Script generated by TTT

Title: Nipkow: Theo (04.07.2019)

Date: Thu Jul 04 14:25:31 CEST 2019

Duration: 76:55 min

Pages: 107

1. Polynomielle Reduzierbarkeit $\leq_p$
2. NP-vollständige Probleme = härteste Probleme in NP, alle anderen Probleme in NP darauf polynomiell reduzierbar

1. Polynomielle Reduzierbarkeit $\leq_p$
2. NP-vollständige Probleme = härteste Probleme in NP, alle anderen Probleme in NP darauf polynomiell reduzierbar
3. Satz: SAT ist NP-vollständig

Definition 6.10
Sei $A \subseteq \Sigma^*$ und $B \subseteq \Gamma^*$.

Definition 6.10
Sei $A \subseteq \Sigma^*$ und $B \subseteq \Gamma^*$.
Dann heißt A polynomiell reduzierbar auf B, $A \leq_p B$,
gdw es eine totale und von einer DTM in polynomieller Zeit
berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ gibt, so dass für alle $w \in \Sigma^*$

$$w \in A \iff f(w) \in B$$

Definition 6.10
Sei $A \subseteq \Sigma^*$ und $B \subseteq \Gamma^*$.
Dann heißt A polynomiell reduzierbar auf B, $A \leq_p B$,
gdw es eine totale und von einer DTM in polynomieller Zeit
berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ gibt, so dass für alle $w \in \Sigma^*$

$$w \in A \iff f(w) \in B$$

Lemma 6.11
Die Relation $\leq_p$ ist transitiv.

Definition 6.10
Sei $A \subseteq \Sigma^*$ und $B \subseteq \Gamma^*$.
Dann heißt A polynomiell reduzierbar auf B, $A \leq_p B$,
gdw es eine totale und von einer DTM in polynomieller Zeit
berechenbare Funktion $f : \Sigma^* \to \Gamma^*$ gibt, so dass für alle $w \in \Sigma^*$

$$w \in A \iff f(w) \in B$$

Lemma 6.11
Die Relation $\leq_p$ ist transitiv.

Da $p_2(p_1(n))$ ein Polynom ist falls p_1 und p_2 Polynome sind.

Beispiel 6.12

HAMILTONKREIS

Gegeben: Ungerichteter Graph G

Beispiel 6.12

HAMILTONKREIS

Gegeben: Ungerichteter Graph G

Problem: Enthält G einen Hamilton-Kreis, dh einen geschlossenen Pfad, der jeden Knoten genau einmal enthält?

Beispiel 6.12

HAMILTONKREIS

Gegeben: Ungerichteter Graph G

Problem: Enthält G einen Hamilton-Kreis, dh einen geschlossenen Pfad, der jeden Knoten genau einmal enthält?

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

Problem: Gibt es eine „Rundreise“ (Hamilton-Kreis) der Länge $\leq k$?

Beispiel 6.12

HAMILTONKREIS

Gegeben: Ungerichteter Graph G

Problem: Enthält G einen Hamilton-Kreis, dh einen geschlossenen Pfad, der jeden Knoten genau einmal enthält?

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

Problem: Gibt es eine „Rundreise“ (Hamilton-Kreis) der Länge $\leq k$?

HAMILTON $\leq_p$ TSP

$$(\{1, \ldots, n\}, E) \mapsto (M, n)$$

wobei

$$M_{ij} := \begin{cases} 1 & \text{falls } \{i,j\} \in E \\ 2 & \text{sonst} \end{cases}$$

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

- $M_f[w]$ macht $\leq p(|w|)$ Schritte.

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

- $M_f[w]$ macht $\leq p(|w|)$ Schritte.
- Ausgabe $f(w)$ von M_f hat Länge $\leq |w| + p(|w|)$.

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

- $M_f[w]$ macht $\leq p(|w|)$ Schritte.
- Ausgabe $f(w)$ von M_f hat Länge $\leq |w| + p(|w|)$.
- M macht $\leq q(|f(w)|) \leq q(|w|+p(|w|))$ Schritte (q monoton)

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

- $M_f[w]$ macht $\leq p(|w|)$ Schritte.
- Ausgabe $f(w)$ von M_f hat Länge $\leq |w| + p(|w|)$.
- M macht $\leq q(|f(w)|) \leq q(|w|+p(|w|))$ Schritte (q monoton)

Daher macht $(M_f; M)[w]$ maximal $p(|w|) + q(|w| + p(|w|))$ Schritte, ein Polynom in $|w|$.

Lemma 6.13

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f, die von DTM M_f berechnet wird.
  Polynom p beschränkt Rechenzeit von M_f.
- Sei $B \in$ P mittels DTM M.
  Polynom q beschränkt Rechenzeit von M.

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

- $M_f[w]$ macht $\leq p(|w|)$ Schritte.
- Ausgabe $f(w)$ von M_f hat Länge $\leq |w| + p(|w|)$.
- M macht $\leq q(|f(w)|) \leq q(|w|+p(|w|))$ Schritte (q monoton)

Daher macht $(M_f; M)[w]$ maximal $p(|w|) + q(|w| + p(|w|))$ Schritte, ein Polynom in $|w|$.

Analog: $A \leq_p B \in$ NP $\implies A \in$ NP □

Ein Problem ist NP-schwer,
wenn es mindestens so schwer wie alles in NP ist:

Definition 6.14

Eine Sprache L heißt NP-schwer gdw $A \leq_p L$ für alle $A \in$ NP.

Ein Problem ist NP-schwer,
wenn es mindestens so schwer wie alles in NP ist:

Definition 6.14

Eine Sprache L heißt NP-schwer gdw $A \leq_p L$ für alle $A \in$ NP.

Definition 6.15

Eine Sprache L heißt NP-vollständig gdw
L NP-schwer ist und $L \in$ NP.

Ein Problem ist NP-schwer,
wenn es mindestens so schwer wie alles in NP ist:

Definition 6.14

Eine Sprache L heißt NP-schwer gdw $A \leq_p L$ für alle $A \in$ NP.

Definition 6.15

Eine Sprache L heißt NP-vollständig gdw
L NP-schwer ist und $L \in$ NP.

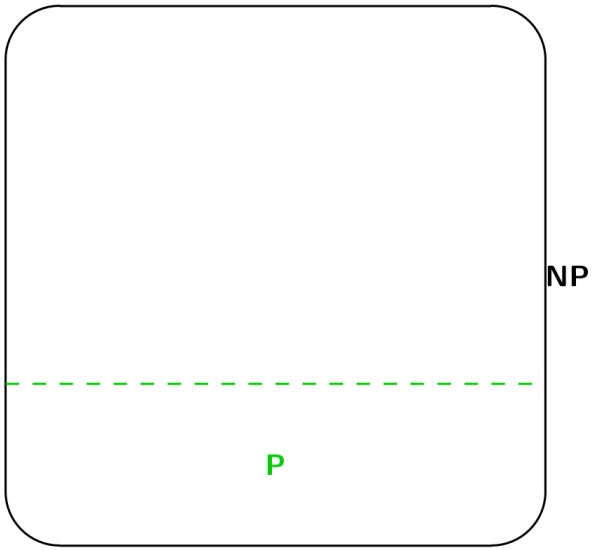
NP-vollständige Probleme sind die schwierigsten Probleme in NP:

Ein Problem ist NP-schwer,
wenn es mindestens so schwer wie alles in NP ist:

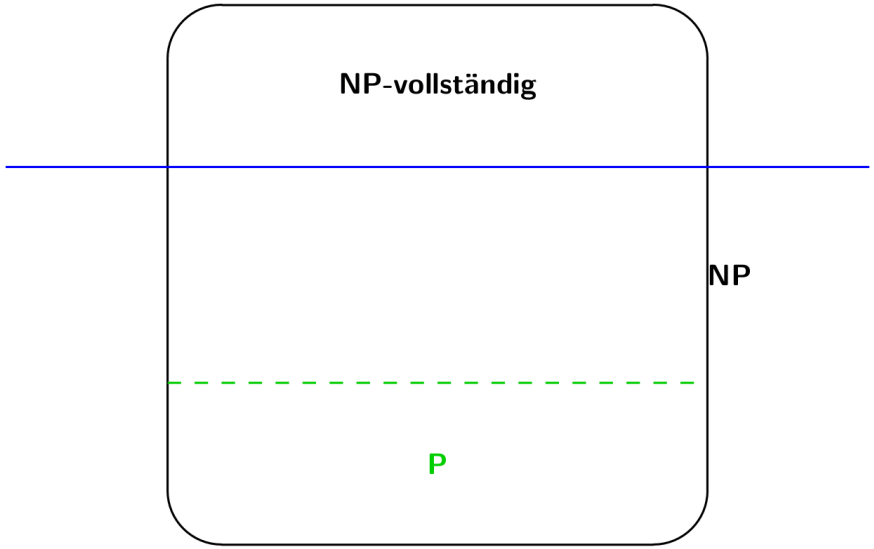
Definition 6.14
Eine Sprache L heißt NP-schwer gdw $A \leq_p L$ für alle $A \in$ NP.

Definition 6.15
Eine Sprache L heißt NP-vollständig gdw
L NP-schwer ist und $L \in$ NP.

NP-vollständige Probleme sind die schwierigsten Probleme in NP:
alle Probleme in NP sind polynomiell auf sie reduzierbar.

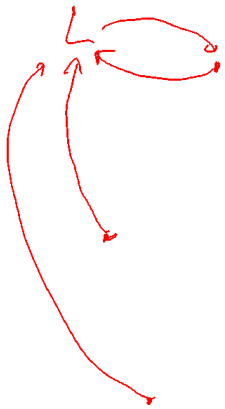


NP-schwer



Wie man P$\stackrel{?}{=}$NP lösen kann:

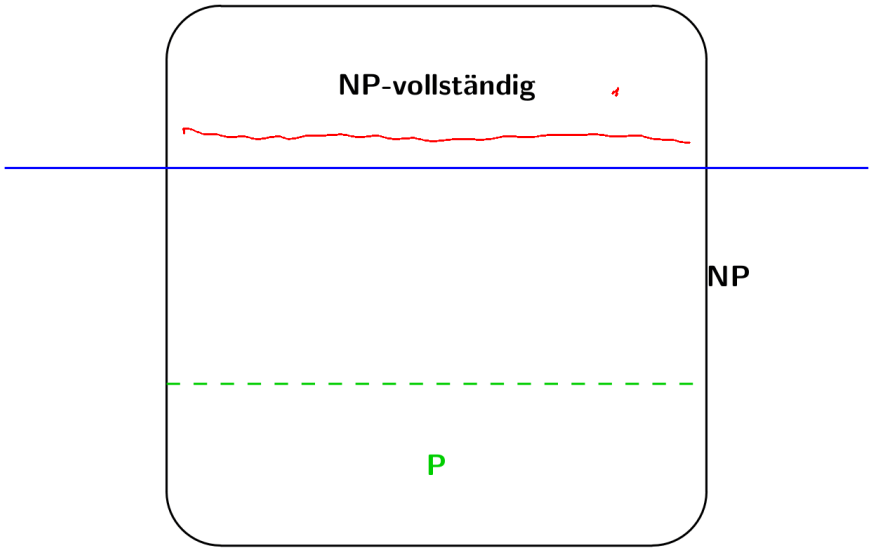
Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.



Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

NP-schwer



Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

Beweis:
„$\Rightarrow$“: Falls P=NP, so liegt jedes NP-vollständige Problem in P.

„$\Leftarrow$“: Sei L ein NP-vollständiges Problem in P.

Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

Beweis:
„$\Rightarrow$“: Falls P=NP, so liegt jedes NP-vollständige Problem in P.

„$\Leftarrow$“: Sei L ein NP-vollständiges Problem in P. Dann gilt P $\supseteq$ NP: Ist $A \in$ NP, so gilt $A \leq_p L$ (da L NP-schwer) und nach Lemma 6.13 $A \in$ P (da $L \in$ P). □

Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

Beweis:
„$\Rightarrow$“: Falls P=NP, so liegt jedes NP-vollständige Problem in P.

„$\Leftarrow$“: Sei L ein NP-vollständiges Problem in P. Dann gilt P $\supseteq$ NP: Ist $A \in$ NP, so gilt $A \leq_p L$ (da L NP-schwer) und nach Lemma 6.13 $A \in$ P (da $L \in$ P). □

Starke Vermutung:

- P $\neq$ NP
- dh kein NP-vollständiges Problem ist in P.

Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

Beweis:
„$\Rightarrow$“: Falls P=NP, so liegt jedes NP-vollständige Problem in P.

„$\Leftarrow$“: Sei L ein NP-vollständiges Problem in P. Dann gilt P $\supseteq$ NP: Ist $A \in$ NP, so gilt $A \leq_p L$ (da L NP-schwer) und nach Lemma 6.13 $A \in$ P (da $L \in$ P). □

Starke Vermutung:

- P $\neq$ NP
- dh kein NP-vollständiges Problem ist in P.

Wie man P$\stackrel{?}{=}$NP lösen kann:

Lemma 6.16
Es gilt P=NP gdw ein NP-vollständiges Problem in P liegt.

Beweis:
„$\Rightarrow$“: Falls P=NP, so liegt jedes NP-vollständige Problem in P.

„$\Leftarrow$“: Sei L ein NP-vollständiges Problem in P. Dann gilt P $\supseteq$ NP: Ist $A \in$ NP, so gilt $A \leq_p L$ (da L NP-schwer) und nach Lemma 6.13 $A \in$ P (da $L \in$ P). □

Starke Vermutung:

- P $\neq$ NP
- dh kein NP-vollständiges Problem ist in P.

Aber gibt es überhaupt NP-vollständige Probleme?

Aussagenlogik

Syntax der Aussagenlogik:

Aussagenlogik

Syntax der Aussagenlogik:

Variablen: $X \rightarrow x \mid y \mid z \mid \ldots$

Aussagenlogik

Syntax der Aussagenlogik:

Variablen: $X \rightarrow x \mid y \mid z \mid \ldots$

Formeln: $F \rightarrow X \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid X$

Bsp: $((\neg x \wedge y) \vee (x \wedge \neg z))$

Aussagenlogik

Syntax der Aussagenlogik:

Variablen: $X \rightarrow x \mid y \mid z \mid \ldots$

Formeln: $F \rightarrow X \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid X$

Bsp: $((\neg x \wedge y) \vee (x \wedge \neg z))$

Man darf einige Klammern weglassen:

- Äußerste Klammern: $(x \vee y) \wedge z$ statt $((x \vee y) \wedge z)$
- Assoziativität: $(x \vee y \vee z) \wedge \neg x$ statt $((x \vee y) \vee z) \wedge \neg x$.

Abkürzungen:

$F_1 \rightarrow F_2 \equiv \neg F_1 \vee F_2$

Aussagenlogik

Syntax der Aussagenlogik:

Variablen: $X \rightarrow x \mid y \mid z \mid \ldots$

Formeln: $F \rightarrow X \mid \neg F \mid (F \wedge F) \mid (F \vee F) \mid X$

Bsp: $((\neg x \wedge y) \vee (x \wedge \neg z))$

Man darf einige Klammern weglassen:

- Äußerste Klammern: $(x \vee y) \wedge z$ statt $((x \vee y) \wedge z)$
- Assoziativität: $(x \vee y \vee z) \wedge \neg x$ statt $((x \vee y) \vee z) \wedge \neg x$.

Abkürzungen:

$F_1 \rightarrow F_2 \equiv \neg F_1 \vee F_2$

$\bigwedge_{i=1}^{n} F_i \equiv F_1 \wedge \cdots \wedge F_n$

Semantik der Aussagenlogik:

Semantik der Aussagenlogik:

- Eine Belegung ist eine Funktion von Variablen auf $\{0, 1\}$.
  Bsp: $\sigma = \{x \mapsto 0, y \mapsto 1, z \mapsto 0, \dots\}$
- Belegungen werden mittels Wahrheitstabellen auf Formeln erweitert. Bsp: $\sigma((\neg x \wedge y) \vee (x \wedge \neg z)) = 1$
- Eine Formel F ist erfüllbar gdw es eine Belegung σ gibt mit $\sigma(F) = 1$.

SAT

Gegeben: Eine aussagenlogische Formel F.

Problem: Ist F erfüllbar?

Lemma 6.17
SAT $\in$ *NP*

SAT

Gegeben: Eine aussagenlogische Formel F.

Problem: Ist F erfüllbar?

Lemma 6.17
SAT $\in$ *NP*

Beweis:
Belegungen sind Zertifikate, die in polynomieller Zeit geprüft werden können:

SAT

Gegeben: Eine aussagenlogische Formel F.

Problem: Ist F erfüllbar?

Lemma 6.17

SAT $\in$ *NP*

Beweis:

Belegungen sind Zertifikate, die in polynomieller Zeit geprüft werden können:
Es gibt eine DTM, die bei Eingabe einer Formel F und einer Belegung σ für die Variablen in F, in polynomieller Zeit $\sigma(F)$ berechnet. □

Satz 6.18 (Cook 1971)

SAT ist NP-vollständig.

Beweis:

Da SAT $\in$ NP, bleibt noch zu zeigen, SAT ist NP-schwer.

Satz 6.18 (Cook 1971)

SAT ist NP-vollständig.

Beweis:

Da SAT $\in$ NP, bleibt noch zu zeigen, SAT ist NP-schwer.
Sei $A \in$ NP. Wir zeigen $A \leq_p$ SAT.

Da $A \in$ NP gibt es NTM M mit $A = L(M)$ und
Polynom p mit $ntime_M(w) \leq p(|w|)$.

Satz 6.18 (Cook 1971)

SAT ist NP-vollständig.

Beweis:

Da SAT $\in$ NP, bleibt noch zu zeigen, SAT ist NP-schwer.
Sei $A \in$ NP. Wir zeigen $A \leq_p$ SAT.

Da $A \in$ NP gibt es NTM M mit $A = L(M)$ und
Polynom p mit $ntime_M(w) \leq p(|w|)$.

Reduktion bildet $w = x_1 \dots x_n \in \Sigma^*$ auf eine Formel F ab.

Satz 6.18 (Cook 1971)

SAT ist NP-vollständig.

Beweis:

Da SAT $\in$ NP, bleibt noch zu zeigen, SAT ist NP-schwer.
Sei $A \in$ NP. Wir zeigen $A \leq_p$ SAT.

Da $A \in$ NP gibt es NTM M mit $A = L(M)$ und
Polynom p mit $\mathit{ntime}_M(w) \leq p(|w|)$.

Reduktion bildet $w = x_1 \dots x_n \in \Sigma^*$ auf eine Formel F ab.

- In polynomieller Zeit.

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

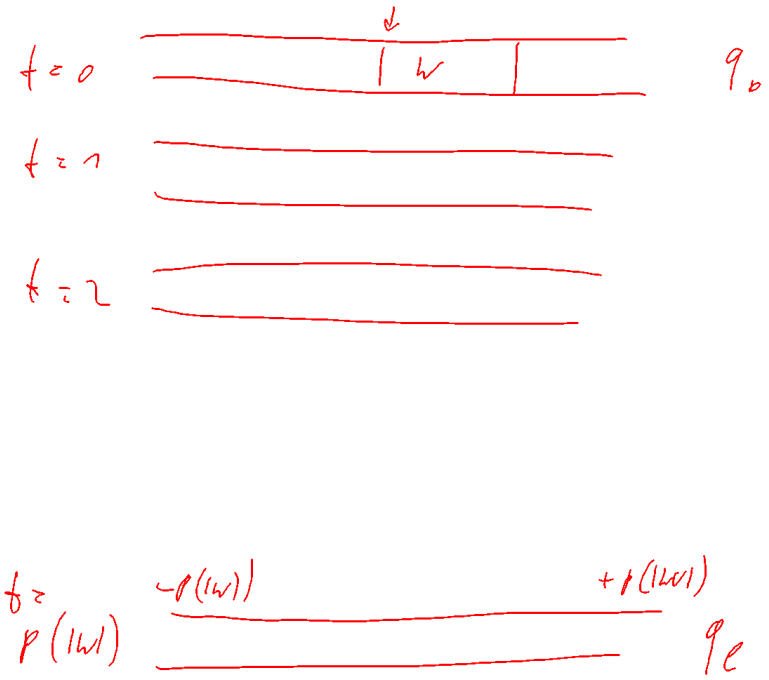
Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

$\mathit{zust}_{t,q}$	$t = 0, \dots, p(n)$ $q \in Q$	



Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	$pos_{t,i} = 1 \Leftrightarrow$ Kopfposition nach t Schritten ist i

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	$pos_{t,i} = 1 \Leftrightarrow$ Kopfposition nach t Schritten ist i
$band_{t,i,a}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots, p(n)$ $a \in \Gamma$	

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	$pos_{t,i} = 1 \Leftrightarrow$ Kopfposition nach t Schritten ist i
$band_{t,i,a}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots, p(n)$ $a \in \Gamma$	$band_{t,i,a} = 1 \Leftrightarrow$ Bandinhalt nach t Schritten auf Bandposition i ist Zeichen a

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	$pos_{t,i} = 1 \Leftrightarrow$ Kopfposition nach t Schritten ist i
$band_{t,i,a}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots, p(n)$ $a \in \Gamma$	$band_{t,i,a} = 1 \Leftrightarrow$ Bandinhalt nach t Schritten auf Bandposition i ist Zeichen a

Jede Berechnunge von $M[w]$ ist als Variablenbelegung kodierbar,

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	$pos_{t,i} = 1 \Leftrightarrow$ Kopfposition nach t Schritten ist i
$band_{t,i,a}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots, p(n)$ $a \in \Gamma$	$band_{t,i,a} = 1 \Leftrightarrow$ Bandinhalt nach t Schritten auf Bandposition i ist Zeichen a

Jede Berechnunge von $M[w]$ ist als Variablenbelegung kodierbar, aber nicht umgekehrt.

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F := R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

$R \;\Leftrightarrow$ Zu jeder Zeit: Ein Zustand, eine Position, ein Zeichen pro Feld

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

$R \;\Leftrightarrow$ Zu jeder Zeit: Ein Zustand, eine Position, ein Zeichen pro Feld

$$R \;:=\; \bigwedge_{t=0}^{p(n)} [G(\mathit{zust}_{t,q_1}, \ldots, \mathit{zust}_{t,q_k}) \wedge$$

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

$R \;\Leftrightarrow$ Zu jeder Zeit: Ein Zustand, eine Position, ein Zeichen pro Feld

$$R \;:=\; \bigwedge_{t=0}^{p(n)} [G(\mathit{zust}_{t,q_1}, \ldots, \mathit{zust}_{t,q_k}) \wedge G(\mathit{pos}_{t,-p(n)}, \ldots, \mathit{pos}_{t,p(n)}) \wedge$$

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

$R \;\Leftrightarrow$ Zu jeder Zeit: Ein Zustand, eine Position, ein Zeichen pro Feld

$$R \;:=\; \bigwedge_{t=0}^{p(n)} [G(\mathit{zust}_{t,q_1}, \ldots, \mathit{zust}_{t,q_k}) \wedge G(\mathit{pos}_{t,-p(n)}, \ldots, \mathit{pos}_{t,p(n)}) \wedge \bigwedge_{i=-p(n)}^{p(n)} G(\mathit{band}_{t,i,a_1}, \ldots, \mathit{band}_{t,i,a_l})]$$

Beweis (Forts.):

$A \;\Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

Beweis (Forts.):

$A \;\Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

$$A \;:=\; \mathit{zust}_{0,q_1}$$

Beweis (Forts.):

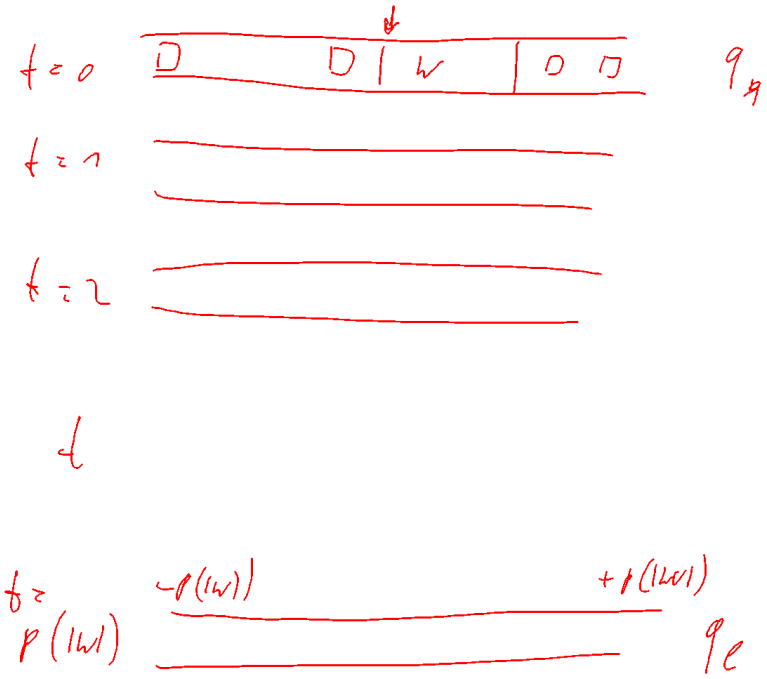
$A \;\Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

$$A \;:=\; \mathit{zust}_{0,q_1} \wedge \mathit{pos}_{0,1}$$

Beweis (Forts.):

Die Variablen von F beschreiben das *mögliche* Verhalten von $M[w]$:

		Intendierte Bedeutung
$zust_{t,q}$	$t = 0, \ldots, p(n)$ $q \in Q$	$zust_{t,q} = 1 \Leftrightarrow$ Zustand nach t Schritten ist q
$pos_{t,i}$	$t = 0, \ldots, p(n)$ $i = -p(n), \ldots p(n)$	



Beweis (Forts.):

$A \Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

$$A := zust_{0,q_1} \wedge pos_{0,1} \wedge \bigwedge_{j=1}^{n} band_{0,j,x_j} \wedge \bigwedge_{j=-p(n)}^{0} band_{0,j,\square} \wedge \bigwedge_{j=n+1}^{p(n)} band_{0,j,\square}$$

Beweis (Forts.):

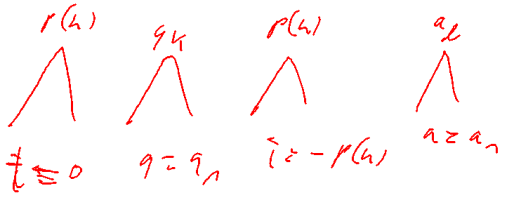
$A \Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

$$A := zust_{0,q_1} \wedge pos_{0,1} \wedge \bigwedge_{j=1}^{n} band_{0,j,x_j} \wedge \bigwedge_{j=-p(n)}^{0} band_{0,j,\square} \wedge \bigwedge_{j=n+1}^{p(n)} band_{0,j,\square}$$

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 \quad := \quad \bigwedge_{t,q,i,a}$$



Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 \quad := \quad \bigwedge_{t,q,i,a} [(\mathit{zust}_{t,q} \wedge \mathit{pos}_{t,i} \wedge \mathit{band}_{t,i,a})$$

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 \quad := \quad \bigwedge_{t,q,i,a} [(\mathit{zust}_{t,q} \wedge \mathit{pos}_{t,i} \wedge \mathit{band}_{t,i,a}) \rightarrow \bigvee_{(q',a',y)\in\delta(q,a)}$$

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 \quad := \quad \bigwedge_{t,q,i,a} [(\mathit{zust}_{t,q} \wedge \mathit{pos}_{t,i} \wedge \mathit{band}_{t,i,a}) \rightarrow \bigvee_{(q',a',y)\in\delta(q,a)} (\mathit{zust}_{t+1,q'} \wedge \mathit{pos}_{t+1,i+y} \wedge \mathit{band}_{t+1,i,a'})]$$

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 := \bigwedge_{t,q,i,a} [(zust_{t,q} \wedge pos_{t,i} \wedge band_{t,i,a}) \rightarrow \bigvee_{(q',a',y)\in\delta(q,a)} (zust_{t+1,q'} \wedge pos_{t+1,i+y} \wedge band_{t+1,i,a'})]$$

$$T_2 := \bigwedge_{t,i,a} [(\neg pos_{t,i} \wedge band_{t,i,a}) \rightarrow band_{t+1,i,a}]$$

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 := \bigwedge_{t,q,i,a} [(zust_{t,q} \wedge pos_{t,i} \wedge band_{t,i,a}) \rightarrow \bigvee_{(q',a',y)\in\delta(q,a)} (zust_{t+1,q'} \wedge pos_{t+1,i+y} \wedge band_{t+1,i,a'})]$$

$$T_2 := \bigwedge_{t,i,a} [(\neg pos_{t,i} \wedge band_{t,i,a}) \rightarrow band_{t+1,i,a}]$$

$E \not\approx$ Berechnung erreicht einen Endzustand

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 := \bigwedge_{t,q,i,a} [(zust_{t,q} \wedge pos_{t,i} \wedge band_{t,i,a}) \rightarrow \bigvee_{(q',a',y)\in\delta(q,a)} (zust_{t+1,q'} \wedge pos_{t+1,i+y} \wedge band_{t+1,i,a'})]$$

$$T_2 := \bigwedge_{t,i,a} [(\neg pos_{t,i} \wedge band_{t,i,a}) \rightarrow band_{t+1,i,a}]$$

$E \approx$ Berechnung erreicht einen Endzustand

$$E := \bigvee_{t} \bigvee_{q\in F} zust_{t,q}$$

Beweis (Forts.):

$T_1 \wedge T_2 \Leftrightarrow$ Berechnung respektiert δ von M

$$T_1 := \bigwedge_{t,q,i,a} [(zust_{t,q} \wedge pos_{t,i} \wedge band_{t,i,a}) \rightarrow \bigvee_{(q',a',y)\in\delta(q,a)} (zust_{t+1,q'} \wedge pos_{t+1,i+y} \wedge band_{t+1,i,a'})]$$

$$T_2 := \bigwedge_{t,i,a} [(\neg pos_{t,i} \wedge band_{t,i,a}) \rightarrow band_{t+1,i,a}]$$

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

Beweis (Forts.):

Nun einfach zu sehen:

Akzeptierende Berechnung von $M[w]$ $\Leftrightarrow$ Erfüllende Belegung von F

Größe von F polynomiell in n:

Beweis (Forts.):

Nun einfach zu sehen:

Akzeptierende Berechnung von $M[w]$ $\Leftrightarrow$ Erfüllende Belegung von F

Größe von F polynomiell in n:

Mit $|Q| = k$, $|\Gamma| = l$, $|w| = n$:

Beweis (Forts.):

Nun einfach zu sehen:

Akzeptierende Berechnung von $M[w]$ $\Leftrightarrow$ Erfüllende Belegung von F

Größe von F polynomiell in n:

Mit $|Q| = k$, $|\Gamma| = l$, $|w| = n$:

Beweis (Forts.):

Sei $Q = \{q_1, \ldots, q_k\}$ und $\Gamma = \{a_1, \ldots, a_l\}$.

$$F \;:=\; R \wedge A \wedge T_1 \wedge T_2 \wedge E$$

Hilfsformel „Genau ein Argument ist 1“:

$$G(v_1, \ldots, v_r) := (\bigvee_{i=1}^{r} v_i) \wedge \left(\bigwedge_{i=1}^{r-1} \bigwedge_{j=i+1}^{r} \neg(v_i \wedge v_j) \right)$$

$R \;\Leftrightarrow$ Zu jeder Zeit: Ein Zustand, eine Position, ein Zeichen pro Feld

$$R := \bigwedge_{t=0}^{p(n)} [G(\mathit{zust}_{t,q_1}, \ldots, \mathit{zust}_{t,q_k}) \wedge G(\mathit{pos}_{t,-p(n)}, \ldots, \mathit{pos}_{t,p(n)}) \wedge \bigwedge_{i=-p(n)}^{p(n)} G(\mathit{band}_{t,i,a_1}, \ldots, \mathit{band}_{t,i,a_l})]$$

Beweis (Forts.):

Nun einfach zu sehen:

Akzeptierende Berechnung von $M[w] \;\Leftrightarrow$ Erfüllende Belegung von F

Größe von F polynomiell in n:

Beweis (Forts.):

$A \Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

$$A \;:=\; \mathit{zust}_{0,q_1}$$

Beweis (Forts.):

Nun einfach zu sehen:

Akzeptierende Berechnung von $M[w] \;\Leftrightarrow$ Erfüllende Belegung von F

Größe von F polynomiell in n:

Mit $|Q| = k$, $|\Gamma| = l$, $|w| = n$:

Beweis (Forts.):

$A \Leftrightarrow$ Berechnung startet aus der Anfangskonfiguration mit w

Beweis (Forts.):

Nun einfach zu sehen:

Akzeptierende Berechnung von $M[w]$ $\Leftrightarrow$ Erfüllende Belegung von F

Größe von F polynomiell in n:

Mit $|Q| = k$, $|\Gamma| = l$, $|w| = n$:

$\lvert G(v_1, \ldots, v_r)\rvert$:	$O(r^2)$
$\lvert R\rvert$:	$O\big(p(n) \cdot \big(k^2 + (2 \cdot p(n))^2 + 2 \cdot p(n) \cdot l^2\big)\big)$
$\lvert A\rvert$:	$O(p(n))$
$\lvert T_1 \wedge T_2\rvert$:	$O(p(n)^2 \cdot k^2 \cdot l^2)$
$\lvert E\rvert$:	$O(p(n) \cdot k)$

$\Longrightarrow$ $|F| \in O(p(n)^3)$

□

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**
    if $F[x_i := 0] \in$ SAT **then** $b := 0$ **else** $b := 1$

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**
    if $F[x_i := 0] \in$ SAT **then** $b := 0$ **else** $b := 1$
    output(x_i "=" b)

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**
    if $F[x_i := 0] \in$ SAT **then** $b := 0$ **else** $b := 1$
    output(x_i "=" b)
    $F := F[x_i := b]$

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**
    if $F[x_i := 0] \in$ SAT **then** $b := 0$ **else** $b := 1$
    output(x_i "=" b)
    $F := F[x_i := b]$

wobei $F[x := b] = F$ mit x ersetzt durch b.

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**
    if $F[x_i := 0] \in$ SAT **then** $b := 0$ **else** $b := 1$
    output(x_i "=" b)
    $F := F[x_i := b]$

wobei $F[x := b] = F$ mit x ersetzt durch b.

Entscheidung von SAT in Zeit $O(f(n))$
$\Longrightarrow$ Berechnung einer erf. Bel. in Zeit $O(n \cdot (f(n) + n))$
(falls es eine gibt.)

$f(n)$ polynomiell $\Longrightarrow$ $n \cdot (f(n) + n)$ polynomiell

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen $x_1, \ldots, x_k$:

if $F \notin$ SAT **then** output("nicht lösbar")
else
  for $i := 1$ **to** k **do**
    if $F[x_i := 0] \in$ SAT **then** $b := 0$ **else** $b := 1$
    output(x_i "=" b)
    $F := F[x_i := b]$

wobei $F[x := b] = F$ mit x ersetzt durch b.

Entscheidung von SAT in Zeit $O(f(n))$
$\Longrightarrow$ Berechnung einer erf. Bel. in Zeit $O(n \cdot (f(n) + n))$
(falls es eine gibt.)

$f(n)$ polynomiell $\Longrightarrow$ $n \cdot (f(n) + n)$ polynomiell
$f(n)$ exponentiell $\Longrightarrow$ $n \cdot (f(n) + n)$ exponentiell

Bemerkungen:

- Die Reduktion der Lösungsberechnung auf SAT ist eine rein theoretische Konstruktion.

Bemerkungen:

- Die Reduktion der Lösungsberechnung auf SAT ist eine rein theoretische Konstruktion.
- Sie zeigt, dass man sich auf SAT beschränken kann, wenn man nur an polynomiell/exponentiell interessiert ist.
- Alle bekannten Entscheidungsverfahren für SAT berechnen auch eine Lösung.

351

Tutoren gesucht!

Tutoren gesucht!

Diskrete Strukturen (Brandt)
Funktionale Programmierung/Info 2 (Nipkow)
Theo im SS20 (Nipkow)

- Sie hatten Spaß an DS/FP/Theo,
- hatten keine Probleme mit der Klausur,
- hätten Lust als Tutor zu arbeiten?

352