			
	$\vec{b}$		$f(\vec{b})$	$K_{\vec{b}}$	$D_{\vec{b}}$
1	1	1	1	$A_1 \wedge A_2 \wedge A_3 =: K_{111}$	
1	1	0	0		$\neg A_1 \vee \neg A_2 \vee A_3 =: D_{110}$
1	0	1	0		$\neg A_1 \vee A_2 \vee \neg A_3 =: D_{101}$
1	0	0	1	$A_1 \wedge \neg A_2 \wedge \neg A_3 =: K_{100}$	
0	1	1	1	$\neg A_1 \wedge A_2 \wedge A_3 =: K_{011}$	
0	1	0	0		$A_1 \vee \neg A_2 \vee A_3 =: D_{010}$
0	0	1	0		$A_1 \vee A_2 \vee \neg A_3 =: D_{001}$
0	0	0	0		$A_1 \vee A_2 \vee A_3 =: D_{000}$

$\mathrm{DNF}_f = K_{111} \vee K_{100} \vee K_{011}$

$\mathrm{KNF}_f = D_{110} \wedge D_{101} \wedge D_{010} \wedge D_{001} \wedge D_{000}$

Folgerung:

$\{\mathrm{not}, \mathrm{and}, \mathrm{or}\}$ ist funktional vollständig.

Was Sie heute erwartet

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen
   - 3.3. Syntax und Semantik der Aussagenlogik
   - 3.4. Von der Funktion zur Formel
   - 3.5. Normalformen
   - 3.6. Das Erfüllbarkeitsproblem
   - 3.7. House
   - 3.8. Dualität von Funktionen, Operatoren und Formeln
   - 3.9. Gone Maggie gone

Normalformen

Literal: Variable oder negierte Variable, also A, $\neg A$, B, $\neg B$, ...

Negationsnormalform (NNF)

- Literale sowie $\top$ und $\bot$ sind in NNF.
- $(F \wedge G)$ und $(F \vee G)$ sind in NNF, wenn F und G in NNF sind.
- Keine Formel sonst ist in NNF.

NNF: $(\neg A \vee ((B \vee \neg C) \wedge \top))$ Keine NNFs: $\neg\neg A$, $\neg(A \wedge B)$, $\neg\bot$
DNF_f und KNF_f sind Formeln in NNF.

Disjunktive Normalform (DNF)

$\top$, $\bot$ sowie Disjunktionen von Konjunktion von Literalen:
$(^{(\neg)}A_{1,1} \wedge {}^{(\neg)}A_{1,2} \wedge {}^{(\neg)}A_{1,3} \wedge \cdots) \vee (^{(\neg)}A_{2,1} \wedge {}^{(\neg)}A_{2,2} \wedge {}^{(\neg)}A_{2,3} \wedge \cdots) \vee \cdots$

Konjunktive Normalform (KNF)

$\top$, $\bot$ sowie Konjunktionen von Disjunktion von Literalen:
$(^{(\neg)}A_{1,1} \vee {}^{(\neg)}A_{1,2} \vee {}^{(\neg)}A_{1,3} \vee \cdots) \wedge (^{(\neg)}A_{2,1} \vee {}^{(\neg)}A_{2,2} \vee {}^{(\neg)}A_{2,3} \vee \cdots) \wedge \cdots$

Normalformen

Formeln, die gleichzeitig in DNF und KNF sind:

- $\top$
- $\bot$
- $(\neg)A_1 \wedge (\neg)A_2 \wedge \cdots \wedge (\neg)A_n$
- $(\neg)A_1 \vee (\neg)A_2 \vee \cdots \vee (\neg)A_n$

Normalformen für die Funktion f von vorhin

$\mathrm{DNF}_f = K_{111} \vee K_{100} \vee K_{011}$	kanonische (maximale) DNF, NNF
$(A_2 \wedge A_3) \vee (A_1 \wedge \neg A_2 \wedge \neg A_3)$	minimale DNF, NNF
$\mathrm{KNF}_f = D_{110} \wedge D_{101} \wedge D_{010} \wedge D_{001} \wedge D_{000}$	kanonische KNF, NNF
$(A_1 \vee A_3) \wedge (\neg A_2 \vee A_3) \wedge (A_2 \vee \neg A_3)$	minimale KNF, NNF
$(A_1 \vee A_2) \wedge (\neg A_2 \vee A_3) \wedge (A_2 \vee \neg A_3)$	andere minimale KNF, NNF

Normalformen sind in der Regel nicht eindeutig.
Typische Problemstellung: Finde kleine oder kleinste Normalform.

Normalformen

Weitere Normalformen:

- Beschränkung auf andere Operatoren, etwa $\uparrow$
- Andere Einschränkungen der Struktur, etwa
  Konjunktion von Disjunktionen von Konjunktionen von Literalen
  (ermöglicht kleinere Formeln als DNF oder KNF)

Noch mehr Normalformen für die Funktion f von vorhin

$$(A_2 \uparrow A_3) \uparrow (A_1 \uparrow ((A_2 \uparrow A_2) \uparrow (A_3 \uparrow A_3) \uparrow (A_2 \uparrow A_2) \uparrow (A_3 \uparrow A_3)))$$

$$((A_1 \wedge \neg A_3) \vee A_2) \wedge (\neg A_2 \vee A_3) \qquad \text{NNF}$$

Konstruktion von DNFs/KNFs – Semantische Methode

Gegeben: Aussagenlogische Formel F
Gesucht: Äquivalente Formel in DNF/KNF

1. Stelle die zu F gehörige Funktion f als Wahrheitstafel dar.
2. Konstruiere DNF_f bzw. KNF_f.

A_1	A_2	A_3	$F := (A_1 \supset (A_2 \equiv A_3)) \wedge (\neg A_1 \supset (A_2 \wedge A_3))$		
1	1	1	1	K_{111}	
1	1	0	0		D_{110}
1	0	1	0		D_{101}
1	0	0	1	K_{100}	
0	1	1	1	K_{011}	
0	1	0	0		D_{010}
0	0	1	0		D_{001}
0	0	0	0		D_{000}

DNF: $F = K_{111} \vee K_{100} \vee K_{011}$
KNF: $F = D_{110} \wedge D_{101} \wedge D_{010} \wedge D_{001} \wedge D_{000}$

Konstruktion von DNFs/KNFs – Algebraische Methode

Gegeben: Aussagenlogische Formel F
Gesucht: Äquivalente Formel in DNF/KNF

1. Ersetze alle Junktoren durch $\wedge$, $\vee$ und $\neg$.
   $A \uparrow B = \neg A \vee \neg B \qquad A \downarrow B = \neg A \wedge \neg B \qquad A \supset B = \neg A \vee B \qquad A \subset B = A \vee \neg B$
   $A \equiv B = (\neg A \vee B) \wedge (A \vee \neg B) = (A \wedge B) \vee (\neg A \wedge \neg B)$
   $A \not\equiv B = (\neg A \vee \neg B) \wedge (A \vee B) = (A \wedge \neg B) \vee (\neg A \wedge B)$
2. Verschiebe Negationen nach innen, eliminiere Doppelnegationen.
   $\neg(A \wedge B) = \neg A \vee \neg B \qquad \neg(A \vee B) = \neg A \wedge \neg B \qquad \neg\neg A = A$
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 $\bot$.
   $A \wedge \top = A \qquad A \wedge \bot = \bot \qquad A \wedge \neg A = \bot \qquad \neg\top = \bot$
   $A \vee \bot = A \qquad A \vee \top = \top \qquad A \vee \neg A = \top \qquad \neg\bot = \top$

(Äquivalenzen werden hier von links nach rechts angewendet.)

$((A_1 \uparrow A_2) \supset \neg A_2) \wedge (\neg A_1 \supset (A_2 \wedge \bot))$

1. Ersetze alle Junktoren durch $\wedge$, $\vee$ und $\neg$:
   $(\ \ (\neg A_1 \vee \neg A_2) \supset \neg A_2) \wedge (\ \neg A_1 \supset (A_2 \wedge \bot))$
   $(\neg(\neg A_1 \vee\ \neg A_2) \vee \neg A_2) \wedge (\ \neg A_1 \supset (A_2 \wedge \bot))$
   $(\neg(\neg A_1 \vee\ \neg A_2) \vee \neg A_2) \wedge (\neg\neg A_1 \vee (A_2 \wedge \bot))$
2. Verschiebe Negationen nach innen, eliminiere Doppelnegationen:
   $((\neg\neg A_1 \wedge \neg\neg A_2) \vee \neg A_2) \wedge (\neg\neg A_1 \vee (A_2 \wedge \bot))$
   $(\quad (A_1 \wedge \quad A_2) \vee \neg A_2) \wedge (\quad A_1 \vee (A_2 \wedge \bot))$
3. Wende das Distributivgesetz an:

DNF: $(((A_1 \wedge A_2) \vee \neg A_2) \wedge A_1) \vee (((A_1 \wedge A_2) \vee \neg A_2) \wedge (A_2 \wedge \bot))$
$(((A_1 \wedge A_2) \vee \neg A_2) \wedge A_1) \vee (A_1 \wedge A_2 \wedge A_2 \wedge \bot) \vee (\neg A_2 \wedge A_2 \wedge \bot)$
$(A_1 \wedge A_2 \wedge A_1) \vee (\neg A_2 \wedge A_1) \vee (A_1 \wedge A_2 \wedge A_2 \wedge \bot) \vee (\neg A_2 \wedge A_2 \wedge \bot)$
$(A_1 \wedge A_2) \vee (\neg A_2 \wedge A_1) \vee (A_1 \wedge A_2 \wedge \bot) \vee (\neg A_2 \wedge A_2 \wedge \bot)$ (Idemp.)

KNF: $(A_1 \vee \neg A_2) \wedge (A_2 \vee \neg A_2) \wedge (A_1 \vee (A_2 \wedge \bot))$
$(A_1 \vee \neg A_2) \wedge (A_2 \vee \neg A_2) \wedge (A_1 \vee A_2) \wedge (A_1 \vee \bot)$

4. Vereinfache mit den Regeln für $\top$ und $\bot$:

DNF: $(A_1 \wedge A_2) \vee (\neg A_2 \wedge A_1) \vee (A_1 \wedge A_2 \wedge \bot) \vee (\neg A_2 \wedge A_2 \wedge \bot)$

$(A_1 \wedge A_2) \vee (\neg A_2 \wedge A_1) \vee (A_1 \wedge A_2 \wedge \bot) \vee \bot$

$(A_1 \wedge A_2) \vee (\neg A_2 \wedge A_1) \vee (A_1 \wedge A_2 \wedge \bot)$

$(A_1 \wedge A_2) \vee (\neg A_2 \wedge A_1) \vee \bot$

$(A_1 \wedge A_2) \vee (\neg A_2 \wedge A_1)$ DNF erreicht!

$A_1 \wedge (A_2 \vee \neg A_2)$ (Distributivgesetz, keine DNF mehr)

$A_1 \wedge \top$

A_1 (wieder DNF)

KNF: $(A_1 \vee \neg A_2) \wedge (A_2 \vee \neg A_2) \wedge (A_1 \vee A_2) \wedge (A_1 \vee \bot)$

$(A_1 \vee \neg A_2) \wedge (A_2 \vee \neg A_2) \wedge (A_1 \vee A_2) \wedge A_1$ KNF erreicht!

$(A_1 \vee \neg A_2) \wedge (A_2 \vee \neg A_2) \wedge A_1$ (Absorption)

$(A_1 \vee \neg A_2) \wedge \top \wedge A_1$ (keine KNF mehr!)

$(A_1 \vee \neg A_2) \wedge A_1$ (wieder KNF)

A_1 (Absorption)

Welche Methode ist besser?

Gefühlsmäßig: Die semantische Methode ist übersichtlicher.

Theoretisch: Beide Methoden sind schlecht, denn beide sind im schlechtesten Fall exponentiell.

- Semantische Methode: Aufwand immer exponentiell in Variablenzahl! Wahrheitstafel besitzt $2^{\text{Variablenzahl}}$ Zeilen.
- Algebraische Methode: Schritt 3 (Distributivgesetz) ist aufwändig, kann zu einer exponentiellen Verlängerung der Formel führen.

Praktisch:

- Semantische Methode nur brauchbar bei Formeln mit sehr wenigen Variablen. Immer exponentiell in Variablenzahl, liefert immer die maximale DNF/KNF.
- Algebraische Methode teilweise auch für große Formeln brauchbar, insbesondere mit Computerunterstützung. Kann auch kleine DNFs/KNFs liefern.

Was Sie heute erwartet

1. Organisatorisches
2. Was bedeutet Modellierung?
3. Aussagenlogik
   - 3.1. Was ist Logik?
   - 3.2. Aussagenlogische Funktionen
   - 3.3. Syntax und Semantik der Aussagenlogik
   - 3.4. Von der Funktion zur Formel
   - 3.5. Normalformen
   - 3.6. Das Erfüllbarkeitsproblem
   - 3.7. House
   - 3.8. Dualität von Funktionen, Operatoren und Formeln
   - 3.9. 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:

$$
\begin{aligned}
G \text{ gültig} &\iff \neg G \text{ unerfüllbar} \\
G \text{ widerlegbar} &\iff \neg G \text{ erfüllbar} \\
G = H &\iff G \not\equiv H \text{ unerfüllbar} \\
F_1, \ldots, F_n \models G &\iff F_1 \wedge \cdots \wedge F_n \wedge \neg G \text{ unerfüllbar}
\end{aligned}
$$

Methoden zur Lösung von SAT

Wahrheitstafel:

- 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 $\bot$ 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!

$1.000.000,– Prämie für einen effizienten SAT-Solver

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

Abzuholen beim Clay Mathematics Institute (www.claymath.org)
für das offene Milleniumsproblem „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 $\mathrm{P} = \mathrm{NP}$ oder $\mathrm{P} \neq \mathrm{NP}$ (gleichbedeutend mit $\mathrm{P} \subsetneq \mathrm{NP}$)?

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

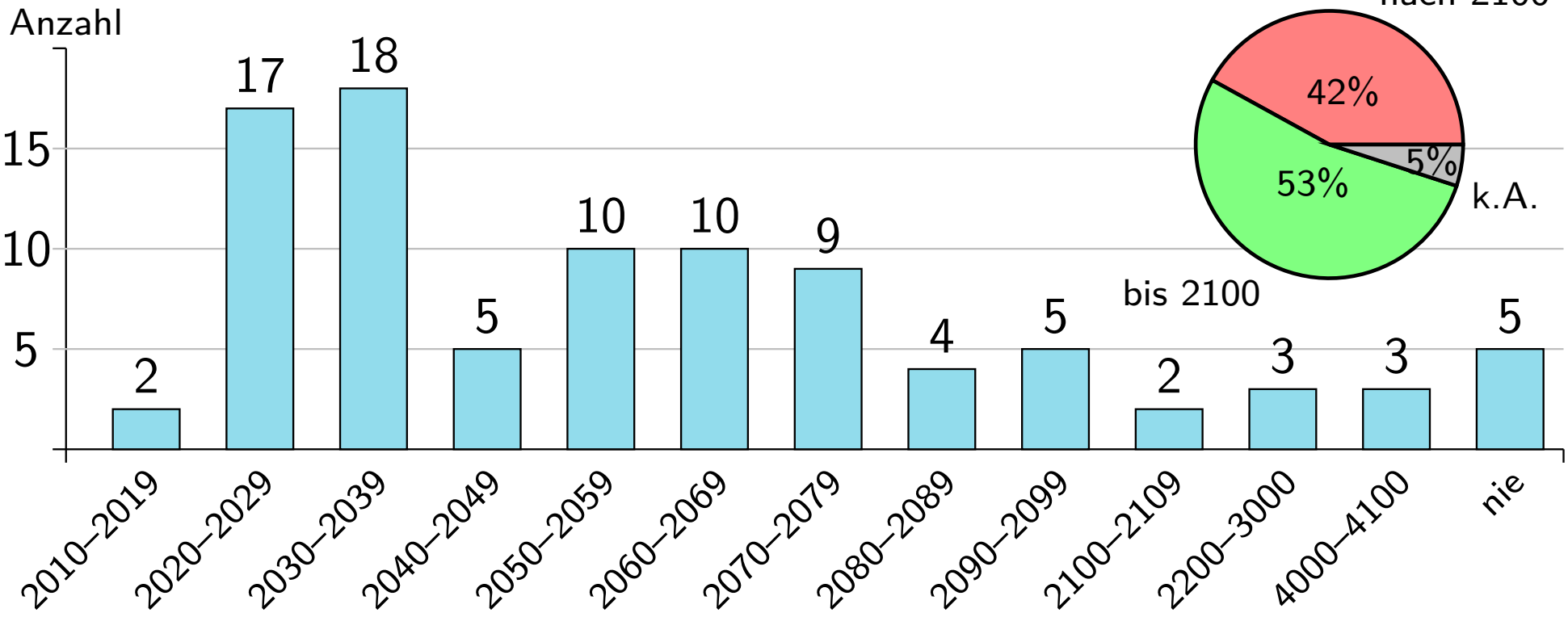
Gegeben: eine aussagenlogische Formel.
Frage: Ist die Formel erfüllbar?

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

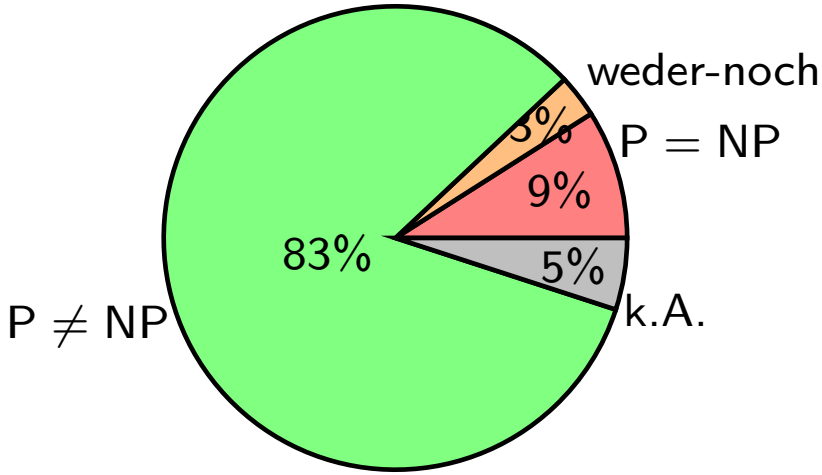
SAT polynomiell lösbar $\Longrightarrow$ P = NP

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

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



Wie wird die Antwort lauten?



[W.I.Gasarch, 2012, Meinungsumfrage unter 152 Experten]

Falls Sie SAT nicht ausreichend inspiriert . . .

MINESWEEPER ist NP-vollständig

Gegeben: eine Minesweeper-Stellung
Frage: Ist die Stellung möglich?

Beispiel einer unmöglichen Stellung:

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

MINESWEEPER polynomiell lösbar $\Longrightarrow$ P = NP

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

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