3.0 VU Formale Modellierung

Gernot Salzer

Forschungsbereich Theory and Logic
Institut für Logic and Computation

19.3.2019

Nächste Vorlesung:

Morgen, 20.3.2019, 15:15, AudiMax

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

Induktive Definitionen

$\mathcal{U}$ ... 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 $\mathcal{M}$

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

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 $f_2(x_1, \ldots, x_{n_2}) \in \mathcal{M}$.
- ...

Beispiel: Geschachtelte Klammern

Gesucht: Spezifikation aller richtig geschachtelten Folgen von runden, eckigen und geschwungenen Klammern, wie etwa `([[{()}]])`

Induktive Definition:

Die Menge $\mathcal{K}$ der Klammernfolgen ist die kleinste Menge, für die gilt:

(k1) $\texttt{()}, \texttt{[]}, \texttt{\{\}} \in \mathcal{K}$ alternativ: $\{\texttt{()}, \texttt{[]}, \texttt{\{\}}\} \subseteq \mathcal{K}$

(k2) Wenn $x \in \mathcal{K}$, dann auch $\texttt{(}x\texttt{)} \in \mathcal{K}$.

(k3) Wenn $x \in \mathcal{K}$, dann auch $\texttt{[}x\texttt{]} \in \mathcal{K}$.

(k4) Wenn $x \in \mathcal{K}$, dann auch $\texttt{\{}x\texttt{\}} \in \mathcal{K}$.

Wir zeigen, dass `([[{()}]])` in der Menge $\mathcal{K}$ liegt.

1. $\texttt{()} \in \mathcal{K}$ wegen (k1)
2. Da $\texttt{()} \in \mathcal{K}$, gilt auch $\texttt{\{()\}} \in \mathcal{K}$. wegen (k4)
3. Da $\texttt{\{()\}} \in \mathcal{K}$, gilt auch $\texttt{[\{()\}]} \in \mathcal{K}$. wegen (k3)
4. Da $\texttt{[\{()\}]} \in \mathcal{K}$, gilt auch $\texttt{[[\{()\}]]} \in \mathcal{K}$. wegen (k3)
5. Da $\texttt{[[\{()\}]]} \in \mathcal{K}$, gilt auch $\texttt{([[\{()\}]])} \in \mathcal{K}$. wegen (k2)

Aussagenlogik – Syntax

$\mathcal{V} = \{A, B, C, \dots, A_0, A_1, \dots\}$ 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) $\{\top, \bot\} \subseteq \mathcal{A}$ $\top$ 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.

$\neg(((A \vee B) \equiv \neg(B \downarrow C)) \subset ((A \vee \bot) \wedge B)) \ \in \mathcal{A}$

Aussagenlogik – Semantik

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

Semantik aussagenlogischer Formeln

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

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

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

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

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

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:

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

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

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

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

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.

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

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

$F = G$ gilt genau dann, wenn $F \equiv G$ eine gültige Formel ist.

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

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

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

Distributivität

Weitere Äquivalenzen

$$\begin{array}{rcl}
A \uparrow B = \neg A \vee \neg B & A \equiv B = (\neg A \vee B) \wedge (A \vee \neg B) & \neg(A \wedge B) = \neg A \vee \neg B \\
A \downarrow B = \neg A \wedge \neg B & = (A \wedge B) \vee (\neg A \wedge \neg B) & \neg(A \vee B) = \neg A \wedge \neg B \\
A \supset B = \neg A \vee B & A \not\equiv B = (\neg A \vee \neg B) \wedge (A \vee B) & \neg\neg A = A \\
A \subset B = A \vee \neg B & = (A \wedge \neg B) \vee (\neg A \wedge B) &
\end{array}$$

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

Logische Konsequenz

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

Logische Konsequenz

Die Formel G folgt aus den Formeln $F_1, \dots, F_n$, geschrieben $F_1, \dots, F_n \models G$, wenn $F_1, \dots, F_n \models_I G$ für alle Interpretationen I gilt.

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

$A,\ A \supset B \models B$

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

$A,\ A \vee B \not\models B$

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

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

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

Von der Funktion zur Formel

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

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

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

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

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
4. Endliche Automaten

Normalformen

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

Negationsnormalform (NNF)

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

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

Disjunktive Normalform (DNF)

$\top$, $\bot$ sowie Disjunktionen von Konjunktion von Literalen:

$$({\scriptstyle(\neg)}A_{1,1} \land {\scriptstyle(\neg)}A_{1,2} \land {\scriptstyle(\neg)}A_{1,3} \land \cdots) \lor ({\scriptstyle(\neg)}A_{2,1} \land {\scriptstyle(\neg)}A_{2,2} \land {\scriptstyle(\neg)}A_{2,3} \land \cdots) \lor \cdots$$

Konjunktive Normalform (KNF)

$\top$, $\bot$ sowie Konjunktionen von Disjunktion von Literalen:

$$({\scriptstyle(\neg)}A_{1,1} \lor {\scriptstyle(\neg)}A_{1,2} \lor {\scriptstyle(\neg)}A_{1,3} \lor \cdots) \land ({\scriptstyle(\neg)}A_{2,1} \lor {\scriptstyle(\neg)}A_{2,2} \lor {\scriptstyle(\neg)}A_{2,3} \lor \cdots) \land \cdots$$

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

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

$((A_1 \land \neg A_3) \lor A_2) \land (\neg A_2 \lor A_3)$ 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 $\neg$:
   $(\quad (\neg A_1 \vee \neg A_2) \supset \neg A_2) \wedge (\ \neg A_1 \supset (A_2 \wedge \bot))$
   $(\neg(\neg A_1 \vee \neg A_2) \vee \neg A_2) \wedge (\ \neg A_1 \supset (A_2 \wedge \bot))$
   $(\neg(\neg A_1 \vee \neg A_2) \vee \neg A_2) \wedge (\neg\neg A_1 \vee (A_2 \wedge \bot))$
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

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 $\mathrm{val}_I(F) = 1$?

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:

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

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 $\perp$ 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!

$ 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

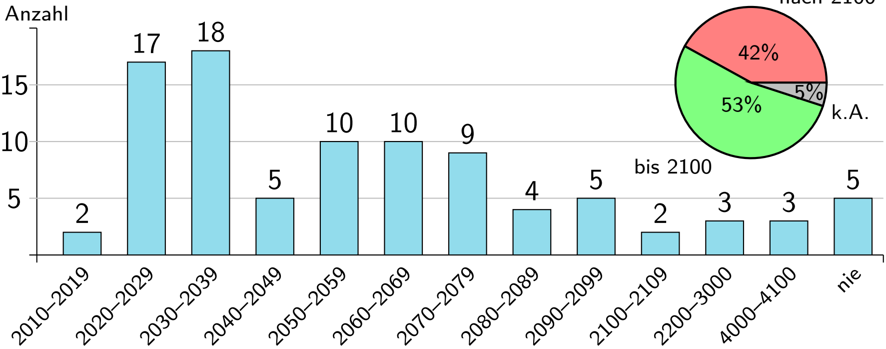
Gegeben: eine aussagenlogische Formel.
Frage: Ist die Formel erfüllbar?

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

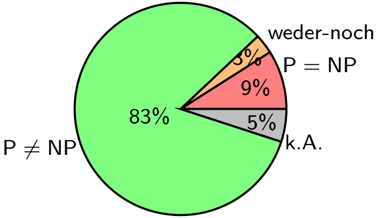
SAT polynomiell lösbar $\Longrightarrow \mathsf{P} = \mathsf{NP}$

SAT nicht polynomiell lösbar $\Longrightarrow \mathsf{P} \neq \mathsf{NP}$

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.

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
4. Endliche Automaten

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: $A =$ „krank“ oder $A =$ „Fieber“.

Möglich: $A =$ „Max ist krank“ oder $A =$ „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 zusammenfasst 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.	$F_1 := F \wedge S$
House: „Wenn der Patient Fieber hat, handelt es sich um Grippe oder Erkältung."	$F_2 := F \supset (G \vee E)$
Cameron: „Wenn er keine starken Gliederschmerzen hat, dann hat er auch keine Grippe."	$F_3 := \neg S \supset \neg G$
House: „Jedenfalls weisen hohes Fieber und starke Gliederschmerzen immer auf Grippe hin."	$F_4 := (F \wedge S) \supset G$
Cameron: "Er hat sicher nicht beide Krankheiten gleichzeitig."	$F_5 := \neg(G \wedge E)$

House – Diagnose

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

Methode 1: Wahrheitstafel

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

F	S	G	E	F_1	$F \supset (G \vee E)$	$\neg S \supset \neg G$	$(F \wedge S) \supset G$	$\neg(G \wedge E)$
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

$I(G) = 1$, $I(E) = 0 \Longrightarrow$ 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 $F_1 \wedge \cdots \wedge F_5 \wedge F_6$ das Ergebnis „unerfüllbar", es gibt also keine weiteren Lösungen.

Methode 3: Umwandlung in DNF und Vereinfachung

$$\overbrace{F \land S}^{F_1} \land \overbrace{(\neg F \lor G \lor E)}^{F_2} \land \overbrace{(S \lor \neg G)}^{F_3} \land \overbrace{(\neg F \lor \neg S \lor G)}^{F_4} \land \overbrace{(\neg G \lor \neg E)}^{F_5}$$

$$(\underbrace{(F \land S \land \neg F)}_{=\bot} \lor (F \land S \land G) \lor (F \land S \land E)) \land \cdots$$

$$((F \land S \land G) \lor (F \land S \land E)) \land (S \lor \neg G) \land \cdots$$

$$((F \land S \land G) \lor (F \land S \land E) \lor \underbrace{(F \land S \land G \land \neg G)}_{=\bot} \lor \underbrace{(F \land S \land E \land \neg G)}_{\text{Absorption } F \land S \land E}) \land \cdots$$

$$((F \land S \land G) \lor (F \land S \land E)) \land (\neg F \lor \neg S \lor G) \land \cdots$$

$$((F \land S \land G \land G) \lor (F \land S \land E \land G)) \land \cdots$$

$$((F \land S \land G) \lor \underbrace{(F \land S \land E \land G)}_{\text{Absorption } F \land S \land G}) \land \cdots$$

$$(F \land S \land G) \land (\neg G \lor \neg E)$$

$$\underbrace{(F \land S \land G \land \neg G)}_{=\bot} \lor (F \land S \land G \land \neg E)$$

$F \land S \land G \land \neg E$ DNF mit Lösung $I(F) = I(S) = I(G) = 1$ und $I(E) = 0$

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
4. Endliche Automaten

Dualität von Funktionen, Operatoren und Formeln

Beobachtung 1: „and“ und „or“ verhalten sich spiegelbildlich bzgl. 0 und 1.

x	y	x and y	x or y
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

x	y	x or y	x and y
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

„and“ ist eine Konjunktion für 1 und eine Disjunktion für 0.
„or“ ist eine Konjunktion für 0 und eine Disjunktion für 1.

Beobachtung 2: Boolesche Algebra ist symmetrisch bzgl. $\wedge/\vee$ und $\top/\bot$.

$$
\begin{array}{ll}
(A \wedge B) \wedge C = A \wedge (B \wedge C) & (A \vee B) \vee C = A \vee (B \vee C) \\
A \wedge B = B \wedge A & A \vee B = B \vee A \\
A \wedge A = A & A \vee A = A \\
A \wedge \top = A & A \vee \bot = A \\
A \wedge \neg A = \bot & A \vee \neg A = \top \\
A \wedge (A \vee B) = A & A \vee (A \wedge B) = A \\
A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C) & A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)
\end{array}
$$

Duale Funktionen

Zwei n-stellige Funktionen f und g heißen dual zueinander, wenn gilt:
$\text{not}\, f(x_1, \ldots, x_n) = g(\text{not}\, x_1, \ldots, \text{not}\, x_n)$.

Diese Bedingung ist gleichbedeutend mit jeder der folgenden:

$$\begin{aligned} \text{not}\, f(\text{not}\, x_1, \ldots, \text{not}\, x_n) &= g(x_1, \ldots, x_n) \\ f(x_1, \ldots, x_n) &= \text{not}\, g(\text{not}\, x_1, \ldots, \text{not}\, x_n) \\ f(\text{not}\, x_1, \ldots, \text{not}\, x_n) &= \text{not}\, g(x_1, \ldots, x_n) \end{aligned}$$

„and“ und „or“ sind dual, da $\text{not}(x \text{ and } y) = (\text{not}\, x) \text{ or } (\text{not}\, y)$ gilt.

Duale Operatoren

Zwei Operatoren heißen dual, wenn die zugehörigen Funktionen dual sind.

true / $\top$	not / $\neg$	and / $\wedge$	nand / $\uparrow$	iff / $\equiv$	implies / $\supset$	if / $\subset$

ist dual zu

false / $\perp$	not / $\neg$	or / $\vee$	nor / $\downarrow$	xor / $\not\equiv$	— / $\not\subset$	— / $\not\supset$

(und umgekehrt).

$G[A_1, \dots, A_n]$ … „Formel G enthält die Variablen A_1, …, A_n"
$G[H_1, \dots, H_n]$ … Formel, die aus $G[A_1, \dots, A_n]$ entsteht, wenn A_i überall durch H_i ersetzt wird.

Duale Formeln

Zwei Formeln $F[A_1, \dots, A_n]$ und $G[A_1, \dots, A_n]$ heißen dual zueinander, wenn gilt: $\neg F[A_1, \dots, A_n] = G[\neg A_1, \dots, \neg A_n]$

$\neg F[\neg A_1, \dots, \neg A_n]$ ist dual zu $F[A_1, \dots, A_n]$.

$\neg((\neg A \lor \neg\neg B) \supset \neg A)$ ist dual zu $(A \lor \neg B) \supset A$.

Sei G die Formel, die aus F durch Ersetzen aller Operatoren durch ihre dualen hervorgeht. Dann ist G dual zu F.

$\neg(((A \land B) \not\equiv \neg(B \uparrow C)) \not\supset ((A \land \top) \lor B))$ ist dual zu
$\neg(((A \lor B) \equiv \neg(B \downarrow C)) \subset ((A \lor \bot) \land B))$

F^*, G^* ... irgendwelche dualen Formeln zu F bzw. G

$F = G$ gilt genau dann, wenn $F^* = G^*$ gilt.

$F = G$	$F^* = G^*$
$(A \wedge B) \wedge C = A \wedge (B \wedge C)$	$(A \vee B) \vee C = A \vee (B \vee C)$
$A \wedge B = B \wedge A$	$A \vee B = B \vee A$
$A \wedge A = A$	$A \vee A = A$
$A \wedge \top = A$	$A \vee \bot = A$
$A \wedge \neg A = \bot$	$A \vee \neg A = \top$
$A \wedge (A \vee B) = A$	$A \vee (A \wedge B) = A$
$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

- $(F^*)^* = F$
- F ist gültig genau dann, wenn F^* unerfüllbar ist.
- $F \supset G$ ist gültig genau dann, wenn $G^* \supset F^*$ gültig ist.
- ...

Dualität ist nicht dasselbe wie Negation!