Theorie der Informatik

1. Aussagenlogik I

Malte Helmert Gabriele Röger

Universität Basel

19. Februar 2014

Theorie der Informatik

19. Februar 2014 — 1. Aussagenlogik I

1.1 Motivation

Warum Logik?

- Formalisierung der Mathematik
  - Was ist ein valider Beweis?
  - Was sind gültige Schlussfolgerungen aus einer Menge von Axiomen?
- Basis vieler Werkzeuge in der Informatik
  - Beschreibung von Schaltkreisen
  - Repräsentation des Wissens von Agenten (z.B. Robotern)
  - Formale Spezifikation von Programmen und Überprüfung des Verhalten eines Systems mit automatisierter Modellprüfung
  - ...

Beispiel: Gruppentheorie

Beispiel für Gruppe: $(\mathbb{Z}, +, 0)$
Menge der ganzen Zahlen mit Addition und neutralem Element 0

Gruppenaxiome für allgemeines $(G, \circ, e)$:

1. Für alle $x, y, z \in G$ gilt $(x \circ y) \circ z = x \circ (y \circ z)$.
2. Für alle $x \in G$ gilt $x \circ e = x$.
3. Für alle $x \in G$ gibt es ein $y \in G$ mit $x \circ y = e$.

Beispiel: Gruppentheorie

Theorem (Existenz des Linksinversen)

Sei $(G, \circ, e)$ eine Gruppe. Für alle $x \in G$ gibt es ein $y \in G$ mit $y \circ x = e$.

Beweis.

Betrachte ein beliebiges x. Wegen 3. gibt es ein y mit $x \circ y = e$ (*). Analog gibt es für dieses y ein z mit $y \circ z = e$ (**). Es gilt:

$$
\begin{aligned}
y \circ x &\overset{(2.)}{=} (y \circ x) \circ e \overset{(**)}{=} (y \circ x) \circ (y \circ z) \\
&\overset{(1.)}{=} y \circ (x \circ (y \circ z)) \overset{(1.)}{=} y \circ ((x \circ y) \circ z) \\
&\overset{(*)}{=} y \circ (e \circ z) \overset{(1.)}{=} (y \circ e) \circ z \\
&\overset{(2.)}{=} y \circ z \overset{(**)}{=} e
\end{aligned}
$$

$\square$

Allgemeine Fragestellung

Allgemeine Fragestellung

- Gegeben eine Menge (eine Wissensbasis) von Axiomen (z.B. Gruppenaxiome)
- Was können wir daraus folgern? (z.B. Theorem über Existenz des Linksinversen)
- Und auf welcher Basis dürfen wir argumentieren? (Warum folgt z.B. aus Gruppenaxiom 2., dass $y \circ x = (y \circ x) \circ e$?)

Ziel: „Mechanisches“ Beweisen

- formales „Spiel mit Buchstaben“
- losgelöst von einer konkreten Bedeutung

Aussagenlogik

Aussagenlogik ist einfache Logik ohne Zahlen oder Objekte

Bausteine der Aussagenlogik

- Aussage ist ein Satz, der entweder wahr oder falsch sein kann
- Atomare Aussage kann nicht weiter in Teilaussagen zerlegt werden
- Junktoren verbinden (Teil-)Aussagen zu neuen Aussagen

Beispiele für Bausteine

Wenn ich kein Bier zu einer Mahlzeit trinke, dann habe ich immer Fisch.
Immer wenn ich Fisch und Bier zur selben Mahlzeit habe, dann verzichte ich auf Eiscreme.
Wenn ich Eiscreme habe oder Bier meide, dann rühre ich Fisch nicht an.

- Jeder Satz ist eine Aussage, besteht aber wiederum aus Teilaussagen (z.B. „Eiscreme habe oder Bier meide“).
- Atomare Aussagen „Trinkt Bier“, „Isst Fisch“, “Isst Eiscreme“
- Junktoren „und“, „oder“, Verneinung, „wenn, dann“

Aufgabe aus U. Schöning: Logik für Informatiker
Foto mit freundlicher Genehmigung von graur razvan ionut / FreeDigitalPhotos.net

Beispiele für Bausteine

Wenn ich kein Bier zu einer Mahlzeit trinke, dann habe ich immer Fisch.
Immer wenn ich Fisch und Bier zur selben Mahlzeit habe, dann verzichte ich auf Eiscreme.
Wenn ich Eiscreme habe oder Bier meide, dann rühre ich Fisch nicht an.

- Jeder Satz ist eine Aussage, besteht aber wiederum aus Teilaussagen (z.B. „Eiscreme habe oder Bier meide“).
- Atomare Aussagen „Trinkt Bier“, „Isst Fisch“, “Isst Eiscreme“
- Junktoren „und“, „oder“, Verneinung, „wenn, dann“

Aufgabe aus U. Schöning: Logik für Informatiker
Foto mit freundlicher Genehmigung von graur razvan ionut / FreeDigitalPhotos.net

Probleme mit natürlicher Sprache

Wenn ich kein Bier zu einer Mahlzeit trinke, dann habe ich immer Fisch.
Immer wenn ich Fisch und Bier zur selben Mahlzeit habe, verzichte ich auf Eiscreme.
Wenn ich Eiscreme habe oder Bier meide, dann rühre ich Fisch nicht an.

- „Irrelevante“ Information

Aufgabe aus U. Schöning: Logik für Informatiker
Foto mit freundlicher Genehmigung von graur razvan ionut / FreeDigitalPhotos.net

Probleme mit natürlicher Sprache

Wenn ich kein Bier trinke, dann habe ich Fisch.
Wenn ich Fisch und Bier habe, verzichte ich auf Eiscreme.
Wenn ich Eiscreme habe oder Bier meide, dann rühre ich Fisch nicht an.

- „Irrelevante“ Information
- Verschiedene Formulierungen für gleichen Junktor/gleiche Aussage

Aufgabe aus U. Schöning: Logik für Informatiker
Foto mit freundlicher Genehmigung von graur razvan ionut / FreeDigitalPhotos.net

Probleme mit natürlicher Sprache

Wenn nicht TrinktBier, dann IsstFisch.
Wenn IsstFisch und TrinktBier, dann nicht IsstEiscreme.
Wenn IsstEiscreme oder nicht TrinktBier, dann nicht IsstFisch.

- „Irrelevante“ Information
- Verschiedene Formulierungen für gleichen Junktor/gleiche Aussage

Aufgabe aus U. Schöning: Logik für Informatiker
Foto mit freundlicher Genehmigung von graur razvan ionut / FreeDigitalPhotos.net

Wie geht es weiter?

- Was sind sinnvolle (wohldefinierte) Aneinanderreihung von atomaren Formeln und Junktoren?
  „wenn dann IsstEiscreme nicht oder TrinktBier und“ nicht sinnvoll
  $\rightarrow$ Syntax
- Was bedeutet es über eine Aussage zu sagen, dass sie wahr ist?
  Ist „TrinktBier und IsstFisch“ wahr?
  $\rightarrow$ Semantik
- Wann folgt eine Aussage aus einer anderen Aussage?
  Folgt „IsstFisch“ aus „Wenn TrinktBier, dann IsstFisch“?
  $\rightarrow$ Logische Folgerung

1.2 Syntax

Syntax der Aussagenlogik

Definition (Syntax der Aussagenlogik)

Sei A eine Menge von atomaren Aussagen. Die Menge der aussagenlogischen Formeln (über A) ist induktiv wie folgt definiert:

- Jedes Atom $a \in A$ ist eine aussagenlogische Formel über A.
- Ist ϕ eine aussagenlogische Formel über A, dann auch die Negation $\neg\phi$.
- Sind ϕ und ψ aussagenlogische Formeln über A, dann ist es auch die Konjunktion $(\phi \wedge \psi)$.
- Sind ϕ und ψ aussagenlogische Formeln über A, dann ist es auch die Disjunktion $(\phi \vee \psi)$.

Die Implikation $(\phi \rightarrow \psi)$ ist eine Abkürzung für $(\neg\phi \vee \psi)$.
Das Bikonditional $(\phi \leftrightarrow \psi)$ ist Abk. für $((\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi))$.

Syntax: Beispiele

Welche der folgenden Zeichenfolgen sind aussagenlogische Formeln über der Menge aller möglichen Buchstabenfolgen?

- $(A \land (B \lor C))$
- ((IsstFisch $\land$ TrinktBier) $\rightarrow$ $\neg$IsstEiscreme)
- $\neg$($\land$ Regen $\lor$ Strassenass)
- $\neg$(Regen $\lor$ Strassenass)
- $\neg(A = B)$
- $(A \land \neg(B \leftrightarrow)C)$
- $(A \lor \neg(B \leftrightarrow C))$
- $((A \leq B) \land C)$
- $((A_1 \land A_2) \lor \neg(A_3 \leftrightarrow A_2))$

Welcher Art sind die Formeln (Atom, Konjunktion, ...)?

1.3 Semantik

Bedeutung aussagenlogischer Formeln?

Aussagenlogische Formeln bisher blosse Zeichenfolgen ohne Bedeutung.

Was heisst z.B. ((IsstFisch $\land$ TrinktBier) $\rightarrow$ $\neg$IsstEiscreme)?

▷ Wir brauchen Semantik!

Semantik der Aussagenlogik

Definition (Semantik der Aussagenlogik)

Eine Wahrheitsbelegung (oder Interpretation) für eine Menge von atomaren Aussagen A ist eine Funktion $\mathcal{I} : A \rightarrow \{0, 1\}$. Eine aussagenlogische Formel ϕ (über A) gilt unter Belegung $\mathcal{I}$ (geschrieben $\mathcal{I} \models \phi$) nach folgender Definition:

- $\mathcal{I} \models a$ (für $a \in A$) gdw. $\mathcal{I}(a) = 1$
- $\mathcal{I} \models \neg\phi$ gdw. nicht $\mathcal{I} \models \phi$
- $\mathcal{I} \models (\phi \land \psi)$ gdw. $\mathcal{I} \models \phi$ und $\mathcal{I} \models \psi$
- $\mathcal{I} \models (\phi \lor \psi)$ gdw. $\mathcal{I} \models \phi$ oder $\mathcal{I} \models \psi$

Für $\mathcal{I} \models \phi$ sagen wir auch $\mathcal{I}$ ist ein Modell für ϕ.

Gilt $\mathcal{I} \models \phi$ nicht, schreiben wir das als $\mathcal{I} \not\models \phi$.

$\models$ ist nicht Teil der Formel, sondern ein Symbol der Metasprache.

Semantik: Beispiel

$A = \{\text{TrinktBier}, \text{IsstFisch}, \text{IsstEiscreme}\}$

$\mathcal{I} = \{\text{TrinktBier} \mapsto 1, \text{IsstFisch} \mapsto 0, \text{IsstEiscreme} \mapsto 1\}$

$\phi = (\neg\text{TrinktBier} \to \text{IsstFisch})$

Gilt $\mathcal{I} \models \phi$?

Semantik: Beispiel

$$\begin{aligned}
\mathcal{I} \models \phi \text{ gdw. } & \mathcal{I} \models (\neg\text{TrinktBier} \to \text{IsstFisch})\\
\text{gdw. } & \mathcal{I} \models (\neg\neg\text{TrinktBier} \lor \text{IsstFisch})\\
\text{gdw. } & \mathcal{I} \models \neg\neg\text{TrinktBier oder } \mathcal{I} \models \text{IsstFisch}\\
\text{gdw. } & \mathcal{I} \models \neg\neg\text{TrinktBier oder } \mathcal{I}(\text{IsstFisch}) = 1\\
\text{gdw. } & \mathcal{I} \models \neg\neg\text{TrinktBier}\\
\text{gdw. } & \text{nicht } \mathcal{I} \models \neg\text{TrinktBier}\\
\text{gdw. } & \text{nicht nicht } \mathcal{I} \models \text{TrinktBier}\\
\text{gdw. } & \mathcal{I} \models \text{TrinktBier}\\
\text{gdw. } & \mathcal{I}(\text{TrinktBier}) = 1
\end{aligned}$$

1.4 Formeleigenschaften

Eigenschaften von Formeln

Eine aussagenlogische Formel ϕ ist

- erfüllbar, falls ϕ mindestens ein Modell besitzt.
- unerfüllbar, falls ϕ nicht erfüllbar ist.
- gültig (oder Tautologie), falls ϕ unter jeder Wahrheitsbelegung gilt.
- falsifizierbar, falls ϕ keine Tautologie ist.

Wie zeigen wir, dass eine Formel eine dieser Eigenschaften hat?

Beispiele

- Zeigen Sie, dass $(A \wedge B)$ erfüllbar ist.
  $\mathcal{I} = \{A \mapsto 1, B \mapsto 1\}$
- Zeigen Sie, dass $(A \wedge B)$ falsifizierbar ist.
  $\mathcal{I} = \{A \mapsto 0, B \mapsto 1\}$
- Zeigen Sie, dass $(A \wedge B)$ nicht gültig ist.
  Folgt direkt aus Falsifizierbarkeit
- Zeigen Sie, dass $(A \wedge B)$ nicht unerfüllbar ist.
  Folgt direkt aus Erfüllbarkeit

Bisher alles durch Angabe einer Belegung gezeigt.

Was ist mit gültig, unerfüllbar, nicht erfüllbar, nicht falsifizierbar?

▷ Benötigen Aussagen über alle möglichen Belegungen

Wahrheitstafeln

Werte für alle möglichen Belegungen aus, ob sie ein Modell für die betrachtete Formel sind.

$\mathcal{I}(A)$	$\mathcal{I} \models \neg A$
0	Ja
1	Nein

$\mathcal{I}(A)$	$\mathcal{I}(B)$	$\mathcal{I} \models (A \wedge B)$
0	0	Nein
0	1	Nein
1	0	Nein
1	1	Ja

$\mathcal{I}(A)$	$\mathcal{I}(B)$	$\mathcal{I} \models (A \vee B)$
0	0	Nein
0	1	Ja
1	0	Ja
1	1	Ja

Wahrheitstafeln allgemein

Betrachte alle Möglichkeiten, wie Belegungen die kleinsten Teilformeln (nicht) erfüllen können, und werte jeweils aus, ob sie ein Modell für die betrachtete Gesamtformel sind.

$\mathcal{I} \models \phi$	$\mathcal{I} \models \psi$	$\mathcal{I} \models (\phi \wedge \psi)$
Nein	Nein	Nein
Nein	Ja	Nein
Ja	Nein	Nein
Ja	Ja	Ja

Übung: Wahrheitstafel für $(\phi \rightarrow \psi)$

Wahrheitstafeln für Formeleigenschaften

Ist $\phi = ((A \rightarrow B) \vee (\neg B \rightarrow A))$ gültig, unerfüllbar,...?

$\mathcal{I}(A)$	$\mathcal{I}(B)$	$\mathcal{I} \models \neg B$	$\mathcal{I} \models (A \rightarrow B)$	$\mathcal{I} \models (\neg B \rightarrow A)$	$\mathcal{I} \models \phi$
0	0	Ja	Ja	Nein	Ja
0	1	Nein	Ja	Ja	Ja
1	0	Ja	Nein	Ja	Ja
1	1	Nein	Ja	Ja	Ja

Zusammenhang Formeleigenschaften und Wahrheitstafeln

Eine aussagenlogische Formel ϕ ist

- erfüllbar, falls ϕ mindestens ein Modell besitzt.
  ▷ Ergebnis in mindestens einer Zeile „Ja“
- unerfüllbar, falls ϕ nicht erfüllbar ist.
  ▷ Ergebnis in allen Zeilen „Nein“
- gültig (oder Tautologie), falls ϕ unter jeder Wahrheitsbelegung gilt.
  ▷ Ergebnis in allen Zeilen „Ja“
- falsifizierbar, falls ϕ keine Tautologie ist.
  ▷ Ergebnis in mindestens einer Zeile „Nein“

Grosser Nachteil von Wahrheitstafeln

Wie gross wird eine Wahrheitstafel mit n atomaren Aussagen?

1	2 Belegungen (Zeilen)
2	4 Belegungen (Zeilen)
3	8 Belegungen (Zeilen)
n	??? Belegungen

Einige Beispiele: $2^{10} = 1024$, $2^{20} = 1048576$, $2^{30} = 1073741824$

▷ Für grosse Formeln nicht praktikabel, brauchen andere Lösung
$\rightsquigarrow$ nächste Vorlesungsstunde

1.5 Zusammenfassung

Zusammenfassung

- Aussagenlogik basiert auf atomaren Aussagen
- Syntax legt fest, was wohlgeformte Formeln sind
- Semantik definiert, wann eine Formel wahr ist
- Wahrheitsbelegungen sind wichtigste Grundlage der Semantik.
- Erfüllbarkeit und Gültigkeit sind wichtige Formeleigenschaften.
- Wahrheitstafeln betrachten systematisch alle möglichen Wahrheitsbelegungen.
- Wahrheitstafeln nur für kleine Formeln nützlich