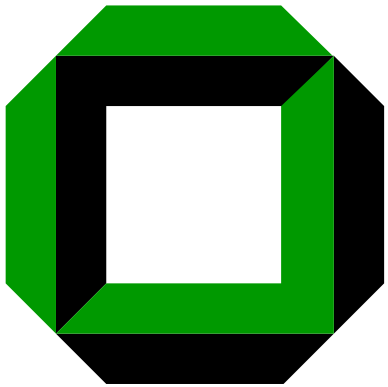
Formale Systeme

Prof. Dr. Bernhard Beckert

Fakultät für Informatik
Universität Karlsruhe (TH)



Winter 2008/2009

Das SAT Problem

oder Erfüllbarkeitsproblem

SAT

Instanz: Eine aussagenlogische Formel $F \in For0$

Frage: Ist F erfüllbar?

Gibt es eine Interpretation I mit $val_I(F) = \mathbf{1}$?

Das SAT Problem

oder Erfüllbarkeitsproblem

SAT

Instanz: Eine aussagenlogische Formel $F \in For0$

Frage: Ist F erfüllbar?

Gibt es eine Interpretation I mit $val_I(F) = \mathbf{1}$?

SAT ist ein *NP-vollständiges* Problem:

Das SAT Problem

oder Erfüllbarkeitsproblem

SAT

Instanz: Eine aussagenlogische Formel $F \in For0$

Frage: Ist F erfüllbar?
Gibt es eine Interpretation I mit $val_I(F) = \mathbf{1}$?

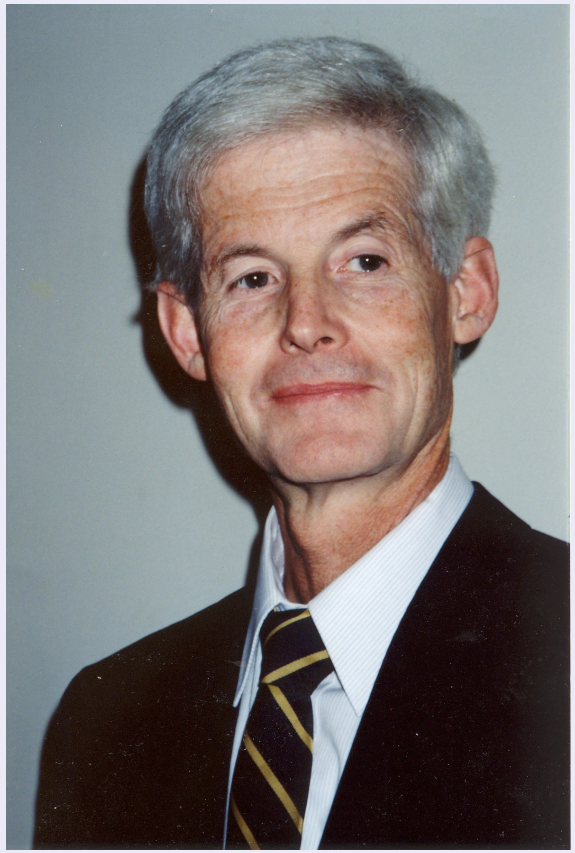
SAT ist ein *NP-vollständiges* Problem:

Gäbe es einen (deterministischen) polynomialen Entscheidungsalgorithmus für die Erfüllbarkeit, dann wäre $NP = P$, d. h. jedes nichtdeterministisch-polynomiale Entscheidungsproblem auch deterministisch-polynomial.

Satz von Cook

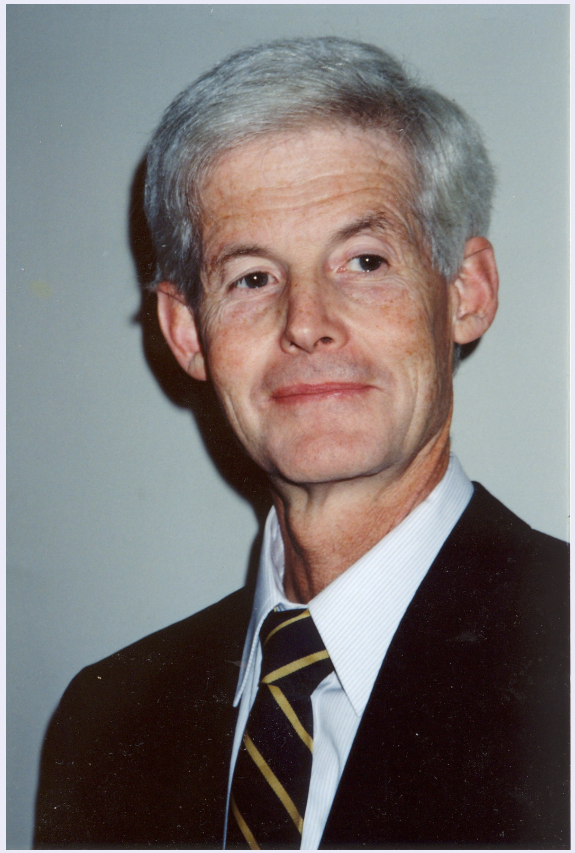
Stephen A. Cook $\star 1939$

- Informatik-Professor and der Universität Toronto



Satz von Cook

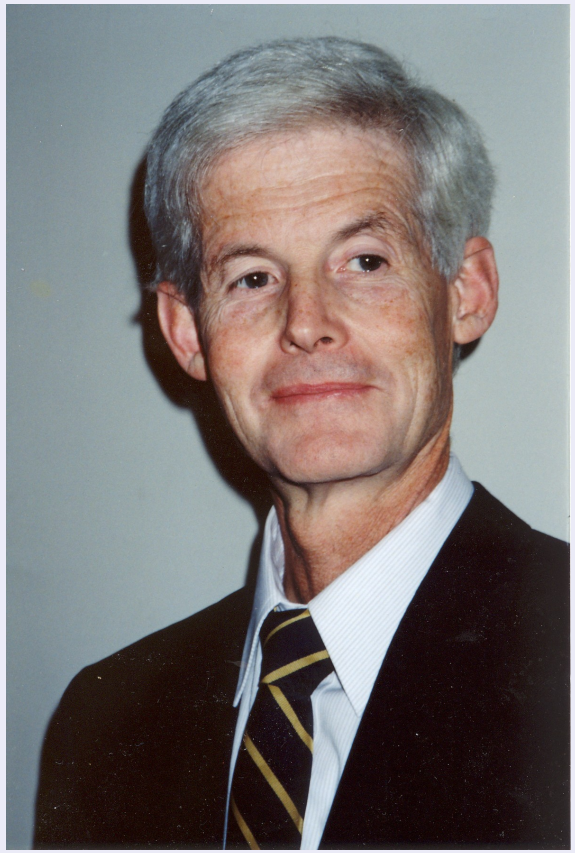
Stephen A. Cook $\star 1939$



- Informatik-Professor and der Universität Toronto
- 1971: „Das Erfüllbarkeitsproblem der Aussagenlogik (SAT) ist NP-vollständig“

Satz von Cook

Stephen A. Cook $\star$ *1939*



- Informatik-Professor and der Universität Toronto
- 1971: „Das Erfüllbarkeitsproblem der Aussagenlogik (SAT) ist NP-vollständig“
- Turing-Preisträger

Teilklassen

Das Erfüllbarkeitsproblem für Formeln A

- in KNF ist NP-vollständig

Teilklassen

Das Erfüllbarkeitsproblem für Formeln A

- in KNF ist NP-vollständig
- in 3-KNF ist NP-vollständig

Teilklassen

Das Erfüllbarkeitsproblem für Formeln A

- in KNF ist NP-vollständig
- in 3-KNF ist NP-vollständig
- in 2-KNF ist polynomial entscheidbar

Teilklassen

Das Erfüllbarkeitsproblem für Formeln A

- in KNF ist NP-vollständig
- in 3-KNF ist NP-vollständig
- in 2-KNF ist polynomial entscheidbar
- in DNF ist polynomiell entscheidbar ($O(n \log n)$ oder besser)

Teilklassen

Das Erfüllbarkeitsproblem für Formeln A

- in KNF ist NP-vollständig
- in 3-KNF ist NP-vollständig
- in 2-KNF ist polynomial entscheidbar
- in DNF ist polynomiell entscheidbar ($O(n \log n)$ oder besser)

- k-KNF Formeln sind Konjunktionen von Disjunktionen mit höchstens k Literalen.

Teilklassen

Das Erfüllbarkeitsproblem für Formeln A

- in KNF ist NP-vollständig
- in 3-KNF ist NP-vollständig
- in 2-KNF ist polynomial entscheidbar
- in DNF ist polynomiell entscheidbar ($O(n \log n)$ oder besser)

- k-KNF Formeln sind Konjunktionen von Disjunktionen mit höchstens k Literalen.
- 2-KNF Formeln heißen auch Krom Formeln.

Horn Formeln

Definition

Eine *Horn-Formel* ist eine aussagenlogische Formel in KNF, in der jede Disjunktion höchstens ein positives Literale enthält. Eine solche Disjunktion heißt eine *Horn-Klausel*.

Horn Formeln

Definition

Eine *Horn-Formel* ist eine aussagenlogische Formel in KNF, in der jede Disjunktion höchstens ein positives Literale enthält. Eine solche Disjunktion heißt eine *Horn-Klausel*.

Alternative Schreibweise:

$\neg B_1 \vee \ldots \vee \neg B_m \vee A$	$B_1 \wedge \ldots \wedge B_m \rightarrow A$
$\neg B_1 \vee \ldots \vee \neg B_m$	$B_1 \wedge \ldots \wedge B_m \rightarrow \mathbf{0}$
A	A

Horn Formeln

Definition

Eine *Horn-Formel* ist eine aussagenlogische Formel in KNF, in der jede Disjunktion höchstens ein positives Literale enthält. Eine solche Disjunktion heißt eine *Horn-Klausel*.

Alternative Schreibweise:

$\neg B_1 \vee \ldots \vee \neg B_m \vee A$	$B_1 \wedge \ldots \wedge B_m \rightarrow A$
$\neg B_1 \vee \ldots \vee \neg B_m$	$B_1 \wedge \ldots \wedge B_m \rightarrow \mathbf{0}$
A	A

Dabei heißt $B_1 \wedge \ldots \wedge B_m$ der *Rumpf* und A der *Kopf* der Horn-Klausel $B_1 \wedge \ldots \wedge B_m \rightarrow A$.

Beispiel einer Horn Formel

$$
\begin{array}{ll}
 & \neg P \\
\wedge & (Q \vee \neg R \vee \neg S) \\
\wedge & (\neg Q \vee \neg S) \\
\wedge & R \wedge S \wedge (\neg Q \vee P)
\end{array}
$$

Alternative Schreibweise

$$
\begin{array}{ll}
 & (P \rightarrow \mathbf{0}) \\
\wedge & (R \wedge S \rightarrow Q) \\
\wedge & (Q \wedge S \rightarrow \mathbf{0}) \\
\wedge & R \wedge S \wedge (Q \rightarrow P)
\end{array}
$$

Erfüllbarkeitsproblem für Horn Formeln

Theorem

Für Horn-Formeln ist die Erfüllbarkeit in quadratischer Zeit entscheidbar.

Erfüllbarkeitstest

Sei $C = D_1 \wedge \ldots \wedge D_m$ eine Hornformel.
Ein Atom in C *markieren*, bedeutet, es an allen Stellen seines Auftretens in C zu markieren.

- Schritt 0:
  Markiere alle Fakten. Wenn keine vorhanden sind: gib aus „erfüllbar“ und halte an.

Erfüllbarkeitstest

Sei $C = D_1 \wedge \ldots \wedge D_m$ eine Hornformel.
Ein Atom in C *markieren*, bedeutet, es an allen Stellen seines Auftretens in C zu markieren.

- Schritt 0:
  Markiere alle Fakten. Wenn keine vorhanden sind: gib aus „erfüllbar“ und halte an.
- Schritt 1:
  Suche nach einem $D_i = R_i \rightarrow K_i$ in C, so daß alle Atome im Rumpf markiert sind aber K_i noch nicht. Falls keines existiert, gebe aus „erfüllbar“ und halte an.
  Andernfalls sei $R_j \rightarrow K_j$ das erste solche D_i.

Erfüllbarkeitstest

Sei $C = D_1 \wedge \ldots \wedge D_m$ eine Hornformel.
Ein Atom in C *markieren*, bedeutet, es an allen Stellen seines Auftretens in C zu markieren.

- Schritt 0:
  Markiere alle Fakten. Wenn keine vorhanden sind: gib aus „erfüllbar“ und halte an.
- Schritt 1:
  Suche nach einem $D_i = R_i \rightarrow K_i$ in C, so daß alle Atome im Rumpf markiert sind aber K_i noch nicht. Falls keines existiert, gebe aus „erfüllbar“ und halte an.
  Andernfalls sei $R_j \rightarrow K_j$ das erste solche D_i.
  - falls $K_j \neq \mathbf{0}$: markiere K_j überall in C und wiederhole Schritt 1.

Erfüllbarkeitstest

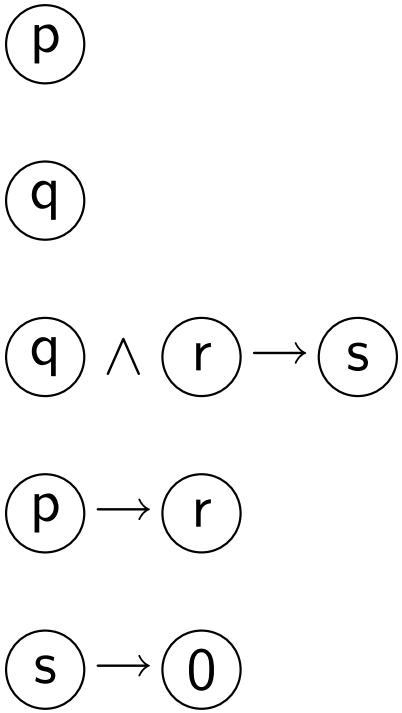
Sei $C = D_1 \wedge \ldots \wedge D_m$ eine Hornformel.
Ein Atom in C *markieren*, bedeutet, es an allen Stellen seines Auftretens in C zu markieren.

- Schritt 0:
  Markiere alle Fakten. Wenn keine vorhanden sind: gib aus „erfüllbar“ und halte an.
- Schritt 1:
  Suche nach einem $D_i = R_i \rightarrow K_i$ in C, so daß alle Atome im Rumpf markiert sind aber K_i noch nicht. Falls keines existiert, gebe aus „erfüllbar“ und halte an.

  Andernfalls sei $R_j \rightarrow K_j$ das erste solche D_i.
  - falls $K_j \neq \mathbf{0}$: markiere K_j überall in C und wiederhole Schritt 1.
  - falls $K_j = \mathbf{0}$: gebe aus „unerfüllbar“ und halte an.

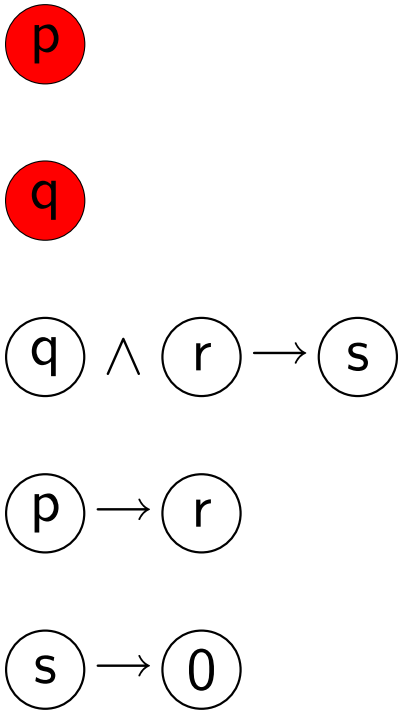
Erfüllbarkeitstest

Beispiel



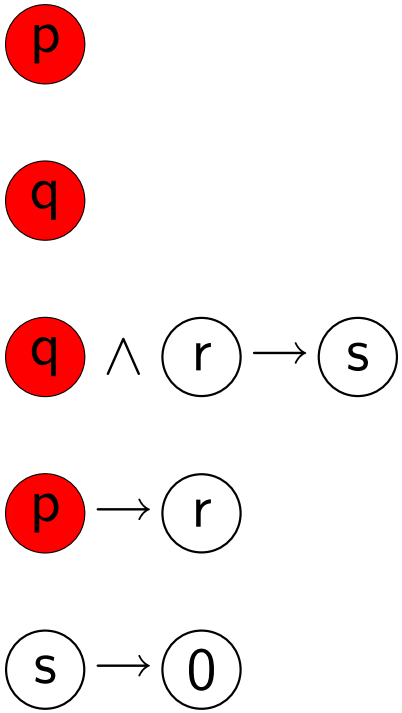
Erfüllbarkeitstest

Beispiel



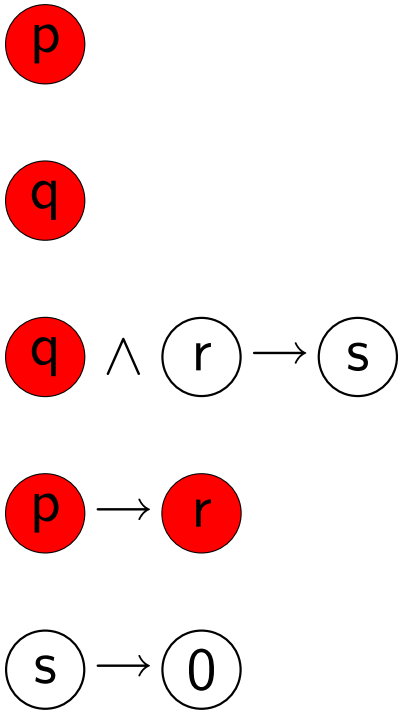
Erfüllbarkeitstest

Beispiel



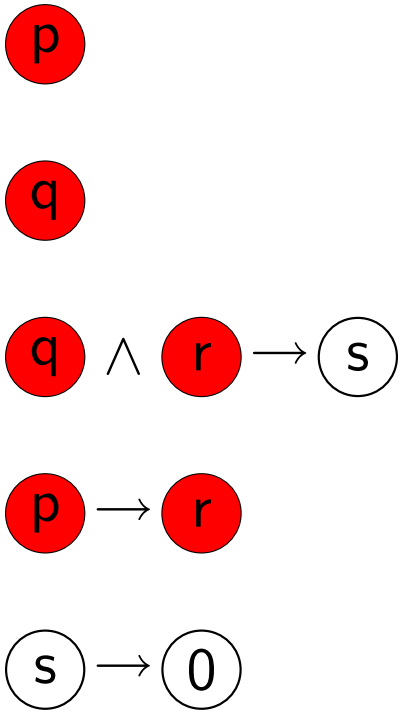
Erfüllbarkeitstest

Beispiel



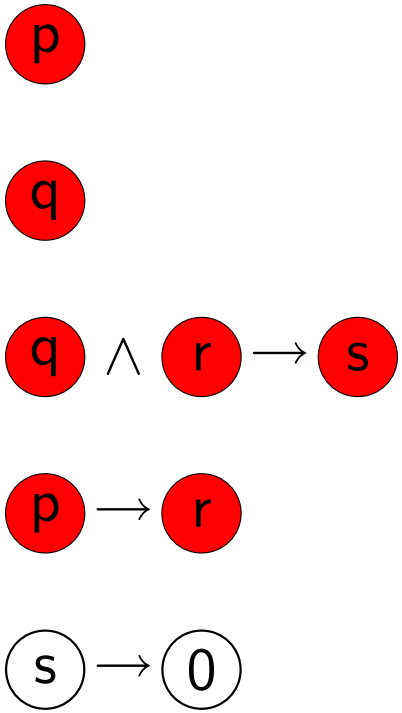
Erfüllbarkeitstest

Beispiel



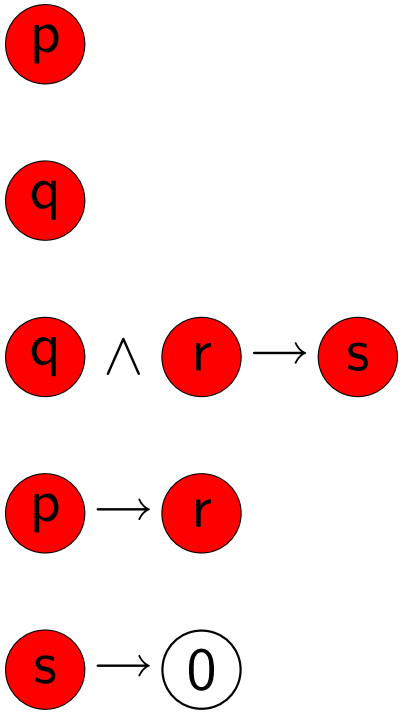
Erfüllbarkeitstest

Beispiel



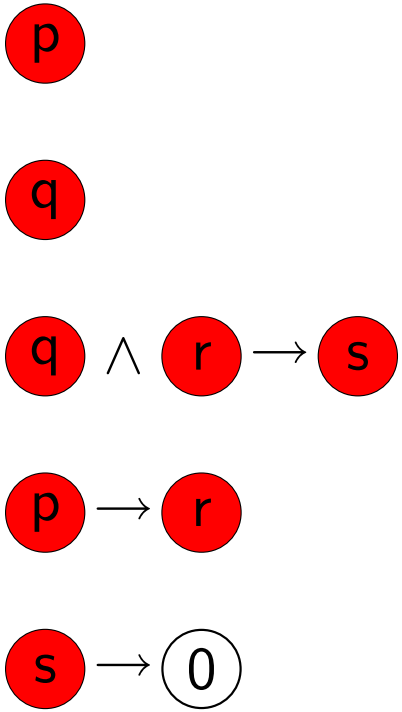
Erfüllbarkeitstest

Beispiel



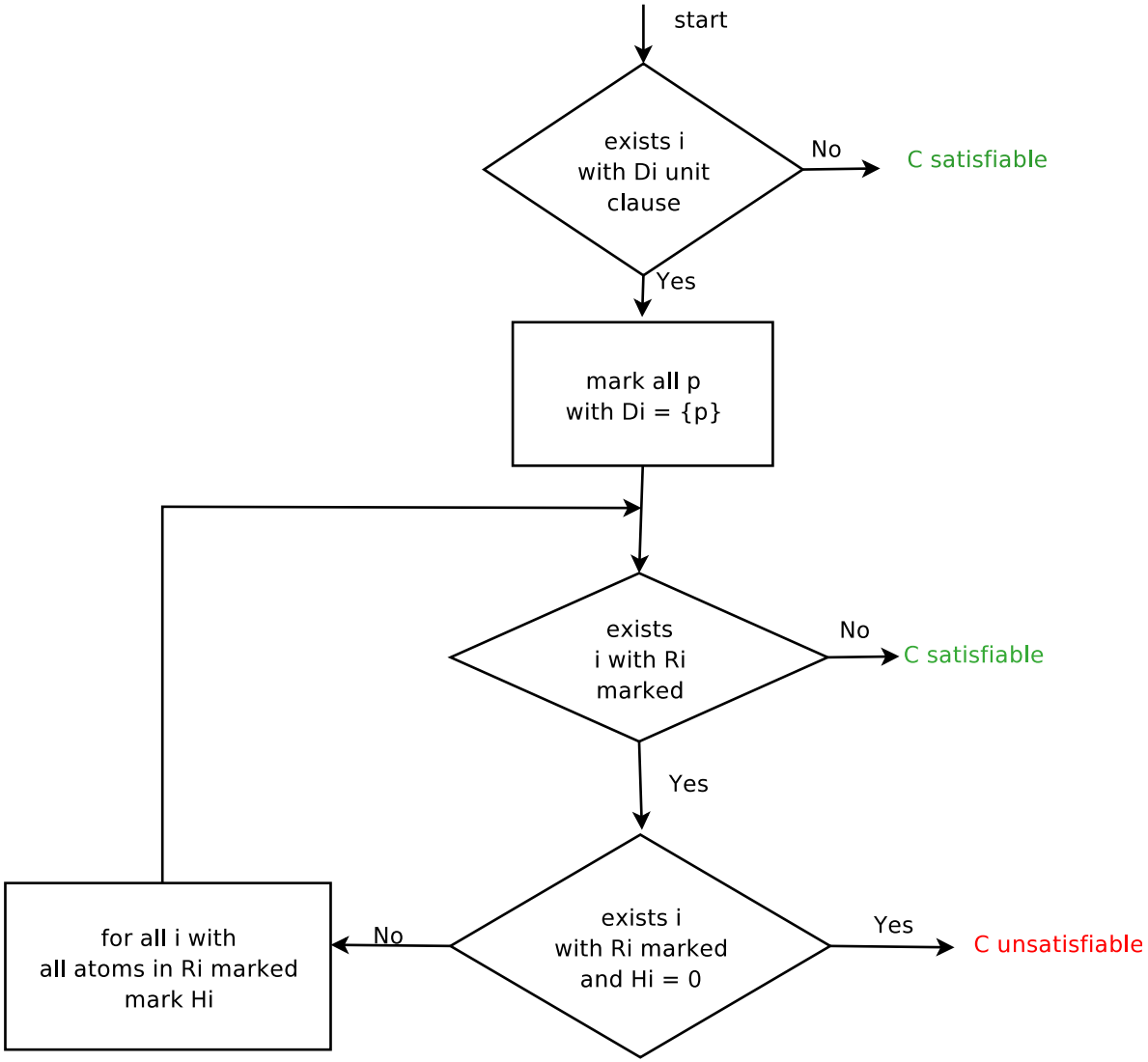
Erfüllbarkeitstest

Beispiel



Formelmenge nicht erfüllbar

Flußdiagramm



Korrektheitsaussagen

Da höchstens so viele Schritte zu machen sind, wie es Atome in C gibt, hat der Algorithmus einen quadratischen Zeitaufwand.
Zu zeigen ist noch, dass

1. wenn der Algorithmus mit „erfüllbar“ endet, auch eine erfüllende Belegung gefunden werden kann und

Korrektheitsaussagen

Da höchstens so viele Schritte zu machen sind, wie es Atome in C gibt, hat der Algorithmus einen quadratischen Zeitaufwand.
Zu zeigen ist noch, dass

1. wenn der Algorithmus mit „erfüllbar“ endet, auch eine erfüllende Belegung gefunden werden kann und
2. wenn C erfüllbar ist, der Algorithmus mit „erfüllbar“ abbricht.

Korrektheitsbeweis
Teil 1

Angenommen der Algorithmus endet mit der Ausgabe „erfüllbar“. Wir definieren I durch:

$$I(P) = W \quad \Leftrightarrow \quad P \text{ wurde markiert.}$$

Wir zeigen:
$val_I(D_i) = W$ für $i = 1, \ldots, m$,
woraus $val_I(C) = W$ folgt.
Fallunterscheidungen:

1. D_i ist ein Atom

Korrektheitsbeweis
Teil 1

Angenommen der Algorithmus endet mit der Ausgabe „erfüllbar“. Wir definieren I durch:

$$I(P) = W \quad \Leftrightarrow \quad P \text{ wurde markiert.}$$

Wir zeigen:
$val_I(D_i) = W$ für $i = 1, \ldots, m$,
woraus $val_I(C) = W$ folgt.
Fallunterscheidungen:

1. D_i ist ein Atom
2. $D_i = R_i \rightarrow \mathbf{0}$

Korrektheitsbeweis
Teil 1

Angenommen der Algorithmus endet mit der Ausgabe „erfüllbar“. Wir definieren I durch:

$$I(P) = W \quad \Leftrightarrow \quad P \text{ wurde markiert.}$$

Wir zeigen:
$val_I(D_i) = W$ für $i = 1, \ldots, m$,
woraus $val_I(C) = W$ folgt.
Fallunterscheidungen:

1. D_i ist ein Atom
2. $D_i = R_i \rightarrow \mathbf{0}$
3. $D_i = R_i \rightarrow K_i$

Korrektheitsbeweis
Teil 2

Sei I eine Interpretation mit $val_I(C) = W$.

Korrektheitsbeweis
Teil 2

Sei I eine Interpretation mit $val_I(C) = W$.

Wir zeigen für jedes markierte Atom A $val_I(A) = W$.

Korrektheitsbeweis
Teil 2

Sei I eine Interpretation mit $val_I(C) = W$.

Wir zeigen für jedes markierte Atom A $val_I(A) = W$.

Daraus folgt, dass der Algorithmus nicht mit „unerfüllbar“ abbrechen kann, da nicht alle Atome in einer Horn-Klausel der Form $R_i \rightarrow \mathbf{0}$ markiert werden können.

Für jedes markierte Atom: $\mathsf{val}_I(A) = W$

Induktion nach Anzahl der Durchläufe.

Für jedes markierte Atom: $\mathsf{val}_I(A) = W$

Induktion nach Anzahl der Durchläufe.

Offensichtlich wahr für die Markierungen im Schritt 0.

Für jedes markierte Atom: $\mathsf{val}_I(A) = W$

Induktion nach Anzahl der Durchläufe.

Offensichtlich wahr für die Markierungen im Schritt 0.

Angenommen das Atom A wird im $(t+1)$-ten Durchlauf markiert.

Für jedes markierte Atom: $val_I(A) = W$

Induktion nach Anzahl der Durchläufe.

Offensichtlich wahr für die Markierungen im Schritt 0.

Angenommen das Atom A wird im $(t+1)$-ten Durchlauf markiert.

Dann gibt es ein $D_i = R_i \longrightarrow A$ in C, so dass im t-ten Durchlauf alle Atome von R_i markiert waren.

Für jedes markierte Atom: $val_I(A) = W$

Induktion nach Anzahl der Durchläufe.

Offensichtlich wahr für die Markierungen im Schritt 0.

Angenommen das Atom A wird im $(t+1)$-ten Durchlauf markiert.

Dann gibt es ein $D_i = R_i \rightarrow A$ in C, so dass im t-ten Durchlauf alle Atome von R_i markiert waren.

Nach Induktionsvoraussetzung wissen wir, dass $val_I(R_i) = W$ gilt. Da ausserdem nach Annahme $val_I(D_i) = W$ sein soll, gilt auch $val_I(A) = W$.

Äquivalenzformeln

Wir betrachten das Fragment *ÄqFor* aussagenlogischer Formeln, das einzig aus

$$\leftrightarrow, \mathbf{1}, \mathbf{0}$$

und aussagenlogischen Variablen aufgebaute Formeln enthält.

Äquivalenzformeln

Wir betrachten das Fragment *ÄqFor* aussagenlogischer Formeln, das einzig aus

$$\leftrightarrow, \mathbf{1}, \mathbf{0}$$

und aussagenlogischen Variablen aufgebaute Formeln enthält.

Theorem

Eine Formel A aus ÄqFor ist eine Tautologie
gdw.
jede Aussagenvariable hat eine gerade Anzahl von Vorkommen in A
und die Konstante $\mathbf{0}$ *hat eine gerade Anzahl von Vorkommen in A.*

Beispiele

$$\Big((P \leftrightarrow \mathbf{1}) \leftrightarrow (\mathbf{0} \leftrightarrow Q)\Big) \leftrightarrow \Big((P \leftrightarrow Q) \leftrightarrow \mathbf{0}\Big)$$

ist eine Tautologie,

$$\Big((P \leftrightarrow \mathbf{0}) \leftrightarrow P\Big) \leftrightarrow \Big(Q \leftrightarrow (\mathbf{0} \leftrightarrow P) \leftrightarrow P\Big)$$

ist keine Tautologie.

Beweis des 1. Beispiels

Es gilt die Assoziativität

$$[(X \leftrightarrow Y) \leftrightarrow Z] \leftrightarrow [X \leftrightarrow (Y \leftrightarrow Z)]$$

Beweis des 1. Beispiels

Es gilt die Assoziativität

$$[(X \leftrightarrow Y) \leftrightarrow Z] \leftrightarrow [X \leftrightarrow (Y \leftrightarrow Z)]$$

$$\Big((P \leftrightarrow \mathbf{1}) \leftrightarrow (\mathbf{0} \leftrightarrow Q)\Big) \leftrightarrow \Big((P \leftrightarrow Q) \leftrightarrow \mathbf{0}\Big) \qquad \textit{Geg.}$$

Beweis des 1. Beispiels

Es gilt die Assoziativität

$$[(X \leftrightarrow Y) \leftrightarrow Z] \leftrightarrow [X \leftrightarrow (Y \leftrightarrow Z)]$$

$$\Big((P \leftrightarrow \mathbf{1}) \leftrightarrow (\mathbf{0} \leftrightarrow Q)\Big) \leftrightarrow \Big((P \leftrightarrow Q) \leftrightarrow \mathbf{0}\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{1} \leftrightarrow \mathbf{0} \leftrightarrow Q \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \qquad \textit{Assoz.}$$

Beweis des 1. Beispiels

Es gilt die Assoziativität

$$[(X \leftrightarrow Y) \leftrightarrow Z] \leftrightarrow [X \leftrightarrow (Y \leftrightarrow Z)]$$

$$\Big((P \leftrightarrow \mathbf{1}) \leftrightarrow (\mathbf{0} \leftrightarrow Q)\Big) \leftrightarrow \Big((P \leftrightarrow Q) \leftrightarrow \mathbf{0}\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{1} \leftrightarrow \mathbf{0} \leftrightarrow Q \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \qquad \textit{Assoz.}$$

$$\mathbf{1} \leftrightarrow P \leftrightarrow P \leftrightarrow Q \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow \mathbf{0} \qquad \textit{Komm.}$$

Beweis des 1. Beispiels

Es gilt die Assoziativität

$$[(X \leftrightarrow Y) \leftrightarrow Z] \leftrightarrow [X \leftrightarrow (Y \leftrightarrow Z)]$$

$$\Big((P \leftrightarrow \mathbf{1}) \leftrightarrow (\mathbf{0} \leftrightarrow Q)\Big) \leftrightarrow \Big((P \leftrightarrow Q) \leftrightarrow \mathbf{0}\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{1} \leftrightarrow \mathbf{0} \leftrightarrow Q \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \qquad \textit{Assoz.}$$

$$\mathbf{1} \leftrightarrow P \leftrightarrow P \leftrightarrow Q \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow \mathbf{0} \qquad \textit{Komm.}$$

$$\mathbf{1} \qquad (X \leftrightarrow X) \leftrightarrow \mathbf{1}$$

Beweis des 1. Beispiels

Es gilt die Assoziativität

$$[(X \leftrightarrow Y) \leftrightarrow Z] \leftrightarrow [X \leftrightarrow (Y \leftrightarrow Z)]$$

$$\Big((P \leftrightarrow \mathbf{1}) \leftrightarrow (\mathbf{0} \leftrightarrow Q)\Big) \leftrightarrow \Big((P \leftrightarrow Q) \leftrightarrow \mathbf{0}\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{1} \leftrightarrow \mathbf{0} \leftrightarrow Q \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \qquad \textit{Assoz.}$$

$$\mathbf{1} \leftrightarrow P \leftrightarrow P \leftrightarrow Q \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow \mathbf{0} \qquad \textit{Komm.}$$

$$\mathbf{1} \qquad (X \leftrightarrow X) \leftrightarrow \mathbf{1}$$

Tautologie

Beweis des 2. Beispiels

$$\Big((P \leftrightarrow \mathbf{0}) \leftrightarrow P\Big) \leftrightarrow \Big(Q \leftrightarrow (\mathbf{0} \leftrightarrow P) \leftrightarrow P\Big) \qquad \textit{Geg.}$$

Beweis des 2. Beispiels

$$\Big((P \leftrightarrow \mathbf{0}) \leftrightarrow P\Big) \leftrightarrow \Big(Q \leftrightarrow (\mathbf{0} \leftrightarrow P) \leftrightarrow P\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow P \qquad \textit{Assoz.}$$

Beweis des 2. Beispiels

$$\Big((P \leftrightarrow \mathbf{0}) \leftrightarrow P\Big) \leftrightarrow \Big(Q \leftrightarrow (\mathbf{0} \leftrightarrow P) \leftrightarrow P\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow P \qquad \textit{Assoz.}$$

$$P \leftrightarrow P \leftrightarrow P \leftrightarrow P \leftrightarrow \mathbf{0} \leftrightarrow \mathbf{0} \leftrightarrow Q \qquad \textit{Komm.}$$

Beweis des 2. Beispiels

$$\Big((P \leftrightarrow \mathbf{0}) \leftrightarrow P\Big) \leftrightarrow \Big(Q \leftrightarrow (\mathbf{0} \leftrightarrow P) \leftrightarrow P\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow P \qquad \textit{Assoz.}$$

$$P \leftrightarrow P \leftrightarrow P \leftrightarrow P \leftrightarrow \mathbf{0} \leftrightarrow \mathbf{0} \leftrightarrow Q \qquad \textit{Komm.}$$

$$Q \qquad (X \leftrightarrow X) \leftrightarrow \mathbf{1}$$

Beweis des 2. Beispiels

$$\Big((P \leftrightarrow \mathbf{0}) \leftrightarrow P\Big) \leftrightarrow \Big(Q \leftrightarrow (\mathbf{0} \leftrightarrow P) \leftrightarrow P\Big) \qquad \textit{Geg.}$$

$$P \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow Q \leftrightarrow \mathbf{0} \leftrightarrow P \leftrightarrow P \qquad \textit{Assoz.}$$

$$P \leftrightarrow P \leftrightarrow P \leftrightarrow P \leftrightarrow \mathbf{0} \leftrightarrow \mathbf{0} \leftrightarrow Q \qquad \textit{Komm.}$$

$$Q \qquad (X \leftrightarrow X) \leftrightarrow \mathbf{1}$$

keine Tautologie