Vorlesung
Automatisches Beweisen

Elmar Eder

18. Dezember 2018

3.10.2018

S. Tafelfoto

Formalisierung und Axiomatisierung der Logik
Aristoteles
Boole: Aussagenlogik

Gottlob Frege: Begriffsschrift 1879 Prädikatenlogik in Baumnotation, z.B. $\vdash A$ $\begin{array}{l}\vdash B\\ \vdash A\end{array}$
Heute in einer Zeile, etwa mit $\neg$, $\rightarrow$, $\forall$

A	$\neg A$
w	f
f	w

A	B	$A \rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

.....

allgemeingültig, erfüllbar, unerfüllbar in der Aussagenlogik entscheidbar, aber mit hoher Zeitkomplexität.
Erfüllbarkeit in der Aussagenlogik NP-volständig.
L NP-vollständig : $\Leftrightarrow$ $L \in$ NP und L ist NP-hart.
$L' \leq_p L$: $\Leftrightarrow$ ex. p-Zeit-berechenbare Funktion f, sodass für alle $w \in \Sigma^*$ gilt ($w \in L' \Leftrightarrow f(w) \in L$).

.....

Russel'sche Antinomie $P(X)$: $\Leftrightarrow \neg X(X)$ für alle Prädikate X.
$P(P) \Leftrightarrow \neg P(P)$. Widerspruch

1 Klassische Aussagenlogik

10.10.2018

S. Tafelfotos

Grundzeichen

1. abzählbar unendlich viele Aussagensymbole $U, V, W, \ldots$
2. Junktoren *nicht*, $\wedge$, $\vee$
   (auch andere Junktorensysteme mit Junktoren $\bot$, $\to$, $\ldots$)
3. Interpunktionszeichen Klammern (,)

Menge der Aussagensymbole $\mathbb{A}$

Formeln Induktive Definition des Begriffs der Formel

1. Jedes Aussagensymbol ist eine Formel.
2. Wenn F eine Formel ist, dann auch $\neg F$.
3. Wenn F und G Formeln sind, dann auch $(F \wedge G)$ und $(F \vee G)$.

1.1 Semantik

Menge der *Wahrheitswerte* $\mathbb{B} = \{\mathsf{w}, \mathsf{f}\}$ wahr, falsch

Jeder Junktor steht für eine aussagenlogische Verknüpfung, die mit demselben Zeichen bezeichnet wird:
$\neg\colon \mathbb{B} \to \mathbb{B}$, $\neg\mathsf{w} = \mathsf{f}$, $\neg\mathsf{f} = \mathsf{w}$.
$\wedge, \vee\colon \mathbb{B}^2 \to \mathbb{B}$, $\mathsf{w} \vee \mathsf{w} = \mathsf{w}$, $\mathsf{w} \vee \mathsf{f} = \mathsf{w}$, $\mathsf{f} \vee \mathsf{w} = \mathsf{w}$, $\mathsf{f} \vee \mathsf{f} = \mathsf{f}$.

Wahrheitswerttabellen

x	$\neg x$

.....

Eine *Interpretation*

Der *Wahrheitswert* F^I einer Formel F bei einer Interpretation I ist definiert durch

Formeln F, G, H

Wahrheitswerttabellen für Formeln
Beispiel

Modell einer Formel

allgemeingültig erfüllbar unerfüllbar

$\models \sim$

Definition 1 (Grundterm, Herbrand-Universum) Ein *Grundterm* ist ein Term, der keine Variablen enthält. Das *Herbrand-Universum* einer Sprache der Prädikatenlogik erster Stufe ist die Menge der Grundterme.

Definition 2 Eine prädikatenlogische Formel $P(t_1, \ldots, t_n)$, wobei P ein n-stelliges Prädikatszeichen ist und $t_1, \ldots, t_n$ Terme sind, heißt *Atomformel*.

Definition 3 (Literal) Ein *Literal* ist eine Atomformel A (*postives Literal)* oder die Negation $\neg A$ einer Atomformel A (*negatives Literal*).

Definition 4 (Komplementäres Literal) Das zu einem Literal L *komplementäre Literal* $\overline{L}$ ist definiert als das Literal

- $\neg A$, wenn L eine Atomformel A ist
- A, wenn L die Negation $\neg A$ einer Atomformel A ist.

Für eine Menge c von Literalen sei $\overline{c} := \{\overline{L} \mid L \in c\}$.

Definition 5 (Substitution) Eine *Substitution* ist eine Funktion σ von der Menge der Variablen in die Menge der Terme derart, dass nur für endlich viele Variablen x gilt $x \neq \sigma(x)$.

Definition 6 (Anwendung einer Substitution auf einen Term) Für einen Term t und eine Substitution σ ist der Term $t\sigma$, der sich durch Anwendung von σ auf t ergibt, definiert durch Induktion nach dem Aufbau von t wie folgt:

- Wenn t eine Variable ist, dann ist $t\sigma := \sigma(t)$.
- Wenn t eine Konstante ist, dann ist $t\sigma := t$.
- Wenn $t = f(t_1, \ldots, t_n)$ ist, dann ist $t\sigma := f(t_1\sigma, \ldots, t_n\sigma)$.

Man nennt $t\sigma$ eine *Instanz* von t. Eine Instanz, die keine Variablen enthält, heißt *Grundinstanz*.

Für ein Literal L und eine Substitution σ ist $L\sigma$ definiert wie $t\sigma$ für einen Term t. Dabei werden Prädikatszeichen wie Funktionszeichen behandelt. Auch Unifikation von Atomformeln oder von Literalen ist definiert wie Unifikation von Termen, und der Unifikationsalgorithmus ist auch gleich wie für Terme.

Ähnlich ist für jede Formel F, die keine Quantoren enthält, und für jede Substitution σ die *Instanz* $F\sigma$ definiert.

Definition 7 (Unifikator) Ein *Unifikator* einer Menge M von Termen oder von Literalen ist eine Substitution σ, sodass $s\sigma = t\sigma$ für alle $s, t \in M$ gilt.

Allgemeinster Unfikator und Unifikationsalgorithmus s. `lp3.pdf`.

Wenn zwei Terme oder Literale unifizierbar sind, dann haben sie auch einen allgemeinsten Unifikator (mgu), und der Unifikationsalgorithmus liefert einen mgu.

Definition 8 (Klausel) Eine *Klausel* ist eine endliche Menge von Literalen.

Definition 9 (Instanz) Für eine Klausel $c = \{L_1, \ldots, L_n\}$ ist $c\sigma$ die Klausel $\{L_1\sigma, \ldots, L_n\sigma\}$. Sie heißt eine *Instanz* der Klausel c. Eine Instanz, die keine Variablen enthält, heißt *Grundinstanz*.

Definition 10 (Allabschluss) Sei F eine Formel mit den freien Variablen $x_1, \ldots, x_k$. Dann heißt $\forall x_1 \ldots \forall x_k F$ *Allabschluss* oder $\forall$-*Abschluss* der Formel F. Wir bezeichnen ihn mit $\forall[F]$.

Definition 11 (Existenzabschluss) Sei F eine Formel mit den freien Variablen $x_1, \ldots, x_k$. Dann heißt $\exists x_1 \ldots \exists x_k F$ *Existenzabschluss* oder $\exists$-*Abschluss* der Formel F. Wir bezeichnen ihn mit $\exists[F]$.

Eine Klausel $\{L_1, \ldots, L_n\}$ steht im Resolutionskalkül für eine prädikatenlogische Formel $\forall[L_1 \vee \ldots \vee L_n]$. Die leere Klausel $\emptyset$ wird mit $\square$ bezeichnet. Sie steht für einen Widerspruch $\bot$ oder $A \wedge \neg A$.

Wir sagen, eine Klausel d *folge semantisch* aus einer Klausel c, wenn dies für die entsprechenden Formeln gilt.

Wir sagen, eine Klausel d sei *semantisch äquivalent* zu c, wenn dies für die entsprechenden Formeln gilt.

Eine Instanz einer Klausel c folgt stets aus c, also $c \models c\sigma$.

Definition 12 (Variablenumbenennung) Eine *Variablenumbenennung* ist eine Substitution, die eine bijektive Funktion von der Menge der Variablen in die Menge der Variablen ist. Wir nennen sie auch eine *Permutation*.

Definition 13 (Variante einer Klausel) Sei c eine Klausel und π eine Variablenumbenennung. Dann heißt $c\pi$ eine *Variante* von c.

Eine Variante einer Klausel c ist stets semantisch äquivalent zu c, also $c \sim c\pi$, wenn π eine Variablenumbenennung ist.

Definition 14 Die Resolutionsregel

1. Seien c und d zwei Klauseln und sei d' eine Variante von d, die keine Variablen mit c gemeinsam hat.
2. Sei c_0 eine nichtleere Teilmenge von c und d'_0 eine nichtleere Teilmenge von d'. Seien alle Literale aus c_0 positiv und alle Literale aus d'_0 negativ oder umgekehrt (d.h. alle Literale aus c_0 negativ und alle Literale aus d'_0 positiv).

3. Sei $c_0 \cup \overline{d'_0}$ unifizierbar mit mgu σ.
4. Sei $e = (c\sigma \setminus c_0\sigma) \cup (d'\sigma \setminus d'_0\sigma)$.

Dann heißt e eine *Resolvente* von c und d. Die Klauseln c und d heißen *Eltenklauseln*. Wir sagen, dass e durch Resolution aus den Klauseln c und d erschlossen worden ist. Die Literale aus $c_0 \cup d_0$ heißen die *wegresolvierten Literale*.

Die Resolvente e eines Resolutionsschlusses folgt semantisch aus den Elternklauseln c und d, also $\{c, d\} \models e$.

Im Resolutionskalkül versucht man die Unerfüllbarkeit einer Klauselmenge nachzuweisen, indem man durch wiederholte Resolution aus den Klauseln dieser Klauselmenge die leere Klausel $\square$ ableitet.

Definition 15 (Resolutionsableitung, Resolutionswiderlegung) Sei S eine Menge von Klauseln.

- Eine *Resolutionsableitung* aus S ist eine endliche oder unendliche Folge $(c_0, c_1, c_2, \dots)$ von Klauseln derart, dass jedes c_k dieser Folge ein Element der Menge S ist oder durch einen Resolutionsschluss aus Klauseln c_i und c_j mit $i < k$ und $j < k$ erschlossen ist, also Resolvente von c_i und c_j ist.
- Eine *Resolutionsableitung* einer Klausel c aus S ist eine endliche Resolutionsableitung $(c_0, \dots, c_n)$ aus S, die mit der Klausel c endet, also mit $c_n = c$.
- Eine *Resolutionswiderlegung* von S ist eine Resolutionsableitung der leeren Klausel $\square$ aus S.

Man kann zu einer Resolutionsableitung einer Klausel c aus einer Klauselmenge S einen *Ableitungsbaum* angeben, in dem jeder Knoten mit einer Klausel der Ableitung markiert ist. Die Wurzel des Baumes wird mit der Klausel c markiert. Für jeden Resolutionsschritt zeichnet man über der Resolvente die beiden Elternklauseln und verbindet sie mit der Resolvente durch jeweils eine Kante.

Definition 16 Eine Formel ist in *Negationsnormalform (NNF)*, wenn sie Negationszeichen nur unmittelbar vor Atomformeln enthält. Äquivalente induktive Definition:

- Jedes Literal ist in NNF.
- Wenn F und G in NNF sind, dann auch $F \wedge G$ und $F \vee G$.
- Wenn F in NNF ist, dann auch $\forall x F$ und $\exists x F$.

Zu jeder Formel kann man eine semantisch äquivalente Formel in NNF konstruieren. (Negationszeichen nach innen ziehen)

Definition 17 Eine Formel ist in *pränexer Normalform*, wenn sie die Form $Q_1 x_1 \dots Q_k x_k F$ hat, wobei $Q_1, \dots, Q_k$ Quantoren $\forall$ oder $\exists$ sind, $x_1, \dots, x_k$ Variablen sind und F eine Formel ohne Quantoren ist.

Zu jeder Formel kann man eine semantisch äquivalente Formel in pränexer Normalform konstruieren. (Quantoren nach außen ziehen)

Die zu einer Formel F *duale* Formel F_{dual} ist die Formel, die sich aus F ergibt, indem man darin alle $\wedge$ durch $\vee$, alle $\vee$ durch $\wedge$, alle $\forall$ durch $\exists$ und alle $\exists$ durch $\forall$ ersetzt.

Eine Formel F ist genau dann allgemeingültig, wenn F_{dual} unerfüllbar ist.
Eine Formel F ist genau dann unerfüllbar, wenn F_{dual} allgemeingültig ist.

Definition 18 Zwei Formeln F und G heißen *erfüllbarkeitsäquivalent*, wenn F genau dann erfüllbar ist, wenn G erfüllbar ist.

Analog wollen wir F und G *allgemeingültigkeitsäquivalent* nennen, wenn F genau dann allgemeingültig ist, wenn G allgemeingültig ist.

F und G allgemeingültigkeitsäquivalent $\iff$ F_{dual} und G_{dual} erfüllbarkeitsäquivalent.
F und G erfüllbarkeitsäquivalent $\iff$ F_{dual} und G_{dual} allgemeingültigkeitsäquivalent.

Zu jeder Formel kann man eine erfüllbarkeitsäquivalente Formel in pränexer NNF konstruieren, die keine Existenzquantoren enthält.

Beweisidee:

- Verwandle in NNF
- Verwandle weiter in pränexe NNF.
- Skolemisierung (Elimination der Existenzquantoren). Beispiel:
  $\exists u \forall v \forall w \exists x \forall y \exists z \, F(u, v, w, x, y, z)$
  $\forall v \forall w \forall y \, F(a, v, w, f(v, w), y, g(v, w, y))$

Dazu dual:

Zu jeder Formel kann man eine allgemeingültigkeitsäquivalente Formel in pränexer NNF konstruieren, die keine Allquantoren enthält.

Skolemisierung muss dabei die Allquantoren eliminieren.

Beispiel:
$\forall u \exists v \exists w \forall x \exists y \forall z \, F(u, v, w, x, y, z)$
$\exists v \exists w \exists y \, F(a, v, w, f(v, w), y, g(v, w, y))$

Satz von Herbrand:

Ein Existenzabschluss $\exists[F]$ einer quantorenfreien Formel F ist genau dann allgemeingültig, wenn es Grundinstanzen $F_1, \ldots, F_r$ von F gibt, sodass $F_1 \vee \ldots \vee F_r$ allgemeingültig ist.

Dual dazu:

Ein Allabschluss $\forall[F]$ einer quantorenfreien Formel F ist genau dann unerfüllbar, wenn es Grundinstanzen $F_1, \ldots, F_r$ von F gibt, sodass $F_1 \wedge \ldots \wedge F_r$ unerfüllbar ist.

Wenn eine Klauselmenge unerfüllbar ist, dann gibt es eine endliche Menge von Grundinstanzen dieser Klauseln, die unerfüllbar ist.