Theorie der Informatik

3. Aussagenlogik III

Malte Helmert   Gabriele Röger

Universität Basel

26. Februar 2014

Theorie der Informatik

26. Februar 2014 — 3. Aussagenlogik III

3.1 Formelmengen

Wissensbasis: Beispiel

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

$$\begin{aligned}\text{WB} = \{&(\neg\text{TrinktBier} \rightarrow \text{IsstFisch}),\\ &((\text{IsstFisch} \wedge \text{TrinktBier}) \rightarrow \neg\text{IsstEiscreme}),\\ &((\text{IsstEiscreme} \vee \neg\text{TrinktBier}) \rightarrow \neg\text{IsstFisch})\}\end{aligned}$$

Foto mit freundlicher Genehmigung von graur razvan ionut / FreeDigitalPhotos.net

Modelle für Formelmengen

Definition (Modell für Wissensbasis)

Sei WB eine Wissensbasis über A, d.h. eine Menge von aussagenlogischen Formeln über A.

Eine Wahrheitsbelegung $\mathcal{I}$ für A ist ein Modell für WB, wenn $\mathcal{I}$ ein Modell für jede Formel $\varphi \in \mathrm{WB}$ ist.

Eigenschaften von Formelmengen

Eine Wissensbasis WB ist

- erfüllbar, falls WB mindestens ein Modell besitzt.
- unerfüllbar, falls WB nicht erfüllbar ist.
- gültig (oder Tautologie), falls jede Wahrheitsbelegung ein Modell für WB ist.
- falsifizierbar, falls WB keine Tautologie ist.

Beispiel I

Welche der Eigenschaften hat $\mathrm{WB} = \{(A \land \neg B), \neg(B \lor A)\}$?

WB ist unerfüllbar:
Für jedes Modell $\mathcal{I}$ mit $\mathcal{I} \models (A \land \neg B)$ gilt $\mathcal{I}(A) = 1$.
Damit gilt $\mathcal{I} \models (B \lor A)$ und daher nicht $\mathcal{I} \models \neg(B \lor A)$.

Daraus folgt direkt falsifizierbar, nicht erfüllbar, keine Tautologie.

Beispiel II

Welche der Eigenschaften hat

$$\begin{aligned}\mathrm{WB} = \{&(\neg\mathrm{TrinktBier} \rightarrow \mathrm{IsstFisch}),\\ &((\mathrm{IsstFisch} \land \mathrm{TrinktBier}) \rightarrow \neg\mathrm{IsstEiscreme}),\\ &((\mathrm{IsstEiscreme} \lor \neg\mathrm{TrinktBier}) \rightarrow \neg\mathrm{IsstFisch})\}?\end{aligned}$$

- erfüllbar, z.B. mit $\mathcal{I} = \{\mathrm{IsstFisch} \mapsto 1, \mathrm{TrinktBier} \mapsto 1, \mathrm{IsstEiscreme} \mapsto 0\}$
- damit nicht unerfüllbar
- falsifizierbar, z.B. mit $\mathcal{I} = \{\mathrm{IsstFisch} \mapsto 0, \mathrm{TrinktBier} \mapsto 0, \mathrm{IsstEiscreme} \mapsto 1\}$
- damit nicht gültig

3.2 Logische Folgerung

Logische Folgerung: Motivation

Worin besteht das Geheimnis Ihres langen Lebens?

Ich halte mich streng an Diätregeln: 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.

Behauptung: Die Frau trinkt Bier zu jeder Mahlzeit.

Wie können wir das folgern?

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

Logische Folgerung

Definition (Logische Konsequenz)

Sei WB eine Menge von Formeln und φ eine Formel.

Wir sagen, dass φ logisch aus WB folgt (auch: φ ist eine logische Konsequenz von WB, symbolisch WB $\models \varphi$), wenn alle Modelle für WB auch Modelle für φ sind.

Achtung: Das Symbol $\models$ ist „überladen“: WB $\models \varphi$ vs. $\mathcal{I} \models \varphi$.

Was ist, wenn WB unerfüllbar oder die leere Menge ist?

Logische Folgerung: Beispiel

Sei $\varphi = \text{TrinktBier}$ und

$$\begin{aligned}\text{WB} = \{&(\neg\text{TrinktBier} \rightarrow \text{IsstFisch}),\\ &((\text{IsstFisch} \land \text{TrinktBier}) \rightarrow \neg\text{IsstEiscreme}),\\ &((\text{IsstEiscreme} \lor \neg\text{TrinktBier}) \rightarrow \neg\text{IsstFisch})\}.\end{aligned}$$

Zeige: WB $\models \varphi$

Beweis.

Beweis durch Widerspruch: Angenommen $\mathcal{I}$ ist ein Modell von WB, aber $\mathcal{I} \not\models \text{TrinktBier}$. Dann gilt $\mathcal{I} \models \neg\text{TrinktBier}$. Da $\mathcal{I}$ Modell von WB, gilt auch $\mathcal{I} \models (\neg\text{TrinktBier} \rightarrow \text{IsstFisch})$ und damit $\mathcal{I} \models \text{IsstFisch}$. Mit der analogen Argumentation erhalten wir über $\mathcal{I} \models ((\text{IsstEiscreme} \lor \neg\text{TrinktBier}) \rightarrow \neg\text{IsstFisch})$ das Ergebnis $\mathcal{I} \models \neg\text{IsstFisch}$ und damit $\mathcal{I} \not\models \text{IsstFisch}$. $\rightsquigarrow$ Widerspruch $\square$

Wichtige Sätze zur logischen Folgerung

Theorem (Deduktionstheorem)

$WB \cup \{\varphi\} \models \psi$ gdw. $WB \models (\varphi \rightarrow \psi)$

Theorem (Kontrapositionstheorem)

$WB \cup \{\varphi\} \models \neg\psi$ gdw. $WB \cup \{\psi\} \models \neg\varphi$

Theorem (Widerlegungstheorem)

$WB \cup \{\varphi\}$ ist unerfüllbar gdw. $WB \models \neg\varphi$

Beweis des Deduktionstheorems

Deduktionstheorem: WB $\cup \{\varphi\} \models \psi$ gdw. WB $\models (\varphi \rightarrow \psi)$

Beweis.

"$\Rightarrow$": Voraussetzung ist, dass WB $\cup \{\varphi\} \models \psi$.
Wir müssen zeigen, dass WB $\models (\varphi \rightarrow \psi)$, d.h. dass alle Modelle für WB die Formel $(\varphi \rightarrow \psi)$ erfüllen. Betrachte ein beliebiges Modell $\mathcal{I}$ für WB. Wir unterscheiden zwei Fälle:

- Fall 1: $\mathcal{I} \models \varphi$.
  Dann ist $\mathcal{I}$ ein Modell für WB $\cup \{\varphi\}$ und, wegen der Voraussetzung, $\mathcal{I} \models \psi$. Daraus können wir schliessen, dass $\mathcal{I} \models (\varphi \rightarrow \psi)$.
- Fall 2: $\mathcal{I} \not\models \varphi$.
  Wir können direkt schliessen, dass $\mathcal{I} \models (\varphi \rightarrow \psi)$.

... ...

Beweis des Deduktionstheorems

Deduktionstheorem: WB $\cup \{\varphi\} \models \psi$ gdw. WB $\models (\varphi \rightarrow \psi)$

Beweis (Fortsetzung).

"$\Leftarrow$": Voraussetzung ist, dass WB $\models (\varphi \rightarrow \psi)$.
Wir müssen zeigen, dass WB $\cup \{\varphi\} \models \psi$, d.h., dass alle Modelle für WB $\cup \{\varphi\}$ die Formel ψ erfüllen. Betrachte ein beliebiges solches Modell $\mathcal{I}$ für WB $\cup \{\varphi\}$.

Nach Definition gilt $\mathcal{I} \models \varphi$. Da $\mathcal{I}$ ein Modell für WB ist, folgt mit der Voraussetzung, dass $\mathcal{I} \models (\varphi \rightarrow \psi)$.

Zusammen ergibt sich $\mathcal{I} \models (\varphi \wedge (\varphi \rightarrow \psi)) \equiv (\varphi \wedge \psi)$, woraus folgt, dass $\mathcal{I} \models \psi$. $\square$

Beweis des Kontrapositionstheorems

Kontrapositiontheorem: WB $\cup \{\varphi\} \models \neg\psi$ gdw. WB $\cup \{\psi\} \models \neg\varphi$

Beweis.

Wegen des Deduktionstheorems gilt
WB $\cup \{\varphi\} \models \neg\psi$ gdw. WB $\models (\varphi \rightarrow \neg\psi)$.

Aus dem gleichen Grund gilt
WB $\cup \{\psi\} \models \neg\varphi$ gdw. WB $\models (\psi \rightarrow \neg\varphi)$.

Zudem gilt $(\varphi \rightarrow \neg\psi) \equiv (\neg\varphi \vee \neg\psi) \equiv (\neg\psi \vee \neg\varphi) \equiv (\psi \rightarrow \neg\varphi)$.

Zusammen ergibt sich wie gefordert

$$\begin{array}{rl} & \text{WB} \cup \{\varphi\} \models \neg\psi \\ \text{gdw.} & \text{WB} \models (\neg\varphi \vee \neg\psi) \\ \text{gdw.} & \text{WB} \cup \{\psi\} \models \neg\varphi. \end{array}$$

$\square$

Beweis des Widerlegungstheorems

Übungsaufgabe

3.3 Inferenz

Inferenz: Motivation

- Bisher: Beweise über logische Folgerung mit semantischen Argumenten
- Kein allgemeiner Algorithmus
- Lösung: mit syntaktischen Inferenzregeln Formeln produzieren, die logisch aus gegebenen Formeln folgen
- Vorteil: mechanische Arbeitsweise einfach algorithmisch implementierbar

Inferenzregeln

- Inferenzregeln haben die Form

$$\frac{\varphi_1, \dots, \varphi_k}{\psi}.$$

- Bedeutung: „Jedes Modell für $\varphi_1, \dots, \varphi_k$ ist Modell für ψ."
- Eine Inferenzregel mit $k = 0$ heisst Axiom.
- Eine Menge von syntaktischen Inferenzregeln nennt man Kalkül oder Beweissystem.

Einige Inferenzregeln der Aussagenlogik

Modus ponens $\dfrac{\varphi,\ (\varphi \rightarrow \psi)}{\psi}$

Modus tollens $\dfrac{\neg\psi,\ (\varphi \rightarrow \psi)}{\neg\varphi}$

Und-Eliminierung $\dfrac{(\varphi \land \psi)}{\varphi}$ $\dfrac{(\varphi \land \psi)}{\psi}$

Und-Einführung $\dfrac{\varphi,\ \psi}{(\varphi \land \psi)}$

Oder-Einführung $\dfrac{\varphi}{(\varphi \lor \psi)}$

$(\leftrightarrow)$-Eliminierung $\dfrac{(\varphi \leftrightarrow \psi)}{(\varphi \rightarrow \psi)}$ $\dfrac{(\varphi \leftrightarrow \psi)}{(\psi \rightarrow \varphi)}$

Ableitungen

Definition (Ableitung)

Eine Ableitung oder ein Beweis einer Formel φ aus einer Wissensbasis WB ist eine Sequenz von Formeln $\psi_1, \dots, \psi_k$ für die gilt, dass

- $\psi_k = \varphi$ und
- für alle $i \in \{1, \dots, k\}$:
  - $\psi_i \in$ WB, oder
  - ψ_i ist das Ergebnis der Anwendung einer Inferenzregel auf Elemente aus $\{\psi_1, \dots, \psi_{i-1}\}$.

Ableitung: Beispiel

Beispiel

Gegeben: WB $= \{P, (P \rightarrow Q), (P \rightarrow R), ((Q \land R) \rightarrow S)\}$
Gesucht: Ableitung von $(S \land R)$ aus WB.

1. P (WB)
2. $(P \rightarrow Q)$ (WB)
3. Q (1, 2, Modus ponens)
4. $(P \rightarrow R)$ (WB)
5. R (1, 4, Modus ponens)
6. $(Q \land R)$ (3, 5, Und-Einführung)
7. $((Q \land R) \rightarrow S)$ (WB)
8. S (6, 7, Modus ponens)
9. $(S \land R)$ (8, 5, Und-Einführung)

Korrektheit und Vollständigkeit

Definition (Korrektheit und Vollständigkeit eines Kalküls)

Wir schreiben WB $\vdash_K \varphi$, wenn es eine Ableitung von φ aus WB im Kalkül K gibt. (Falls der Kalkül K aus dem Kontext hervor geht, manchmal auch nur WB $\vdash \varphi$.)

Ein Kalkül K ist korrekt, wenn für alle WB und φ aus WB $\vdash_K \varphi$ folgt, dass WB $\models \varphi$.

Ein Kalkül K ist vollständig, wenn für all WB und φ aus WB $\models \varphi$ folgt, dass WB $\vdash_K \varphi$.

Betrachte den Kalkül K, der aus den vorhin gesehenen Ableitungsregeln besteht.
Frage: Ist K korrekt?
Frage: Ist K vollständig?

Widerlegungsvollständigkeit

- Offensichtlich wollen wir korrekte Kalküle
- Brauchen wir immer einen vollständigen Kalkül?
- Widerlegungstheorem:
  $\mathrm{WB} \cup \{\varphi\}$ ist unerfüllbar gdw. $\mathrm{WB} \models \neg\varphi$
- Daraus folgt, dass $\mathrm{WB} \models \varphi$ gdw. $\mathrm{WB} \cup \{\neg\varphi\}$ ist unerfüllbar
- Wir können also das allgemeine Folgerungsproblem auf einen Test auf Unerfüllbarkeit reduzieren.
- Wir verwenden in Kalkülen das spezielle Symbol $\square$ für (bewiesenermassen) unerfüllbare Formeln.

Definition (Widerlegungsvollständigkeit)

Ein Kalkül K ist widerlegungsvollständig, wenn für alle unerfüllbaren WB gilt, dass $\mathrm{WB} \vdash_K \square$.

3.4 Resolutionskalkül

Resolution: Idee

- Resolution ist ein widerlegungsvollständiger Kalkül für Wissensbasen in konjunktiver Normalform.
- Alle Wissensbasen können in äquivalente Formeln in KNF transformiert werden.
  - Transformation kann exponentielle Zeit benötigen.
  - Alternative: Effiziente Transformation in erfüllbarkeitsäquivalente Formeln (nicht Stoff dieser Vorlesung)
- Zeige $\mathrm{WB} \models \varphi$ durch Ableitbarkeit $\mathrm{WB} \cup \{\neg\varphi\} \vdash_R \square$ mit Resolutionskalkül R.
- Resolution kann exponentielle Zeit benötigen.
- Dies ist wahrscheinlich für alle widerlegungsvollständigen Beweismethoden der Fall. $\rightsquigarrow$ Komplexitätstheorie

Wissensbasen als Klauselmengen

Vereinfachte Notation von Wissensbasen in KNF

- Formel in KNF als Menge von Klauseln
  (wegen Kommutativität, Idempotenz, Assoziativität von $\wedge$)
- Menge von Formeln ebenfalls als Menge von Klauseln
- Klausel als Menge von Literalen
  (wegen Kommutativität, Idempotenz, Assoziativität von $\vee$)
- Wissensbasis als Menge von Mengen von Literalen

Beispiel

$$\mathrm{WB} = \{(P \vee P), ((\neg P \vee Q) \wedge (\neg P \vee R) \wedge (\neg P \vee Q) \wedge R), ((\neg Q \vee \neg R \vee S) \wedge P)\}$$

als Klauselmenge:

$$\Delta = \{\{P\}, \{\neg P, Q\}, \{\neg P, R\}, \{R\}, \{\neg Q, \neg R, S\}\}$$

Resolutionsregel

Der Resolutionskalkül besteht aus einer einzigen Regel, genannt Resolutionsregel:

$$\frac{K_1 \cup \{L\},\ K_2 \cup \{\neg L\}}{K_1 \cup K_2},$$

wobei K_1 und K_2 (möglicherweise leere) Klauseln sind und L eine atomare Formel ist.

Leiten wir die leere Klausel ab, schreiben wir $\square$ statt $\{\}$.

Terminologie:

- L und $\neg L$ sind die Resolutionsliterale,
- $K_1 \cup \{L\}$ and $K_2 \cup \{\neg L\}$ sind die Elternklauseln und
- $K_1 \cup K_2$ ist der Resolvent.

Resolutionsbeweis

Definition (Resolutionsbeweis)

Ein Resolutionsbeweis einer Klausel D aus einer Wissensbasis Δ ist eine Sequenz von Klauseln $K_1, \dots, K_n$ mit

- $K_n = D$ und
- für alle $i \in \{1, \dots, n\}$:
  - $K_i \in \Delta$, oder
  - K_i ist Resolvent zweier Klauseln aus $\{K_1, \dots, K_{i-1}\}$.

Wenn es einen Resolutionsbeweis von D aus Δ gibt, sagen wir D kann mit Resolution aus Δ abgeleitet werden und schreiben $\Delta \vdash_R D$.

Anmerkung: Resolution ist ein korrekter, widerlegungsvollständiger, aber unvollständiger Kalkül.

Resolutionsbeweis: Beispiel

Resolutionsbeweis zum Testen einer logischen Folgerung: Beispiel

Gegeben: $\mathrm{WB} = \{P, (P \rightarrow (Q \wedge R))\}$.
Zeige per Resolution, dass $\mathrm{WB} \models (R \vee S)$.

Drei Schritte:

1. Reduziere logische Folgerung auf Unerfüllbarkeit.
2. Transformiere Wissensbasis in Klauselform (KNF).
3. Leite leere Klausel $\square$ mit Resolution ab.

Schritt 1: Reduziere logische Folgerung auf Unerfüllbarkeit.

$\mathrm{WB} \models (R \vee S)$ gdw $\mathrm{WB} \cup \{\neg(R \vee S)\}$ ist unerfüllbar.

Betrachte daher
$\mathrm{WB}' = \mathrm{WB} \cup \{\neg(R \vee S)\} = \{P, (P \rightarrow (Q \wedge R)), \neg(R \vee S)\}$.

...

Resolutionsbeweis: Beispiel (Fortsetzung)

Resolution zum Testen einer logischen Folgerung: Beispiel (Forts.)

$\mathrm{WB}' = \{P, (P \rightarrow (Q \wedge R)), \neg(R \vee S)\}$.

Schritt 2: Transformiere Wissensbasis in Klauselform (KNF).

- P
  $\rightsquigarrow$ Klauseln: $\{P\}$
- $P \rightarrow (Q \wedge R)) \equiv (\neg P \vee (Q \wedge R)) \equiv ((\neg P \vee Q) \wedge (\neg P \vee R))$
  $\rightsquigarrow$ Klauseln: $\{\neg P, Q\}, \{\neg P, R\}$
- $\neg(R \vee S) \equiv (\neg R \wedge \neg S)$
  $\rightsquigarrow$ Klauseln: $\{\neg R\}, \{\neg S\}$

$\Delta = \{\{P\}, \{\neg P, Q\}, \{\neg P, R\}, \{\neg R\}, \{\neg S\}\}$

...

Resolutionsbeweis: Beispiel (Fortsetzung)

Resolution zum Testen einer logischen Folgerung: Beispiel (Forts.)

$\Delta = \{\{P\}, \{\neg P, Q\}, \{\neg P, R\}, \{\neg R\}, \{\neg S\}\}$

Schritt 3: Leite leere Klausel $\square$ mit Resolution ab.

- $K_1 = \{P\}$ (aus Δ)
- $K_2 = \{\neg P, Q\}$ (aus Δ)
- $K_3 = \{\neg P, R\}$ (aus Δ)
- $K_4 = \{\neg R\}$ (aus Δ)
- $K_5 = \{Q\}$ (aus K_1 und K_2)
- $K_6 = \{\neg P\}$ (aus K_3 und K_4)
- $K_7 = \square$ (aus K_1 und K_6)

Hinweis: Es gibt kürzere Beweise. (Zum Beispiel?)

Noch ein Beispiel

Noch ein Resolutionsbeispiel

Zeige mit Resolution, dass WB $\models$ TrinktBier, wobei

$$\begin{aligned}\text{WB} = \{&(\neg\text{TrinktBier} \rightarrow \text{IsstFisch}),\\ &((\text{IsstFisch} \wedge \text{TrinktBier}) \rightarrow \neg\text{IsstEiscreme}),\\ &((\text{IsstEiscreme} \vee \neg\text{TrinktBier}) \rightarrow \neg\text{IsstFisch})\}.\end{aligned}$$

Grösseres Beispiel: Blutgruppen

Wir wissen folgendes:

- Ist Test T positiv, hat die Person Blutgruppe A oder AB.
- Ist Test S positiv, hat die Person Blutgruppe B oder AB.
- Hat eine Person Blutgruppe A, dann ist Test T positiv.
- Hat eine Person Blutgruppe B, dann ist Test S positiv.
- Hat eine Person Blutgruppe AB, sind beide Tests positiv.
- Jede Person hat genau eine der Blutgruppen A, B, AB, 0.
- Für eine gegebene Person ist Test T positiv und Test S negativ.

Zeigen Sie, dass die gegebene Person Blutgruppe A oder 0 hat.

3.5 Zusammenfassung

Zusammenfassung

- Wissensbasis ist Formelmenge, die gegebene Informationen beschreibt.
- Logische Folgerung WB $\models \varphi$ erlaubt auf Basis der Semantik zu schliessen, dass φ aus WB folgt.
- Ein korrekter Kalkül erlaubt solche Schlussfolgerungen auf Basis rein syntaktischer Ableitungen WB $\vdash \varphi$.
- Vollständige Kalküle meist nicht notwendig: Für viele Fragestellungen reicht Widerlegungsvollständigkeit.
- Resolutionskalkül ist korrekt und widerlegungsvollständig.

Weiterführende Themen

Es gibt noch viele Bereiche der Aussagenlogik, die wir in dieser Vorlesung nicht behandeln.

- Resolutionsstrategien, um Resolution in der Praxis so effizient wie möglich zu machen
- Andere Beweissysteme, wie zum Beispiel Tableauxbeweise
- Algorithmen zur Modellkonstruktion, zum Beispiel das Davis-Putnam-Logemann-Loveland-Verfahren (DPLL)