Vorlesung
– Automatisches Beweisen –

Kap. 4.2: AL-Entscheidungsverfahren
Kap. 4.2.1 Aussagenlogische Resolution

Prof. Dr. Wolfgang Küchlin

Dipl.-Inform., Dr. sc. techn. (ETH)

Arbeitsbereich Symbolisches Rechnen
Wilhelm-Schickard-Institut für Informatik
Fakultät für Informations- und Kognitionswissenschaften

Universität Tübingen

Steinbeis Transferzentrum
Objekt- und Internet-Technologien (OIT)

Wolfgang.Kuechlin@uni-tuebingen.de
http://www-sr.informatik.uni-tuebingen.de

SR 

Kap 4.2

Aussagenlogische Entscheidungsverfahren

Vorlesungen 30.10.08—5.11.08

SR

Aussagenlogische Entscheidungsverfahren

- Resolution
- Davis-Putnam-Logemann-Loveland (DPLL)
- Ordered Binary Decision Diagrams (OBDDs)
- Semantische Tableaus
- Boolesche Polynome

Kalkül

- **Kalkül** (= formales Regelsystem) zum Herleiten neuer Formeln aus gegebener Formelmenge
  - Formeln werden „mechanisch“ erzeugt
  - Daher eignet sich ein Kalkül zur Implementierung
- Schreibweise: $\mathcal{F} \vdash F$

  Formel F wird aus der Formelmenge $\mathcal{F}$ hergeleitet
- Sinnvoll ist das nur, falls die neue Formel auch „gilt“

  d.h. falls aus $\mathcal{F} \vdash F$ folgt $\mathcal{F} \models F$
  - wir sagen: der Kalkül ist korrekt (sound).
- Wenn wir alles Wahre ableiten können, ist der Kalkül vollständig (complete): aus $\mathcal{F} \models F$ folgt $\mathcal{F} \vdash F$
- Widerlegungsvollständig: aus $\mathcal{F} \models \bot$ folgt $\mathcal{F} \vdash \bot$

Resolution

- **Kalkül** zum Herleiten (aussagenlogischer) Formeln in CNF
  - **Deduktionsverfahren:** gegeben $\mathcal{F}$, leite neue Formel F daraus her.
- Entwickelt 1965 von **John Alan Robinson**
  - Ursprünglich für Prädikatenlogik erster Stufe
  - A machine-oriented logic based on the resolution principle. *Journal of the ACM* **12**(1), 23—41.
- Aus Axiomensystem $\mathcal{F}$ (in CNF) können neue gültige Formeln (Resolventen) F_i hergeleitet werden, $\mathcal{F} \vdash F_i$
- Erste Idee: beweise $\mathcal{F} \models F$ durch direkte Herleitung $\mathcal{F} \vdash F$
  - geht nicht immer, da Resolution nur widerlegungsvollständig
- Üblicher Umweg:
  - $\mathcal{F} \models F$ gdw. es gilt nie $\mathcal{F} \wedge \neg F$.
  - es gilt nie $\mathcal{F} \wedge \neg F$ gdw. $\mathcal{F} \wedge \neg F \models \bot$
  - da Resolution widerlegungsvollständig: $\mathcal{F} \wedge \neg F \models \bot$ gdw. $\mathcal{F} \wedge \neg F \vdash \bot$
  - Insgesamt: $\mathcal{F} \models F$ gdw. $\mathcal{F} \wedge \neg F \vdash_{Res} \bot$

Resolution

- Anwendung: Beweise **Unerfüllbarkeit** einer Klauselmenge $\mathcal{F}$ durch Herleiten der (unerfüllbaren) leeren Klausel $\{\bot\}$, also $\mathcal{F} \vdash^* \bot$
- Methode:
  - Wende **Inferenzregel(n)** zur Herleitung der leeren Klausel an.

    (Leere Klausel { }, gleichbedeutend mit $\{\bot\}$, im Kalkül üblicherweise symbolisiert durch , ist nicht erfüllbar,)
  - **Axiome**: Klauseln der Ausgangsformel
  - Falls sich leere Klausel herleiten lässt, ist ein **Beweis** der Unerfüllbarkeit gefunden.

J. A. Robinson (Quelle: Wikipedia)

- **John Alan Robinson** (* 1930 in Yorkshire, Großbritannien) ist ein englischer Philosoph und Logiker, der wichtige Beiträge zur Logikprogrammierung geleistet hat.
- Nach einem abgeschlossenen Studium der Klassischen Altertums-wissenschaft an der Uni Cambridge ging er 1952 in die USA. Dort studierte er zunächst Philosophie an der U. Oregon und promovierte 1956 in Princeton zum Ph.D. Danach arbeitete er beim Chemiekonzern DuPont, wo er Programmieren und Mathematik lernte. 1961 wechselte er an die Rice University, wo er sich weiter mit Mathematik beschäftigte.
- 1965 veröffentliche er mit „A machine-oriented logic based on the resolution principle“ [J.ACM 12(1)] wichtige Grundlagen zur automatisierbaren Resolution in der Logik. Auf ihn geht ein Algorithmus zur Unifikation von prädikatenlogischen Formeln zurück, der entscheidend beim Nachweis der Unerfüllbarkeit einer prädikatenlogischen Formel ist.

Resolution (2)

- (Einzige) Inferenzregel:

$$\frac{C \cup \{l\} \qquad D \cup \{\neg l\}}{C \cup D}\,\text{Res}$$

wobei C U $\{\ell\}$, D U $\{\neg\ell\}$ Klauseln.

- Beispiele:

$$\frac{\{x, y, \neg z\} \quad \{u, \neg v, z\}}{\{x, y, u, \neg v\}} \qquad \frac{\{x, u, \neg v\} \quad \{\neg u\}}{\{x, \neg v\}}$$

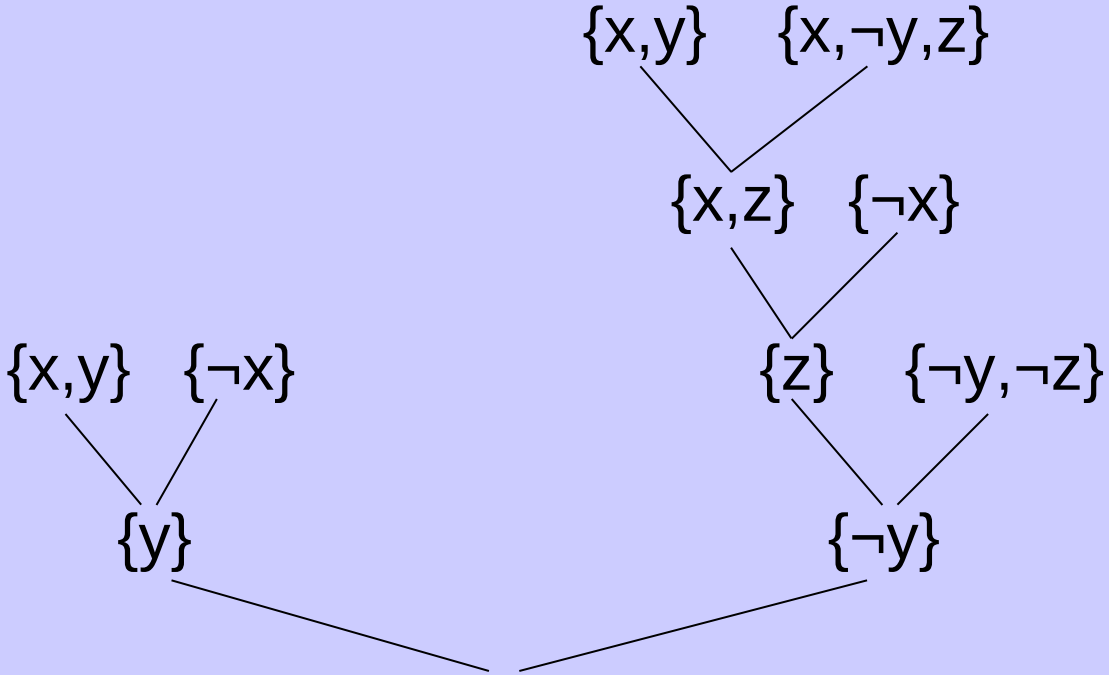
Resolution (3)

$$\frac{K_1 \quad K_2}{R}\text{Res}$$

- Begriffe allgemein bei Kalkül:
  - K_1, K_2: Prämissen
  - R: Konklusion
- Begriffe bei Resolutionsregel:
  - R: Resolvente *(resolvent)*
  - K_1, K_2: Eltern-Klauseln *(parent clauses)*
  - „R entsteht durch Resolution über ℓ aus K_1 und K_2“
  - Leere Klausel ist nicht erfüllbar, steht für {⊥}

Resolutionsbeweis: Beispiel

F3={{x,y},{x,¬y,z},{¬x},{¬y,¬z}}



Resolution (4)

- Herleitungsbegriff: $F \vdash C$
  - Aus der Klauselmenge F lässt sich durch eine endliche Anzahl von Anwendungen der Resolutionsregel die Klausel C herleiten
- Resolutionsabschluss:
  - $Res^0(F) = F$
  - $Res^1(F) = F \cup \{R \mid R$ (nicht-tautologische Resolvente zweier Klauseln K_1, K_2 aus F$\}$
  - $Res^{k+1}(F) = Res^1(Res^k(F))$ für $k \geq 1$
  - $Res^*(F) = \bigcup_{k \geq 0} Res^k(F)$

Resolution (5)

- Der Resolutionskalkül ist korrekt (sound). D.h. für alle Formeln F und alle Klauseln D gilt:

  $F \vdash^*_{Res} D$ impliziert $F \models D$

- Der Resolutionskalkül ist widerlegungsvollständig *(refutation complete)*. D.h. für alle Formeln F gilt:

  F unerfüllbar impliziert $F \vdash^*_{Res}$

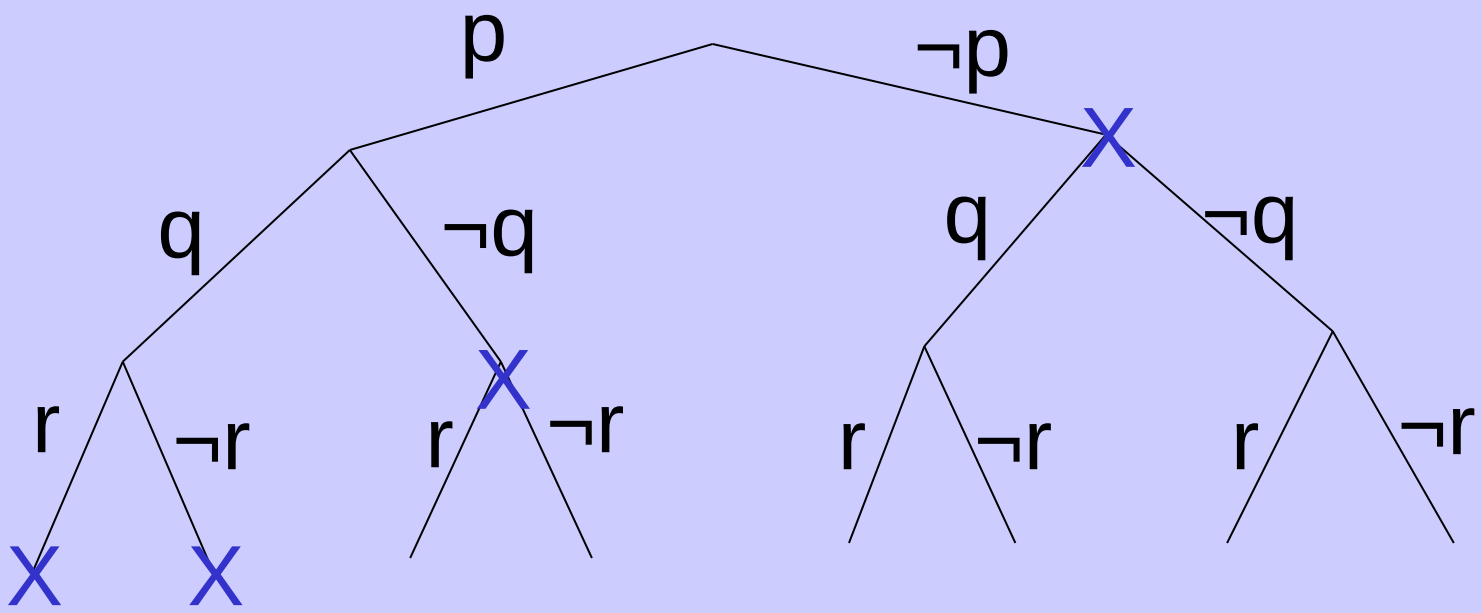
Resolution (6)

- Korrektheit:
  - Die Konklusion C∪D wird von den Prämissen C∪{ℓ}, D∪{¬ℓ} impliziert.
    - Jede Interpretation, die die Prämissen wahr macht, muss entweder ℓ oder ¬ℓ wahr machen.
    - Falls b(ℓ)=1, so b(D)=1; falls b(¬ℓ)=1, so b(C)=1.

      Also in jedem Fall b(C ∪ D)=1
  - Damit ist ein einzelner Beweisschritt korrekt. Korrektheit einer Ableitungskette folgt per Induktion
- Widerlegungs-Vollständigkeit
  - semantische Bäume: Repräsentation aller Belegungen als Baum
  - Auswirkungen eines Resolutionsschritts auf diesen Baum

Semantische Bäume

S = {{p}, {¬p,q}, {¬r}, {¬p,¬q,r}}



Belegung: Pfad im Baum
Fehlerknoten (X): Hier wird eine Klausel falsifiziert

Semantische Bäume (2)

- Jeder Zweig b in $\mathcal{T}$ definiert eine Interpretation β; gilt $\beta(F)=0$, dann heißt b geschlossen, sonst offen.
- $\mathcal{T}$ ist geschlossen, wenn alle Zweige geschlossen sind.

- $\mathcal{T}$ ist geschlossen, genau dann wenn F unerfüllbar.

Semantische Bäume (3)

- Ein Knoten eines Zweiges, der F falsifiziert und der Wurzel am nächsten ist, heißt Fehlerknoten.
- Eine Klausel, die durch einen Fehlerknoten falsifiziert wird, ist die mit diesem Fehlerknoten assoziierte Klausel.
- Ein Inferenzknoten ist ein Knoten, dessen Kinder beide Fehlerknoten sind.

Widerlegungsvollständigkeit der Resolution

- F unerfüllbar genau dann, wenn $\mathcal{T}$ geschlossen.
- In einem (nicht-trivialen) geschlossenen $\mathcal{T}$ gibt es mindestens einen Inferenzknoten n (mit Kindern n_1, n_2).
- Seien C_1 und C_2 die mit den Fehlerknoten n_1 und n_2 assoziierten Klauseln. Diese unterscheiden sich dann (mindestens) in dem unterhalb des Fehlerknotens belegten Literal. Wenn C_1 nach x=1 falsifiziert wird, dann ist $C_1 = C \cup \{\neg x\}$, entsprechend $D_1 = D \cup \{x\}$.
- Dann können C und D resolviert werden. Die partielle Interpretation in n falsifiziert die Resolvente $R=C \cup D$, da sowohl C und D schon am Knoten n falsifiziert werden.
- $F \cup \{R\}$ hat einen Fehlerknoten, der entweder n ist, oder ein Vorgänger von n, und R ist die mit diesem Knoten assoziierte Klausel.

Varianten der Resolution: Unit-Resolution

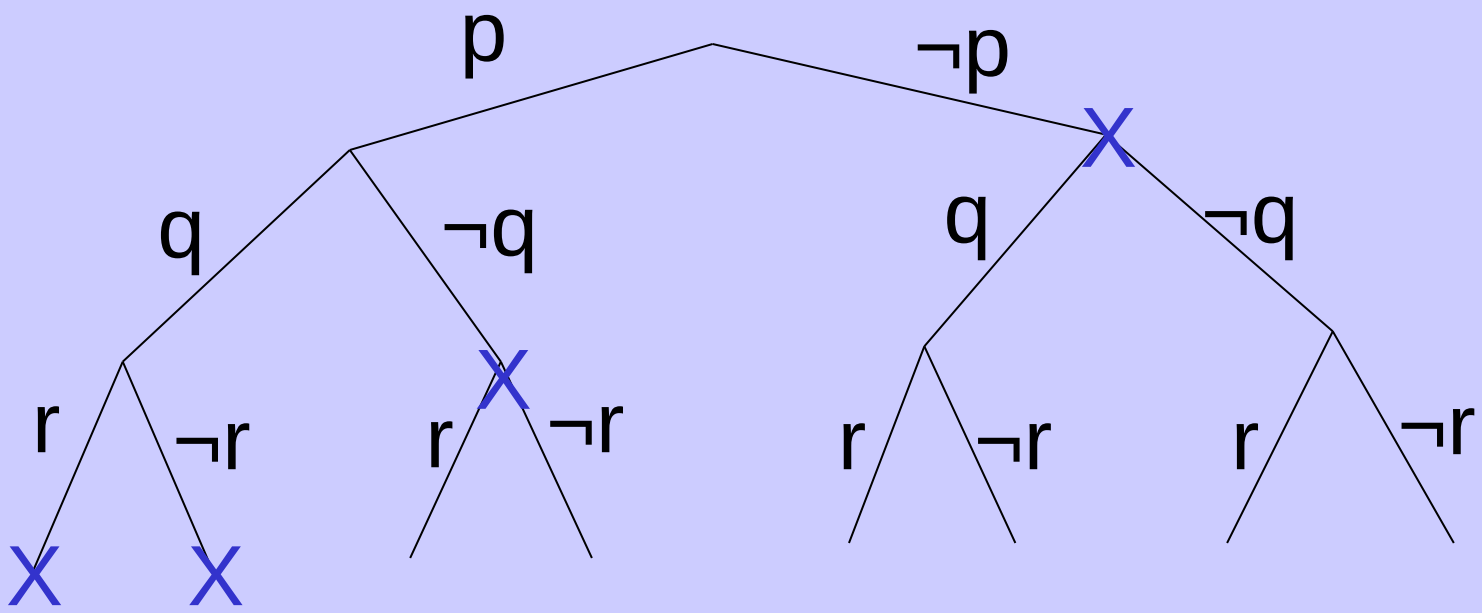
- Ziel: schränke Bildung von Resolventen ein ohne die Vollständigkeit zu verlieren
- Unit-Resolution
  - Mindestens eine Elternklausel ist Unit-Klausel
    - Aus dem Resolutionspartner wird ein Literal gelöscht
  - Unit-Resolution ist widerlegungsvollständig für Hornklauseln
  - $F \vdash_{Ures}$ ist in linearer Zeit entscheidbar
  - Unit-Resolution ist nicht mehr widerlegungsvollständig
    - $\{\{a, b\}, \{a, \neg b\}, \{\neg a, b\}, \{\neg a, \neg b\}\} \models$

Varianten der Resolution: Ordered Resolution

- Geordnete Resolution
  - Voraussetzung: strikte, totale Ordnung $\prec$ auf Variablen
  - Literal, über das resolviert wird, muss in jeder Elternklausel maximal sein.
  - Geordnete Resolution ist widerlegungs-vollständig
    - Baue semantischen Baum mit kleinster Variable an der Wurzel, größter Variable an den Blättern
    - Falls $\mathcal{F}$ unerfüllbar gibt es einen Inferenzknoten n.
    - Die entsprechende Resolution an n ist zulässig, da sie über ein maximales Literal resolviert. (Die beteiligten Klauseln können kein größeres Literal beinhalten, da weiter abwärts im Baum für dieses Literal für beide möglichen Belegungen Zweige enthalten sind.)

Semantische Bäume

S = {{p}, {¬p,q}, {¬r}, {¬p,¬q,r}}



Im ersten Schritt einzig zulässig: R({¬p,¬q,r},{¬r})={¬p,¬q}
Im zweiten Schritt einzig zulässig: R({¬p,¬q},{¬p,q})={¬p}
Im dritten Schritt einzig zulässig: R({¬p},{p})={}

Subsumtion / Subsumption

- Eine Klausel C subsumiert *(subsumes)* eine Klausel D, genau dann wenn $C \subseteq D$.
  - subsumieren: unterordnen, unter etwas einordnen
  - Constraint C ist strenger als Constraint D
- Falls Klausel C die Klausel D subsumiert,
  dann gilt $C \models D$.
- Bei Erfüllbarkeitsprüfung können subsumierte Klauseln gelöscht werden.
  - denn sobald C erfüllt ist, ist auch D erfüllt