

Logik für Informatiker

2. Aussagenlogik

Teil 6

12.05.2016

Viorica Sofronie-Stokkermans

Universität Koblenz-Landau

e-mail: sofronie@uni-koblenz.de

Bis jetzt

- **Syntax** (Formeln)
- **Semantik**
 - Wertebelegungen/Valuationen/Modelle
 - Auswertung von Formeln / Wahrheitstabellen
 - Gültigkeit und Erfüllbarkeit
 - Folgerung, Äquivalenz
- **Kalküle**
 - Wahrheitstafelmethode
 - Äquivalenzumformung
 - nicht sehr effizient.

Unser Ziel

Kalkül(e) zur systematischen Überprüfung von Erfüllbarkeit
(für Formeln und/oder Formelmengen)

Bis jetzt

- **Normalformen**

 - Atome, Literale, Klauseln

 - Konjunktive und Disjunktive Normalform

 - Ablezen von DNF und KNF aus Wahrheitstafeln

 - Umformen in KNF/DNF

 - Mengenschreibweise

 - Subsumption

- **SAT-Problem** (Erfüllbarkeitsproblem)

 - SAT

 - Erfüllbarkeitsproblem für DNF Formeln

 - k -SAT; 3-SAT vs. SAT

 - Horn Formeln

- **Der aussagenlogische Resolutionskalkül**

Resolutionskalkül

Definition: **Resolutionsregel** (einzige Regel des Kalküls)

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

wobei

- P eine aussagenlogische Variable
- C_1, C_2 Klauseln (können leer sein)

Definition:

$C_1 \cup C_2$ heißt **Resolvente** von $C_1 \cup \{P\}, C_2 \cup \{\neg P\}$

Notwendigkeit der Mengenschreibweise

Die Menge

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

ist unerfüllbar.

Notwendigkeit der Mengenschreibweise

Die Menge

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

ist unerfüllbar.

Klauselmenge:

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

Resolution:

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

Notwendigkeit der Mengenschreibweise

Die Menge

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

ist unerfüllbar.

Notwendigkeit der Mengenschreibweise

Die Menge

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

ist unerfüllbar.

Es gibt folgende Resolutionsmöglichkeiten (ohne Mengenschreibweise)

$$\begin{array}{cccc} \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee P_2}{\neg P_2 \vee P_2} & \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee P_2}{\neg P_1 \vee P_1} & \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee \neg P_2}{\neg P_2 \vee \neg P_2} & \frac{P_1 \vee \neg P_2 \quad P_1 \vee P_2}{P_1 \vee P_1} \\ \frac{\neg P_1 \vee P_2 \quad \neg P_1 \vee \neg P_2}{\neg P_1 \vee \neg P_1} & \frac{\neg P_1 \vee P_2 \quad P_1 \vee P_2}{P_2 \vee P_2} & \frac{\neg P_1 \vee \neg P_2 \quad P_1 \vee P_2}{\neg P_1 \vee P_1} & \frac{\neg P_1 \vee \neg P_2 \quad P_1 \vee P_2}{\neg P_2 \vee P_2} \end{array}$$

Notwendigkeit der Mengenschreibweise

Die Menge

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

ist unerfüllbar.

Es gibt folgende Resolutionsmöglichkeiten (ohne Mengenschreibweise)

$$\begin{array}{cccc} \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee P_2}{\neg P_2 \vee P_2} & \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee P_2}{\neg P_1 \vee P_1} & \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee \neg P_2}{\neg P_2 \vee \neg P_2} & \frac{P_1 \vee \neg P_2 \quad P_1 \vee P_2}{P_1 \vee P_1} \\ \frac{\neg P_1 \vee P_2 \quad \neg P_1 \vee \neg P_2}{\neg P_1 \vee \neg P_1} & \frac{\neg P_1 \vee P_2 \quad P_1 \vee P_2}{P_2 \vee P_2} & \frac{\neg P_1 \vee \neg P_2 \quad P_1 \vee P_2}{\neg P_1 \vee P_1} & \frac{\neg P_1 \vee \neg P_2 \quad P_1 \vee P_2}{\neg P_2 \vee P_2} \end{array}$$

Auf diese Weise ist \perp nicht herleitbar

Ohne Mengenschreibweise

Resolutionsregel:

$$\frac{C_1 \vee P \quad \neg P \vee C_2}{C_1 \vee C_2}$$

Faktorisieren:

$$\frac{C \vee L \vee L}{C \vee L}$$

Resolution mit Faktorisierung

Die Menge

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

ist unerfüllbar.

Es gibt folgende Resolutionsmöglichkeiten (mit Faktorisieren)

$$\begin{array}{cccc}
 \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee P_2}{\neg P_2 \vee P_2} & \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee P_2}{\neg P_1 \vee P_1} & \frac{P_1 \vee \neg P_2 \quad \neg P_1 \vee \neg P_2}{\neg P_2 \vee \neg P_2} & \frac{P_1 \vee \neg P_2 \quad P_1 \vee P_2}{P_1 \vee P_1} \\
 \frac{\neg P_1 \vee P_2 \quad \neg P_1 \vee \neg P_2}{\neg P_1 \vee \neg P_1} & \frac{\neg P_1 \vee P_2 \quad P_1 \vee P_2}{P_2 \vee P_2} & \frac{\neg P_1 \vee \neg P_2 \quad P_1 \vee P_2}{\neg P_1 \vee P_1} & \frac{\neg P_1 \vee \neg P_2 \quad P_1 \vee P_2}{\neg P_2 \vee P_2} \\
 & \frac{P_1 \vee P_1}{P_1} & \frac{\neg P_1 \vee \neg P_1}{\neg P_1} & \frac{P_2 \vee P_2}{P_2} & \frac{\neg P_2 \vee \neg P_2}{\neg P_2} \\
 & & \frac{P_1 \quad \neg P_1}{\perp} & &
 \end{array}$$

Resolution: Beispiel

Gegeben die Klauselmenge:

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

Resolution:

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

Insgesamt: $M \vdash_{\text{Res}} \perp$

also: M unerfüllbar

Resolution

Ziele:

- Formalisieren, was $M \vdash_{\text{Res}} \perp$ bedeutet
- Zeigen, dass $M \vdash_{\text{Res}} \perp$ gdw. M unerfüllbar.

Resolution

Sei F eine Klauselmengge und

$$\text{Res}(F) = F \cup \{R \mid R \text{ ist eine Resolvente zweier Klauseln aus } F\}$$

Resolution

Sei F eine Klauselmenge und

$$\text{Res}(F) = F \cup \{R \mid R \text{ ist eine Resolvente zweier Klauseln aus } F\}$$

$$\text{Res}^0(F) = F$$

$$\text{Res}^{n+1}(F) = \text{Res}(\text{Res}^n(F))$$

$$\text{Res}^*(F) = \bigcup_{n \in \mathbb{N}} \text{Res}^n(F)$$

(bezeichnet die Vereinigung der Resolventen aus aller möglichen Resolutionsschritte auf F)

Resolution

Sei F eine Klauselmenge und

$$\text{Res}(F) = F \cup \{R \mid R \text{ ist eine Resolvente zweier Klauseln aus } F\}$$

$$\text{Res}^0(F) = F$$

$$\text{Res}^{n+1}(F) = \text{Res}(\text{Res}^n(F))$$

$$\text{Res}^*(F) = \bigcup_{n \in \mathbb{N}} \text{Res}^n(F)$$

(bezeichnet die Vereinigung der Resolventen aus aller möglichen Resolutionsschritte auf F)

Notation: Falls $C \in \text{Res}^*(F)$, so schreiben wir $F \vdash_{\text{Res}} C$.

Resolution

Sei F eine Klauselmenge und

$$\text{Res}(F) = F \cup \{R \mid R \text{ ist eine Resolvente zweier Klauseln aus } F\}$$

$$\text{Res}^0(F) = F$$

$$\text{Res}^{n+1}(F) = \text{Res}(\text{Res}^n(F))$$

$$\text{Res}^*(F) = \bigcup_{n \in \mathbb{N}} \text{Res}^n(F)$$

(bezeichnet die Vereinigung der Resolventen aus aller möglichen Resolutionsschritte auf F)

Notation: Falls $C \in \text{Res}^*(F)$, so schreiben wir $F \vdash_{\text{Res}} C$.

Definition: Beweis für C (aus F): C_1, \dots, C_n , wobei:

$C_n = C$ und für alle $1 \leq i \leq n$: ($C_i \in F$ oder C_i Resolvente für $\frac{C_{j_1} C_{j_2}}{C_i}$ mit $j_1, j_2 < i$).

Resolution: Weiteres Beispiel

Klauselnormalform:

$$M = \{\{\neg P, Q\}, \{\neg Q, R\}, \{P\}, \{\neg R\}\}$$

- (1) $\{\neg P, Q\}$ gegeben
- (2) $\{\neg Q, R\}$ gegeben
- (3) $\{P\}$ gegeben
- (4) $\{\neg R\}$ gegeben
- (5) $\{Q\}$ aus (1) und (3)
- (6) $\{R\}$ aus (2) und (5)

Beweis für $\{R\}$ aus M

Resolution: Weiteres Beispiel

Klauselnormalform:

$$M = \{\{\neg P, Q\}, \{\neg Q, R\}, \{P\}, \{\neg R\}\}$$

- (1) $\{\neg P, Q\}$ gegeben
- (2) $\{\neg Q, R\}$ gegeben
- (3) $\{P\}$ gegeben
- (4) $\{\neg R\}$ gegeben
- (5) $\{Q\}$ aus (1) und (3)
- (6) $\{R\}$ aus (2) und (5)
- (7) \perp aus (4) und (6)

Beweis für \perp aus M (Widerspruch)

Resolution: Korrektheit und Vollständigkeit

Theorem (Korrektheit)

Für eine Menge M von Klauseln gilt: Falls $M \vdash_{\text{Res}} \perp$, so M unerfüllbar.

Falls aus M die leere Klausel durch Resolution herleitbar ist, ist M unerfüllbar (es gibt keine Wertebelegung \mathcal{A} in der alle Klauseln in M wahr sind).

Äquivalent:

Falls M erfüllbar ist, ist die leere Klausel durch Resolution nicht herleitbar.

Theorem (Vollständigkeit)

Für eine Menge M von Klauseln gilt: Falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Falls M unerfüllbar ist (d.h. es gibt keine Wertebelegung \mathcal{A} in der alle Klauseln in M wahr sind), ist die leere Klausel aus M durch Resolution herleitbar.

Äquivalent:

Falls aus M die leere Klausel durch Resolution nicht herleitbar ist, ist M erfüllbar.

Resolution: Korrektheit

Theorem (Korrektheit)

Für eine Menge M von Klauseln gilt: Falls $M \vdash_{\text{Res}} \perp$, so M unerfüllbar.

Resolution: Korrektheit

Theorem (Korrektheit)

Für eine Menge M von Klauseln gilt: Falls $M \vdash_{\text{Res}} \perp$, so M unerfüllbar.

Beweis

- (1) Wir zeigen, dass falls $C \in \text{Res}^*(M)$, so $M \equiv M \cup \{C\}$.
(Theorem auf Seite 25). (NB: $M \cup \{C\}$: Notation für $M \wedge C$.)
- (2) Es folgt, dass falls $M \vdash_{\text{Res}} \perp$, so $\perp \in \text{Res}^*(M)$, d.h. $M \equiv M \cup \{\perp\}$.
- (3) Aber $M \cup \{\perp\}$ ist unerfüllbar, deshalb ist auch M unerfüllbar.

Resolution: Korrektheit

Theorem (Korrektheit)

Für eine Menge M von Klauseln gilt: Falls $M \vdash_{\text{Res}} \perp$, so M unerfüllbar.

Beweis

- (1) Wir zeigen, dass falls $C \in \text{Res}^*(M)$, so $M \equiv M \cup \{C\}$.
(Theorem auf Seite 25). (NB: $M \cup \{C\}$ Notation für $M \wedge C$.)
- (2) Es folgt, dass falls $M \vdash_{\text{Res}} \perp$, so $\perp \in \text{Res}^*(M)$, d.h. $M \equiv M \cup \{\perp\}$.
- (3) Aber $M \cup \{\perp\}$ ist unerfüllbar, deshalb ist auch M unerfüllbar.

Erklärung 1: Falls $M = \{C_1, \dots, C_n\}$ so $M \cup \{\perp\}$ ist eine Notation für $C_1 \wedge \dots \wedge C_n \wedge \perp$. Aber $C_1 \wedge \dots \wedge C_n \wedge \perp \equiv \perp$, so ist $C_1 \wedge \dots \wedge C_n \wedge \perp$ unerfüllbar (also auch $M \cup \{\perp\}$). Da $M \equiv M \cup \{\perp\}$, ist auch M unerfüllbar.

Erklärung 2: Es gibt keine Wertebelegung \mathcal{A} die alle Klauseln in $M \cup \{\perp\}$ wahr macht (d.h. so dass: $\mathcal{A}(D) = 1$ für alle Klauseln D in M und $\mathcal{A}(\perp) = 1$).

Resolution: Korrektheit

(1) Wir zeigen, dass falls $C \in \text{Res}^*(M)$, so $M \equiv M \cup \{C\}$.

Lemma: $C_1 \vee P, C_2 \vee \neg P \models C_1 \vee C_2$

Beweis:

Sei \mathcal{A} Interpretation mit $\mathcal{A}(C_1 \vee P) = 1$ und $\mathcal{A}(C_2 \vee \neg P) = 1$.

Zu zeigen: $\mathcal{A}(C_1 \vee C_2) = 1$.

Fall 1: $\mathcal{A}(C_1) = 1$. Dann $\mathcal{A}(C_1 \vee C_2) = 1$.

Fall 2: $\mathcal{A}(C_1) = 0$. Dann $\mathcal{A}(P) = 1$.

Da $\mathcal{A}(C_2 \vee \neg P) = 1$, so $\mathcal{A}(C_2) = 1$, d.h. $\mathcal{A}(C_1 \vee C_2) = 1$.

Resolution: Korrektheit

Theorem: Falls $C \in \text{Res}^*(F)$, so $F \equiv F \cup \{C\}$.

Beweis: Annahme: $C \in \text{Res}^n(F)$. Zu zeigen: $F \equiv F \wedge C$, i.e.:

Für alle $\mathcal{A} : \Pi \rightarrow \{0, 1\}$ gilt: $\mathcal{A}(F) = 1$ gdw. ($\mathcal{A}(F) = 1$ und $\mathcal{A}(C) = 1$).

Resolution: Korrektheit

Theorem: Falls $C \in \text{Res}^*(F)$, so $F \equiv F \cup \{C\}$.

Beweis: Annahme: $C \in \text{Res}^n(F)$. Zu zeigen: $F \equiv F \wedge C$, i.e.:

Für alle $\mathcal{A} : \Pi \rightarrow \{0, 1\}$ gilt: $\mathcal{A}(F) = 1$ gdw. ($\mathcal{A}(F) = 1$ und $\mathcal{A}(C) = 1$).

- Sei $\mathcal{A} : \Pi \rightarrow \{0, 1\}$ mit $\mathcal{A}(F) = 1$ (d.h. $\mathcal{A}(C') = 1$ für jede Klausel $C' \in F$).

Zu zeigen: Für alle $m \in \mathbb{N}$ gilt $p(m)$: Falls $D \in \text{Res}^m(F)$, so $\mathcal{A}(D) = 1$.

Beweis durch Induktion:

IB: $m = 0$: Sei $D \in \text{Res}^0(F) = F$. Dann $\mathcal{A}(D) = 1$.

IV: Annahme: $p(m)$ is wahr. **IS:** Zu zeigen: $p(m + 1)$ wahr.

Sei $D \in \text{Res}^{m+1}(F)$. **Fall 1:** $D \in \text{Res}^m(F)$. Nach IV, $\mathcal{A}(D) = 1$.

Fall 2: $D = C_1 \vee C_2$ Resolvente von $C_1 \vee P, C_2 \vee \neg P \in \text{Res}^m(F)$. Nach IV:

$\mathcal{A}(C_1 \vee P) = \mathcal{A}(C_2 \vee \neg P) = 1$. Da $C_1 \vee P, C_2 \vee \neg P \models C_1 \vee C_2$ folgt $\mathcal{A}(D) = 1$.

Dann $\mathcal{A}(C) = 1$, so ($\mathcal{A}(F) = 1$ und $\mathcal{A}(C) = 1$), d.h. $\mathcal{A}(F \wedge C) = 1$.

- Sei $\mathcal{A} : \Pi \rightarrow \{0, 1\}$ mit $\mathcal{A}(F \wedge C) = 1$.

Dann $\mathcal{A}(F) = 1$ und $\mathcal{A}(C) = 1$, so $\mathcal{A}(F) = 1$.

Resolution: Vollständigkeit

Theorem.

Für jede endliche Menge M von Klauseln gilt:
falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Resolution: Vollständigkeit

Theorem.

Für jede endliche Menge M von Klauseln gilt:
falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Beweis: Induktion:

$p(n)$: Sei M Menge von Klauseln mit n Aussagenvariablen.
Falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$

Resolution: Vollständigkeit

Theorem.

Für jede endliche Menge M von Klauseln gilt:
falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Beweis: Induktion:

$p(n)$: Sei M Menge von Klauseln mit n Aussagenvariablen.
Falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$

Induktionsbasis: $n = 0$.

Dann $M = \{\perp\}$, d.h. $M \vdash_{\text{Res}} \perp$

Resolution: Vollständigkeit

Theorem.

Für jede endliche Menge M von Klauseln gilt:
falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Beweis: Induktion:

$p(n)$: Sei M Menge von Klauseln mit n Aussagenvariablen.

Falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$

Induktionsbasis: $n = 0$. Dann $M = \{\perp\}$, d.h. $M \vdash_{\text{Res}} \perp$

Induktionsvoraussetzung: $p(n)$ gilt.

Induktionsschritt: Beweise, dass $p(n + 1)$ gilt.

Sei M Menge von Klauseln mit Aussagenvariablen $\{P_1, \dots, P_n, P_{n+1}\}$.

M_0 sei aus M entstanden durch Ersetzung von P_{n+1} durch \perp

M_1 sei aus M entstanden durch Ersetzung von P_{n+1} durch \top

Resolution: Vollständigkeit

M_0 sei aus M entstanden durch Ersetzung von P_{n+1} durch \perp :

- P_{n+1} wird aus allen Klauseln gelöscht,
- Klauseln, die $\neg P_{n+1}$ enthalten werden ebenfalls gelöscht

M_1 sei aus M entstanden durch Ersetzung von P_{n+1} durch \top :

- $\neg P_{n+1}$ wird aus allen Klauseln gelöscht,
- Klauseln, die P_{n+1} enthalten werden ebenfalls gelöscht

Fakten:

- M_0, M_1 enthalten nur Aussagenvariablen $\{P_1, \dots, P_n\}$
- M_0, M_1 unerfüllbar

Resolution: Vollständigkeit

M_0 sei aus M entstanden durch Ersetzung von P_{n+1} durch \perp :

- P_{n+1} wird aus allen Klauseln gelöscht,
- Klauseln, die $\neg P_{n+1}$ enthalten werden ebenfalls gelöscht

M_1 sei aus M entstanden durch Ersetzung von P_{n+1} durch \top :

- $\neg P_{n+1}$ wird aus allen Klauseln gelöscht,
- Klauseln, die P_{n+1} enthalten werden ebenfalls gelöscht

Fakten:

- M_0, M_1 enthalten nur Aussagenvariablen $\{P_1, \dots, P_n\}$
- M_0, M_1 unerfüllbar

Induktionsvoraussetzung:

$M_0 \vdash_{\text{Res}} \perp$, i.e. es gibt C_1, C_2, \dots, C_m Beweis (aus M_0) für \perp

$M_1 \vdash_{\text{Res}} \perp$, i.e. es gibt D_1, D_2, \dots, D_k Beweis (aus M_1) für \perp

Resolution: Vollständigkeit

M_0 sei aus M entstanden durch Ersetzung von P_{n+1} durch \perp :

- P_{n+1} wird aus allen Klauseln gelöscht,
- Klauseln, die $\neg P_{n+1}$ enthalten werden ebenfalls gelöscht

M_1 sei aus M entstanden durch Ersetzung von P_{n+1} durch \top :

- $\neg P_{n+1}$ wird aus allen Klauseln gelöscht,
- Klauseln, die P_{n+1} enthalten werden ebenfalls gelöscht

Fakten:

- M_0, M_1 enthalten nur Aussagenvariablen $\{P_1, \dots, P_n\}$
- M_0, M_1 unerfüllbar

Induktionsvoraussetzung:

$M_0 \vdash_{\text{Res}} \perp$, i.e. es gibt C_1, C_2, \dots, C_m Beweis (aus M_0) für \perp

P_{n+1} zurück: C'_1, C'_2, \dots, C'_m Beweis (aus M) für \perp oder P_{n+1}

$M_1 \vdash_{\text{Res}} \perp$, i.e. es gibt D_1, D_2, \dots, D_k Beweis (aus M_1) für \perp

$\neg P_{n+1}$ zurück: D'_1, D'_2, \dots, D'_k Beweis (aus M) für \perp oder $\neg P_{n+1}$

Resolution: Vollständigkeit

M_0 sei aus M entstanden durch Ersetzung von P_{n+1} durch \perp :

- P_{n+1} wird aus allen Klauseln gelöscht,
- Klauseln, die $\neg P_{n+1}$ enthalten werden ebenfalls gelöscht

M_1 sei aus M entstanden durch Ersetzung von P_{n+1} durch \top :

- $\neg P_{n+1}$ wird aus allen Klauseln gelöscht,
- Klauseln, die P_{n+1} enthalten werden ebenfalls gelöscht

Fakten:

- M_0, M_1 enthalten nur Aussagenvariablen $\{P_1, \dots, P_n\}$
- M_0, M_1 unerfüllbar

Induktionsvoraussetzung:

$M_0 \vdash_{\text{Res}} \perp$, i.e. es gibt C_1, C_2, \dots, C_m Beweis (aus M_0) für \perp

P_{n+1} zurück: C'_1, C'_2, \dots, C'_m Beweis (aus M) für \perp oder P_{n+1}

$M_1 \vdash_{\text{Res}} \perp$, i.e. es gibt D_1, D_2, \dots, D_k Beweis (aus M_1) für \perp

$\neg P_{n+1}$ zurück: D'_1, D'_2, \dots, D'_k Beweis (aus M) für \perp oder $\neg P_{n+1}$

$\Rightarrow M \vdash_{\text{Res}} \perp$

Resolution: Vollständigkeit

Theorem.

Für jede **endliche** Menge M von Klauseln gilt:
falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Es gilt auch:

Theorem.

Für jede Menge M von Klauseln gilt:
falls M unerfüllbar, so $M \vdash_{\text{Res}} \perp$.

Terminierung

Theorem.

Aussagenlogische Resolution (für Klauselmengen in Mengennotation) terminiert, für jede endliche Menge von Klauseln.

Terminierung

Theorem.

Aussagenlogische Resolution (für Klauselmengen in Mengennotation) terminiert, für jede endliche Menge von Klauseln.

Beweis: Es gibt nicht mehr als 2^{2n} Klauseln (in Mengennotation) mit n Aussagenvariablen.

↳ nicht mehr als $(2^{2n})^2$ mögliche Anwendungen der Resolutionsregel.

2-SAT

Theorem

Erfüllbarkeit für Formeln in 2-KNF (2SAT) ist polynomiell entscheidbar

Beweis (Krom, 1967)

Fall 1: Für jede Aussagenvariable P , entweder enthalten alle Klauseln P oder $\neg P$: erfüllbar.

Fall 2: Es gibt Klauseln $C_1 = L_1 \vee P$, $C_2 = L_2 \vee \neg P$

Resolutionschritt; Resolvente $L_1 \vee L_2$ (Mengennotation)

Fakt: Resolventen sind immer auch in 2-KNF.

Wenn F n Aussagenvariablen enthält, gibt es $2n$ mögliche Literale, und $\leq 4n^2$ nicht-leere verschiedene 2-KNF Klauseln.

F ist erfüllbar gdw. $\perp \notin \text{Res}^*(F)$

Wenn wir $\text{Res}^*(F)$ berechnen: nicht mehr als $(4n^2)^2$ Resolutionschritte notwendig.

\mapsto Erfüllbarkeit von F ist polynomiell entscheidbar.

1-Resolution

Die **1-Resolution** (unit resolution) benutzt dieselbe Notation wie im Resolutionskalkül. Die 1-Resolutionsregel ist ein Spezialfall der allgemeinen Resolutionsregel:

$$\frac{\{P\} \quad \{\neg P\} \cup C}{C} \qquad \frac{\{\neg P\} \quad \{P\} \cup C}{C}$$

Der 1-Resolutionskalkül ist nicht vollständig.

Die Klauselmenge

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

ist nicht erfüllbar, aber mit 1-Resolution ist aus M nichts ableitbar, also auch nicht \perp .

Unser Ziel

Kalkül(e) zur systematischen Überprüfung von Erfüllbarkeit
(für Formeln und/oder Formelmengen)

1. Formeln in KNF (Mengen von Klauseln)

Resolution

bis jetzt

2. Formelmengen

Semantische Tableaux

nächste Vorlesung