Logik / Theoretische Grundlagen der Informatik 3

Stephan Kreutzer

Wintersemester 2014/2015

1. Aussagenlogik

1.1. Einleitung

Einleitung

Beispiel. Betrachten wir folgende Aussage.

- Wenn der Zug zu spät ist und keine Taxis am Bahnhof stehen, kommt Peter zu spät zu seiner Verabredung.
- Peter kam nicht zu spät zu seiner Verabredung.
- Der Zug hatte Verspätung.

Also standen Taxis am Bahnhof.

Ist das Argument gültig?

Einleitung

Beispiel. Sie kann nicht zu hause sein, da sie entweder an Bord oder zu hause ist und ich gerade gehört habe, dass sie an Bord ist.

Ist das Argument gültig?

Was können wir formal beweisen?

- Klar formulierte Aussagen, die entweder richtig oder falsch sind.

  Die Bedeutung aller verwendeten Ausdrücke muss bekannt sein.

  Ebenso das vorausgesetzte Hintergrundwissen.

- Natürliche Sprache ist dafür nicht gut geeignet.

- Wir werden daher formale Sprachen, oder Logiken, verwenden, in denen alle Ausdrücke formal und vollständig definiert sind.

- Ziel ist es, allgemeine Regeln für korrektes Schließen herleiten zu können, möglichst sogar automatisch.

Einleitung

In diesem Teil der Vorlesung werden wir Methoden kennen lernen um

- Aussagen wie auf den vorigen Folien formal auszudrücken
- formalisierte Aussagen zu manipulieren
- logische Behauptungen zu beweisen

Inhaltsübersicht.

1. Was sind Formeln und was bedeuten sie: Syntax und Semantik
2. Wie können wir mit Formeln umgehen: Äquivalenzen und Normalformen
3. Neues Wissen aus altem folgern: Die Semantische Folgerung
4. Andere für uns arbeiten lassen: algorithmische Verfahren für logische Folgerung

1.2. Syntax und Semantik der Aussagenlogik

Syntax der Aussagenlogik

Definition. (Aussagenvariablen)

Eine Aussagenvariable, oder auch einfach Variable, hat die Form V_i für $i \in \mathbb{N}$.

Die Menge aller Variablen bezeichnen wir als AVAR.

Definition. (Alphabet)

Das Alphabet der Aussagenlogik ist

$$\Sigma_{AL} := \mathrm{AVAR} \cup \{\top, \bot, \neg, \vee, \wedge, \rightarrow, \leftrightarrow, (,)\}$$

Aussagenlogik

Definition. (Syntax der Aussagenlogik)

Die Klasse AL der aussagenlogischen Formeln ist induktiv definiert durch

Basis:

- $\top, \bot$ sind aussagenlogische Formeln
- Jede Variable $V_i \in \mathrm{AVAR}$ ist eine aussagenlogische Formel

$\top, \bot$ und die Variablen werden atomare Formeln oder Atome genannt

Induktionsschritt:

- Wenn $\varphi \in \mathrm{AL}$ eine Formel ist, dann auch $\neg\varphi \in \mathrm{AL}$
- Wenn $\varphi, \psi \in \mathrm{AL}$ Formeln sind, dann auch

$$(\varphi \vee \psi), \quad (\varphi \wedge \psi), \quad (\varphi \rightarrow \psi), \quad (\varphi \leftrightarrow \psi)$$

$\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ werden aussagenlogische Verknüpfungen genannt.

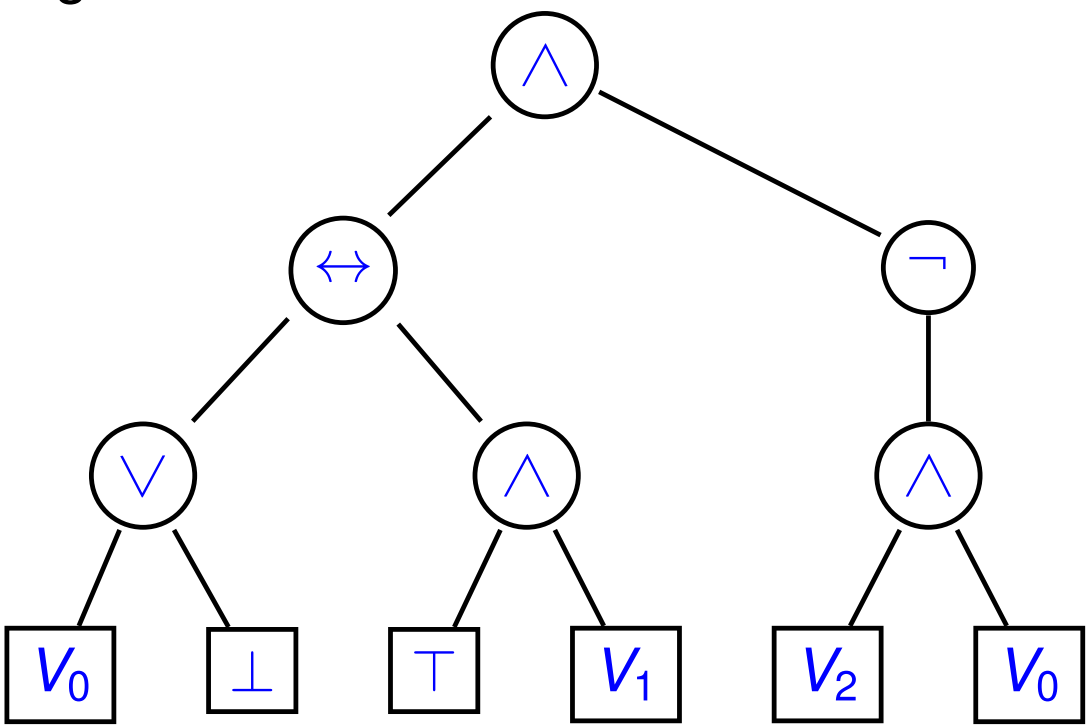
Syntax- oder Ableitungsbäume

Die Struktur einer Formel kann elegant durch ihren Syntax- oder Ableitungsbaum dargestellt werden.

Der Syntaxbaum der Formel

$$\varphi := (((V_0 \vee \bot) \leftrightarrow (\top \wedge V_1)) \wedge \neg(V_2 \wedge V_0))$$

ist definiert wie folgt:



Unterformeln

Definition. Die Menge $\text{sub}(\varphi)$ der Unterformeln einer Formel φ ist induktiv wie folgt definiert:

- Ist φ atomar, dann ist $\text{sub}(\varphi) := \{\varphi\}$.
- Ist $\varphi := \neg\psi$, dann ist $\text{sub}(\varphi) := \{\varphi\} \cup \text{sub}(\psi)$.
- Für alle $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$: Ist $\varphi := (\varphi_1 * \varphi_2)$, dann ist

$$\text{sub}(\varphi) := \{\varphi\} \cup \text{sub}(\varphi_1) \cup \text{sub}(\varphi_2).$$

Wir fassen sub als Funktion $\text{sub} : \text{AL} \rightarrow \mathcal{P}(\text{AL})$ auf, die jeder Formel φ die Menge $\text{sub}(\varphi)$ ihrer Unterformeln zuweist.

Induktive Definitionen

Induktive Definitionen. Eine Funktion $f : \mathrm{AL} \to M$, für eine beliebige Menge M, kann induktiv wie folgt definiert werden:

Basisfälle. Wir definieren zunächst die Funktionswerte für atomare Formeln.

- Definiere $f(\top)$ und $f(\bot)$.
- Definiere $f(X)$ für alle $X \in \mathrm{AVAR}$.

Induktionsschritt. Danach werden die Funktionswerte für zusammengesetzte Formeln definiert.

- Definiere $f(\neg\varphi)$ aus $f(\varphi)$.
- Für $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ definiere $f((\varphi * \psi))$ aus $f(\varphi)$ und $f(\psi)$.

Semantik der Aussagenlogik

Wahrheitsbelegungen

Definition. Die Menge $\mathrm{var}(\varphi)$ der Variablen einer Formel φ ist die Menge

$$\mathrm{var}(\varphi) := \mathrm{AVAR} \cap \mathrm{sub}(\varphi)$$

Definition.

1. Eine Wahrheitsbelegung, oder kurz Belegung, ist eine partielle Funktion
$$\beta : \mathrm{AVAR} \to \{0, 1\}.$$

2. Eine Belegung β ist eine Belegung für eine Formel φ, oder ist passend für φ, wenn $\mathrm{var}(\varphi) \subseteq \mathrm{Dom}(\beta)$.

Intuitiv: 1 steht für *wahr* und 0 für *falsch*.

Semantik der Aussagenlogik

Definition. Per Induktion über die Struktur der Formeln in AL definieren wir eine Funktion $[\![\cdot]\!]^{\cdot}$, die jeder Formel $\varphi \in \mathrm{AL}$ und jeder zu φ passenden Belegung β einen Wahrheitswert $[\![\varphi]\!]^{\beta} \in \{0, 1\}$ zuordnet.

Basisfall.

- $[\![\bot]\!]^{\beta} := 0 \qquad [\![\top]\!]^{\beta} := 1$
- Für alle $X \in \mathrm{AVar}$ gilt $[\![X]\!]^{\beta} := \beta(X)$

Induktionsschritt. Für zusammen gesetzte Formeln φ definieren wir $[\![\varphi]\!]^{\beta}$ durch die folgenden Wahrheitstafeln:

$[\![\varphi]\!]^{\beta}$	$[\![\neg\varphi]\!]^{\beta}$
0	1
1	0

Semantik der Aussagenlogik

Konjunktion

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \wedge \psi)]\!]^\beta$
0	0	0
0	1	0
1	0	0
1	1	1

Disjunktion

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \vee \psi)]\!]^\beta$
0	0	0
0	1	1
1	0	1
1	1	1

Implikation

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \rightarrow \psi)]\!]^\beta$
0	0	1
0	1	1
1	0	0
1	1	1

Biimplikation

$[\![\varphi]\!]^\beta$	$[\![\psi]\!]^\beta$	$[\![(\varphi \leftrightarrow \psi)]\!]^\beta$
0	0	1
0	1	0
1	0	0
1	1	1

Notation

Notation. Wir vereinbaren folgende Notation.

- Belegungen: $\beta, \gamma, \ldots$
- Formeln: $\varphi, \psi, \varphi' \ldots$
- Mengen von Formeln: $\Phi, \Psi, \ldots$
- Wir werden auch X, Y, ... für Variablen verwenden

Präferenzregeln. Um unnötige Klammern zu vermeiden,

- lassen wir die äußersten Klammern weg
- vereinbaren, dass $\neg$ stärker bindet als die anderen Verknüpfungen
- $\wedge, \vee$ bindet stärker als $\rightarrow, \leftrightarrow$

Beispiel

Beispiel. Erinnern wir uns an das Beispiel vom Anfang der Vorlesung:

- Wenn der Zug zu spät ist und keine Taxis am Bahnhof stehen, kommt Peter zu spät zu seiner Verabredung.
- Peter kam nicht zu spät zu seiner Verabredung.
- Der Zug hatte Verspätung.

Also standen Taxis am Bahnhof.

1.3. Erfüllbarkeit und Allgemeingültigkeit

Erfüllbarkeit und Gültigkeit

Definition. Sei $\varphi \in \mathsf{AL}$ eine Formel.

1. Eine zu φ passende Belegung β erfüllt φ, oder ist ein Modell von φ, wenn $[\![\varphi]\!]^{\beta} = 1$.

   Wir schreiben $\beta \models \varphi$.

2. φ ist erfüllbar, wenn es eine Belegung β gibt, die φ erfüllt. Anderenfalls ist φ unerfüllbar.

3. φ ist allgemeingültig, oder eine Tautologie, wenn jede zu φ passende Belegung φ erfüllt.

Wahrheitstafeln

Beispiel. $\big((X_H \to X_M) \land (X_S \to X_H)\big) \to (X_S \to X_M)$

X_H	X_M	X_S	$\big((X_H \to X_M) \land (X_S \to X_H)\big) \to (X_S \to X_M)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Erweiterte Wahrheitstafeln

Beispiel (forts.) $\varphi := \big((X_H \to X_M) \wedge (X_S \to X_H)\big) \to (X_S \to X_M)$

X_H	X_M	X_S	$(X_H \to X_M)$	$(X_S \to X_H)$	$(X_H \to X_M) \wedge (X_S \to X_H)$	$(X_S \to X_M)$	φ
0	0	0	1	1	1	1	1
0	0	1	1	0	0	0	1
0	1	0	1	1	1	1	1
0	1	1	1	0	0	1	1
1	0	0	0	1	0	1	1
1	0	1	0	1	0	0	1
1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1

Wir nennen das die erweiterte Wahrheitstafel.

Das Koinzidenz Lemma

Lemma. (Koinzidenzlemma)

Sei $\varphi \in \mathsf{AL}$ eine Formel und seien β, β' Belegungen so dass

$$\beta(X) = \beta'(X) \qquad \text{für alle } X \in \mathrm{var}(\varphi).$$

Dann gilt $[\![\varphi]\!]^{\beta} = [\![\varphi]\!]^{\beta'}$.

Das Wahrheitstafelverfahren

Beobachtung Sei $\varphi \in$ AL eine Formel.

1. φ ist genau dann erfüllbar, wenn die letzte Spalte der Wahrheitstafel mindestens eine 1 enthält.
2. φ ist genau dann unerfüllbar, wenn alle Einträge der letzten Spalte 0 sind.
3. φ ist genau dann allgemeingültig, wenn alle Einträge der letzten Spalte 1 sind.

Das Wahrheitstafelverfahren.

Eingabe: Eine Formel $\varphi \in$ AL .

Ziel: entscheide, ob φ erfüllbar ist.

Methode:
1. Berechne die Wahrheitstafel für φ.
2. Überprüfe, ob die letzte Spalte eine 1 enthält.

Bemerkung. Für Allgemeingültigkeit entscheide, ob die letzte Spalte nur 1 enthält.

Effizienz des Wahrheitstafelverfahrens

Die Wahrheitstafel einer Formel mit n Variablen hat 2^n Zeilen.

Das macht das Wahrheitstafelverfahren extrem ineffizient außer für sehr kleine Formeln.

Variablen	Zeilen
10	$1{,}024 \approx 10^3$
20	$1{,}048{,}576 \approx 10^6$
30	$1{,}073{,}741{,}824 \approx 10^9$
40	$1{,}099{,}511{,}627{,}776 \approx 10^{12}$
50	$1{,}125{,}899{,}906{,}842{,}624 \approx 10^{15}$
60	$1{,}152{,}921{,}504{,}606{,}846{,}976 \approx 10^{18}$

Das Aussagenlogische Erfüllbarkeitsproblem

Bemerkung.

- Das Erfüllbarkeitsproblem der Aussagenlogik ist eines der am besten studierten Probleme der Informatik.
- Es ist “schwer” zu lösen (NP-vollständig, werden wir später beweisen)
- Allerdings existieren Verfahren, die das Problem für viele in der Praxis vorkommende Formeln sehr effizient lösen können. (Das Wahrheitstafelverfahren gehört nicht dazu)
- Diese haben wichtige Anwendungen in der Informatik, z.B. in der Verifikation.