

# Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2018/2019

Aussagenlogik: Resolutionskalkül

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK

# Kalküle für die Aussagenlogik

## Übersicht

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

## 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.

## 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





Eine *Klausel* ist eine endliche Menge von Literalen.

Eine *Klausel* ist eine endliche Menge von Literalen.

Eine *Klausel* ist eine endliche Menge von Literalen.

$\square$  ist die *leere Klausel*.

Eine *Klausel* ist eine endliche Menge von Literalen.

$\square$  ist die *leere Klausel*.

Eine *Klausel* ist eine endliche Menge von Literalen.

$\square$  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:

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

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

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

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.

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

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.



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

$val_I : \text{Mengen von Klauseln} \rightarrow \{W, F\} :$

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

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

für Klauseln  $C$ ,

Es folgt also

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

$$val_I(\emptyset) = W$$

( $\emptyset$  ist die leere Klauselmenge.)

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

$val_I : \text{Mengen von Klauseln} \rightarrow \{W, F\} :$

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

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

für Klauseln  $C$ ,

Es folgt also

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

$$val_I(\emptyset) = W$$

( $\emptyset$  ist die leere Klauselmenge.)

## 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.

Gegeben sei die Klauselmenge

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

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

Gegeben sei die Klauselmenge

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

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

Gegeben sei die Klauselmenge

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

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

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

Gegeben sei die Klauselmenge

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

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

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

Gegeben sei die Klauselmeng

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

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

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

$$\underline{\{P_1\}, \{\neg P_1\}}$$



Gegeben sei die Klauselmenge

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

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

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

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



Gegeben sei die Klauselmenge

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

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

Insgesamt:

$$M \vdash_{Res} \square$$

# 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

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

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.

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)  $\square \quad \{\neg A, B\}$
- (2)  $\square \quad \{\neg B, C\}$
- (3)  $\square \quad \{A\}$
- (4)  $\square \quad \{\neg C\}$

# Ein zweites Beispiel

## Fortsetzung

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

Ableitung der leeren Klausel aus  $M$ :

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

# Ein zweites Beispiel

## Fortsetzung

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

Ableitung der leeren Klausel aus  $M$ :

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



## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R0}} \square$$

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R0}} \square$$

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{R0} \square$$

*Beweis der Korrektheit* (Beweisidee, Rest Übung):

Die Resolutionsregel erhält Erfüllbarkeit

Wenn  $M$  erfüllbar und  $M \vdash_{R0} A$ , dann  $M \cup \{A\}$  erfüllbar

Dann: Aus  $M \vdash_{R0} \square$  folgt:  $M$  unerfüllbar

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R0}} \square$$

*Beweis der Vollständigkeit:*

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{R0} \square$$

*Beweis der Vollständigkeit:*

- Aus  $M \not\vdash_{R0} \square$  beweisen wir die Erfüllbarkeit von  $M$ .

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{\mathbf{R0}} \Box$$

*Beweis der Vollständigkeit:*

- ▶ Aus  $M \not\vdash_{\mathbf{R0}} \Box$  beweisen wir die Erfüllbarkeit von  $M$ .
- ▶ Beliebige aber feste Reihenfolge der Atome:  $P_0, \dots, P_n, \dots$

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{R0} \square$$

*Beweis der Vollständigkeit:*

- ▶ Aus  $M \not\vdash_{R0} \square$  beweisen wir die Erfüllbarkeit von  $M$ .
- ▶ Beliebige aber feste Reihenfolge der Atome:  $P_0, \dots, P_n, \dots$
- ▶  $M_0$  sei die Menge aller Klauseln  $C$  mit  $M \vdash_{R0} C$ .  
Es gilt also  $M \subseteq M_0$  und  $\square \notin M_0$ .

## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{R0} \square$$

*Beweis der Vollständigkeit:*

- ▶ Aus  $M \not\vdash_{R0} \square$  beweisen wir die Erfüllbarkeit von  $M$ .
- ▶ Beliebige aber feste Reihenfolge der Atome:  $P_0, \dots, P_n, \dots$
- ▶  $M_0$  sei die Menge aller Klauseln  $C$  mit  $M \vdash_{R0} C$ .  
Es gilt also  $M \subseteq M_0$  und  $\square \notin M_0$ .
- ▶ 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.



## Theorem

Für eine Menge  $M$  von Klauseln gilt

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{R0} \square$$

*Beweis der Vollständigkeit:*

- ▶ Aus  $M \not\vdash_{R0} \square$  beweisen wir die Erfüllbarkeit von  $M$ .
- ▶ Beliebige aber feste Reihenfolge der Atome:  $P_0, \dots, P_n, \dots$
- ▶  $M_0$  sei die Menge aller Klauseln  $C$  mit  $M \vdash_{R0} C$ .  
Es gilt also  $M \subseteq M_0$  und  $\square \notin M_0$ .
- ▶ 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

$$M \text{ unerfüllbar} \quad \text{gdw.} \quad M \vdash_{R0} \square$$

*Beweis der Vollständigkeit:*

- ▶ Aus  $M \not\vdash_{R0} \square$  beweisen wir die Erfüllbarkeit von  $M$ .
- ▶ Beliebige aber feste Reihenfolge der Atome:  $P_0, \dots, P_n, \dots$
- ▶  $M_0$  sei die Menge aller Klauseln  $C$  mit  $M \vdash_{R0} C$ .  
Es gilt also  $M \subseteq M_0$  und  $\square \notin M_0$ .
- ▶ 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:

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

Auf diese Weise ist  $\square$  nicht herleitbar.

# Beispiel einer Beweisaufgabe

“Pigeon hole principle”

Zu zeigen ist

$$\begin{array}{l} (p1h1 \rightarrow \neg p2h1) \\ \wedge (p1h1 \rightarrow \neg p3h1) \\ \wedge (p2h1 \rightarrow \neg p3h1) \\ \wedge (p1h2 \rightarrow \neg p2h2) \\ \wedge (p1h2 \rightarrow \neg p3h2) \\ \wedge (p2h2 \rightarrow \neg p3h2) \end{array} \vdash \begin{array}{l} (\neg p1h1 \wedge \neg p1h2) \\ \vee (\neg p2h1 \wedge \neg p2h2) \\ \vee (\neg p3h1 \wedge \neg p3h2) \end{array}$$

## Klauselmenge: Voraussetzungen plus negierte Behauptung

$M =$

$$\left\{ \begin{array}{ll} \{\neg p1h1, \neg p2h1\}, & \{\neg p1h1, \neg p3h1\}, \\ \{\neg p2h1, \neg p3h1\}, & \{\neg p1h2, \neg p2h2\}, \\ \{\neg p1h2, \neg p3h2\}, & \{\neg p2h2, \neg p3h2\}, \\ \\ \{p1h1, p1h2\}, & \{p2h1, p2h2\}, \\ \{p3h1, p3h2\} & \end{array} \right\}$$

## Maschineller Resolutionbeweis (mit Beweiser "otter")

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

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

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

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



# 1-Resolution

unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

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

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

Ist uns bereits begegnet ...

# 1-Resolution

unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

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

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

Ist uns bereits begegnet ...

# 1-Resolution

unit resolution

Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

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

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

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  $\square$ .

## Geordnete Resolution

Gegeben sei eine Aufzählung  $P_0, \dots, P_n$  aller aussagenlogischen Atome.

Die geordnete Resolutionsregel

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

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

## Geordnete Resolution

Gegeben sei eine Aufzählung  $P_0, \dots, P_n$  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?