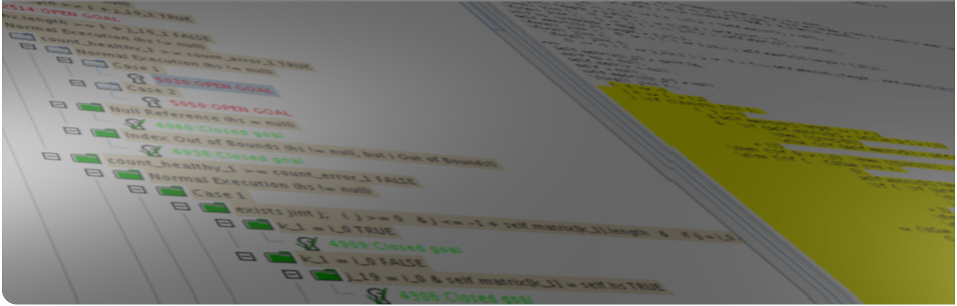
Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2016/2017

Aussagenlogik: Resolutionskalkül

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK



Kalküle für die Aussagenlogik
Übersicht

1. Hilbert-Kalkül
2. Resolutionskalkül
3. Tableaukalkül
4. Sequenzenkalkül

Der aussagenlogische Resolutionkalkül

Merkmale des Resolutionskalküls

- Voraussetzung:
  Alle Formeln sind in konjunktiver Normalform.
- Es gibt eine einzige Regel: die Resolutionsregel
  - Modifikation des Modus Ponens
  - Verallgemeinerung der DPLL-Simplifikation
- Widerlegungskalkül
- Es sind keine logischen Axiome mehr notwendig; insbesondere entfällt die Suche nach („langen“) passenden Instantiierungen der Axiomenschemata Ax1, Ax2, Ax3.

Der aussagenlogische Resolutionkalkül

Merkmale des Resolutionskalküls

- Voraussetzung:
  Alle Formeln sind in konjunktiver Normalform.
- Es gibt eine einzige Regel: die Resolutionsregel
  - Modifikation des Modus Ponens
  - Verallgemeinerung der DPLL-Simplifikation
- Widerlegungskalkül
- Es sind keine logischen Axiome mehr notwendig; insbesondere entfällt die Suche nach („langen“) passenden Instantiierungen der Axiomenschemata Ax1, Ax2, Ax3.

John Alan Robinson (1930 – 2016)

- Studium der Klassischen Altertumswissenschaft (Cambridge 1952) und Philosophie (Princeton 1956)

John Alan Robinson (1930 – 2016)

- Studium der Klassischen Altertumswissenschaft (Cambridge 1952) und Philosophie (Princeton 1956)
- Lehrt Mathematik an der Rice University ab 1961

John Alan Robinson (1930 – 2016)

- Studium der Klassischen Altertumswissenschaft (Cambridge 1952) und Philosophie (Princeton 1956)
- Lehrt Mathematik an der Rice University ab 1961
- Begründung des Resolutionskalküls 1965
  A machine-oriented logic based on the resolution principle

John Alan Robinson (1930 – 2016)

- Studium der Klassischen Altertumswissenschaft (Cambridge 1952) und Philosophie (Princeton 1956)
- Lehrt Mathematik an der Rice University ab 1961
- Begründung des Resolutionskalküls 1965
  A machine-oriented logic based on the resolution principle
- Erfinder des vorgestellten Unifikationsalgorithmus

Syntax

Eine *Klausel* ist eine endliche Menge von Literalen.

Syntax

Eine *Klausel* ist eine endliche Menge von Literalen.

Syntax

Eine *Klausel* ist eine endliche Menge von Literalen.

$\Box$ ist die *leere Klausel*.

Syntax

Eine *Klausel* ist eine endliche Menge von Literalen.

$\square$ ist die *leere Klausel*.

Syntax

Eine *Klausel* ist eine endliche Menge von Literalen.

$\Box$ ist die *leere Klausel*.

Eine Klausel

$$\{P_1, P_2\} \quad \{P_1, \neg P_2\}$$

lesen wir als die Disjunktion der ihr angehörenden Literale:

$$P_1 \vee P_2 \quad P_1 \vee \neg P_2$$

Syntax

Die grundlegende Datenstruktur, auf der wir operieren, sind die *Mengen von Klauseln*,

$$\{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$$

Syntax

Die grundlegende Datenstruktur, auf der wir operieren, sind die *Mengen von Klauseln*,

$$\{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$$

gelesen als Konjunktion der Klauseln.

$$(P_1 \vee P_2) \wedge (P_1 \vee \neg P_2) \wedge (\neg P_1 \vee P_2) \wedge (\neg P_1 \vee \neg P_2)$$

Syntax

Die grundlegende Datenstruktur, auf der wir operieren, sind die *Mengen von Klauseln*,

$$\{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$$

gelesen als Konjunktion der Klauseln.

$$(P_1 \vee P_2) \wedge (P_1 \vee \neg P_2) \wedge (\neg P_1 \vee P_2) \wedge (\neg P_1 \vee \neg P_2)$$

Bis auf die Reihenfolge der Disjunktions- bzw. Konjunktionsglieder sind also in umkehrbar eindeutiger Weise die Formeln in konjunktiver Normalform als Klauselmengen wiedergegeben.

Semantik

Ist $I : \Sigma \rightarrow \{W, F\}$ eine Interpretation der Atome, so hat man als zugehörige Auswertung
val_I : Mengen von Klauseln $\rightarrow \{W, F\}$:

$$val_I(M) = \begin{cases} W & \text{falls für alle } C \in M \text{ gilt: } val_I(C) = W \\ F & \text{sonst} \end{cases}$$

$$val_I(C) = \begin{cases} W & \text{falls ein } L \in C \text{ existiert mit } val_I(L) = W \\ F & \text{sonst} \end{cases}$$

für Klauseln C,
Es folgt also

$$val_I(\{\Box\}) = F,$$

$$val_I(\emptyset) = W$$

($\emptyset$ ist die leere Klauselmenge.)

Semantik

Ist $I : \Sigma \to \{W, F\}$ eine Interpretation der Atome, so hat man als zugehörige Auswertung
val_I : Mengen von Klauseln $\to \{W, F\}$:

$$val_I(M) = \begin{cases} W & \text{falls für alle } C \in M \text{ gilt: } val_I(C) = W \\ F & \text{sonst} \end{cases}$$

$$val_I(C) = \begin{cases} W & \text{falls ein } L \in C \text{ existiert mit } val_I(L) = W \\ F & \text{sonst} \end{cases}$$

für Klauseln C,
Es folgt also

$$val_I(\{\Box\}) = F,$$

$$val_I(\emptyset) = W$$

($\emptyset$ ist die leere Klauselmenge.)

Der Kalkül $R0$

Definition

Die *aussagenlogische Resolutionregel* ist die Regel

$$\frac{C_1 \cup \{P\}, C_2 \cup \{\neg P\}}{C_1 \cup C_2}$$

mit einer AL-Variablen P und Klauseln C_1, C_2
$C_1 \cup C_2$ heisst *Resolvente* von $C_1 \cup \{P\}$, $C_2 \cup \{\neg P\}$.
Der Resolutionskalkül enthält die Resolutionsregel als einzige Regel.

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{}$$

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{\{P_1\}}$$

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{\{P_1\}}$$

$$\frac{\{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}}{}$$

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{\{P_1\}}$$

$$\frac{\{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}}{\{\neg P_1\}}$$

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{\{P_1\}}$$

$$\frac{\{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}}{\{\neg P_1\}}$$

$$\frac{\{P_1\}, \{\neg P_1\}}{}$$

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{\{P_1\}}$$

$$\frac{\{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}}{\{\neg P_1\}}$$

$$\frac{\{P_1\}, \{\neg P_1\}}{\square}$$

Beispiel

Gegeben sei die Klauselmenge
$M = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$

$$\frac{\{P_1, P_2\}, \{P_1, \neg P_2\}}{\{P_1\}}$$

$$\frac{\{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}}{\{\neg P_1\}}$$

$$\frac{\{P_1\}, \{\neg P_1\}}{\Box}$$

Insgesamt:

$$M \vdash_{Res} \Box$$

Ein zweites Beispiel

Es soll gezeigt werden, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.
Dazu werden wir zeigen, dass die Negation dieser Formel

$$\neg((A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C)))$$

nicht erfüllbar ist.

Ein zweites Beispiel

Es soll gezeigt werden, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.
Dazu werden wir zeigen, dass die Negation dieser Formel

$$\neg((A \to B) \to ((B \to C) \to (A \to C)))$$

nicht erfüllbar ist.
Klauselnormalform:

$$M = \{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$$

Ein zweites Beispiel

Fortsetzung

$$M = \{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$$

Ableitung der leeren Klausel aus M:

(1)	[]	$\{\neg A, B\}$
(2)	[]	$\{\neg B, C\}$
(3)	[]	$\{A\}$
(4)	[]	$\{\neg C\}$

Ein zweites Beispiel

Fortsetzung

$$M = \{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$$

Ableitung der leeren Klausel aus M:

(1)	[]	$\{\neg A, B\}$
(2)	[]	$\{\neg B, C\}$
(3)	[]	$\{A\}$
(4)	[]	$\{\neg C\}$
(5)	$[1, 3]$	$\{B\}$

Ein zweites Beispiel

Fortsetzung

$$M = \{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$$

Ableitung der leeren Klausel aus M:

(1)	[]	$\{\neg A, B\}$
(2)	[]	$\{\neg B, C\}$
(3)	[]	$\{A\}$
(4)	[]	$\{\neg C\}$
(5)	$[1, 3]$	$\{B\}$
(6)	$[2, 5]$	$\{C\}$

Ein zweites Beispiel

Fortsetzung

$$M = \{\{\neg A, B\}, \{\neg B, C\}, \{A\}, \{\neg C\}\}$$

Ableitung der leeren Klausel aus M:

(1)	[]	$\{\neg A, B\}$
(2)	[]	$\{\neg B, C\}$
(3)	[]	$\{A\}$
(4)	[]	$\{\neg C\}$
(5)	$[1, 3]$	$\{B\}$
(6)	$[2, 5]$	$\{C\}$
(7)	$[4, 6]$	$\Box$

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \square$$

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \square$$

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Korrektheit (Beweisidee, Rest Übung):

Die Resolutionsregel erhält Erfüllbarkeit

Wenn M erfüllbar und $M \vdash_{\mathbf{R}0} A$, dann $M \cup \{A\}$ erfüllbar

Dann: Aus $M \vdash_{\mathbf{R}0} \Box$ folgt: M unerfüllbar

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

- Aus $M \nvdash_{\mathbf{R}0} \Box$ beweisen wir die Erfüllbarkeit von M.

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

- Aus $M \nvdash_{\mathbf{R}0} \Box$ beweisen wir die Erfüllbarkeit von M.
- Beliebige aber feste Reihenfolge der Atome: $P_0, \ldots, P_n, \ldots$

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

- Aus $M \nvdash_{\mathbf{R}0} \Box$ beweisen wir die Erfüllbarkeit von M.
- Beliebige aber feste Reihenfolge der Atome: $P_0, \ldots, P_n, \ldots$
- M_0 sei die Menge aller Klauseln C mit $M \vdash_{R0} C$.
  Es gilt also $M \subseteq M_0$ und $\Box \notin M_0$.

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

- Aus $M \nvdash_{\mathbf{R}0} \Box$ beweisen wir die Erfüllbarkeit von M.
- Beliebige aber feste Reihenfolge der Atome: $P_0, \ldots, P_n, \ldots$
- M_0 sei die Menge aller Klauseln C mit $M \vdash_{R0} C$.
  Es gilt also $M \subseteq M_0$ und $\Box \notin M_0$.
- Wir definieren (induktiv) eine Interpretation I, so dass:
  für alle $C \in M_0$ gilt $val_I(C) = W$.
  Insbesondere ist dann M als erfüllbar nachgewiesen.

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

- Aus $M \nvdash_{\mathbf{R}0} \Box$ beweisen wir die Erfüllbarkeit von M.
- Beliebige aber feste Reihenfolge der Atome: $P_0, \ldots, P_n, \ldots$
- M_0 sei die Menge aller Klauseln C mit $M \vdash_{R0} C$.
  Es gilt also $M \subseteq M_0$ und $\Box \notin M_0$.
- Wir definieren (induktiv) eine Interpretation I, so dass:
  für alle $C \in M_0$ gilt $val_I(C) = W$.
  Insbesondere ist dann M als erfüllbar nachgewiesen.

Korrektheit und Vollständigkeit

Theorem

Für eine Menge M von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R}0} \Box$$

Beweis der Vollständigkeit:

- Aus $M \not\vdash_{\mathbf{R}0} \Box$ beweisen wir die Erfüllbarkeit von M.
- Beliebige aber feste Reihenfolge der Atome: $P_0, \ldots, P_n, \ldots$
- M_0 sei die Menge aller Klauseln C mit $M \vdash_{R0} C$.
  Es gilt also $M \subseteq M_0$ und $\Box \notin M_0$.
- Wir definieren (induktiv) eine Interpretation I, so dass:
  für alle $C \in M_0$ gilt $val_I(C) = W$.
  Insbesondere ist dann M als erfüllbar nachgewiesen.

Rest des Beweises: Tafel/Skriptum

Notwendigkeit der Mengenschreibweise

Die Menge von Formeln

$$E = \{P_1 \vee \neg P_2, \neg P_1 \vee P_2, \neg P_1 \vee \neg P_2, P_1 \vee P_2\}$$

ist sicherlich nicht erfüllbar.

Notwendigkeit der Mengenschreibweise

Die Menge von Formeln

$$E = \{P_1 \vee \neg P_2, \neg P_1 \vee P_2, \neg P_1 \vee \neg P_2, P_1 \vee P_2\}$$

ist sicherlich nicht erfüllbar.
Es gibt die folgenden Resolutionsmöglichkeiten:

$$\frac{\neg P_1 \vee \neg P_2, P_1 \vee \neg P_2}{\neg P_2 \vee \neg P_2} \qquad \frac{\neg P_1 \vee \neg P_2, \neg P_1 \vee P_2}{\neg P_1 \vee \neg P_1}$$

$$\frac{\neg P_1 \vee \neg P_1, P_1 \vee \neg P_2}{\neg P_1 \vee \neg P_2} \qquad \frac{\neg P_2 \vee \neg P_2, \neg P_1 \vee P_2}{\neg P_1 \vee \neg P_2}$$

Auf diese Weise ist $\Box$ nicht herleitbar.

Beispiel einer Beweisaufgabe

"Pigeon hole principle"

Zu zeigen ist

$$\begin{array}{rl}
& (p1h1 \to \neg p2h1) \\
\wedge & (p1h1 \to \neg p3h1) \\
\wedge & (p2h1 \to \neg p3h1) \\
\wedge & (p1h2 \to \neg p2h2) \\
\wedge & (p1h2 \to \neg p3h2) \\
\wedge & (p2h2 \to \neg p3h2)
\end{array}
\quad \vdash \quad
\begin{array}{rl}
& (\neg p1h1 \wedge \neg p1h2) \\
\vee & (\neg p2h1 \wedge \neg p2h2) \\
\vee & (\neg p3h1 \wedge \neg p3h2)
\end{array}$$

Beispiel einer Beweisaufgabe

Klauselmenge:
Voraussetzungen plus negierte Behauptung

$$
\begin{aligned}
M = \{ \; & \\
& \{\neg p1h1, \neg p2h1\}, \quad \{\neg p1h1, \neg p3h1\}, \\
& \{\neg p2h1, \neg p3h1\}, \quad \{\neg p1h2, \neg p2h2\}, \\
& \{\neg p1h2, \neg p3h2\}, \quad \{\neg p2h2, \neg p3h2\}, \\
& \\
& \{p1h1, p1h2\}, \qquad \{p2h1, p2h2\}, \\
& \{p3h1, p3h2\} \\
& \}
\end{aligned}
$$

Beispiel einer Beweisaufgabe

Maschineller Resolutionbeweis (mit Beweiser “otter”)

```
1 [] -p1h1 v -p2h1.
2 [] -p1h1 v -p3h1.
3 [] -p2h1 v -p3h1.
4 [] -p1h2 v -p2h2.
5 [] -p1h2 v -p3h2.
6 [] -p2h2 v -p3h2.
7 [] p1h1 v p1h2.
8 [] p2h1 v p2h2.
9 [] p3h1 v p3h2.
10 [7,2] p1h2 v -p3h1.
12 [7,5] p1h1 v -p3h2.
14 [8,3] p2h2 v -p3h1.
15 [8,1] p2h2 v -p1h1.
20 [9,6] p3h1 v -p2h2.
23 [10,4] -p3h1 v -p2h2.
49 [23,20]-p2h2.
50 [23,14] -p3h1.
51 [49,15] -p1h1.
54 [50,9] p3h2.
55 [51,12] -p3h2.
56 [55,54] .
----> UNIT CONFLICT .
```

1-Resolution

unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

$$\frac{\{P\}, C_2 \cup \{\neg P\}}{C_2} \qquad \frac{\{\neg P\}, C_2 \cup \{P\}}{C_2}$$

1-Resolution
unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

$$\frac{\{P\}, C_2 \cup \{\neg P\}}{C_2} \qquad \frac{\{\neg P\}, C_2 \cup \{P\}}{C_2}$$

Ist uns bereits begegnet ...

1-Resolution

unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

$$\frac{\{P\}, C_2 \cup \{\neg P\}}{C_2} \qquad \frac{\{\neg P\}, C_2 \cup \{P\}}{C_2}$$

Ist uns bereits begegnet ...

1-Resolution

unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

$$\frac{\{P\}, C_2 \cup \{\neg P\}}{C_2} \qquad \frac{\{\neg P\}, C_2 \cup \{P\}}{C_2}$$

Ist uns bereits begegnet ...

... im DPLL-Algorithmus als “unit propagation”.

1-Resolution

unit resolution

Der 1-Resolutionskalkül ist nicht vollständig.

Die Klauselmenge

$$E = \{\{P_1, P_2\}, \{P_1, \neg P_2\}, \{\neg P_1, P_2\}, \{\neg P_1, \neg P_2\}\}$$

ist nicht erfüllbar, aber mit 1-Resolution ist aus E nichts ableitbar, also auch nicht die leere Klausel $\Box$.

Einschränkung der Resolutionsregel

Geordnete Resolution

Gegeben sei eine Aufzählung $P_0, \ldots, P_n$ aller aussagenlogischen Atome.
Die geordnete Resolutionsregel

$$\frac{C_1 \cup \{P_j\}, C_2 \cup \{\neg P_j\}}{C_1 \cup C_2}$$

ist nur anwendbar wenn für alle in C_1 oder C_2 vorkommenden Atome P_i gilt $i < j$.

Einschränkung der Resolutionsregel

Geordnete Resolution

Gegeben sei eine Aufzählung $P_0, \ldots, P_n$ aller aussagenlogischen Atome.
Die geordnete Resolutionsregel

$$\frac{C_1 \cup \{P_j\}, C_2 \cup \{\neg P_j\}}{C_1 \cup C_2}$$

ist nur anwendbar wenn für alle in C_1 oder C_2 vorkommenden Atome P_i gilt $i < j$.

Frage

Ist der geordnete Resolutionskalkül vollständig?