Theorie der Informatik

5. Aussagenlogik III

Malte Helmert Gabriele Röger

Universität Basel

9. März 2015

Theorie der Informatik

9. März 2015 — 5. Aussagenlogik III

5.1 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:
  WB $\cup \{\varphi\}$ ist unerfüllbar gdw. WB $\models \neg\varphi$
- Daraus folgt, dass WB $\models \varphi$ gdw. 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 WB $\vdash_K \square$.

5.2 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 WB $\models \varphi$ durch Ableitbarkeit 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.)

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

Schritt 2: Transformiere Wissensbasis in Klauselform (KNF).

- P
  $\rightsquigarrow$ Klauseln: $\{P\}$
- $P \rightarrow (Q \land R)) \equiv (\neg P \lor (Q \land R)) \equiv ((\neg P \lor Q) \land (\neg P \lor R))$
  $\rightsquigarrow$ Klauseln: $\{\neg P, Q\}, \{\neg P, R\}$
- $\neg(R \lor S) \equiv (\neg R \land \neg S)$
  $\rightsquigarrow$ 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 $\mathrm{WB} \models \mathrm{TrinktBier}$, wobei

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

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.

5.3 Zusammenfassung

Zusammenfassung

- 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)