

Der Satz von Cook

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für
Theoretische Informatik

Stand: 11. Juli 2023

Folien ursprünglich von PD Dr. David Sabel



Definition (\mathcal{NP} -Vollständigkeit)

Eine Sprache L heißt \mathcal{NP} -vollständig, wenn gilt

1. $L \in \mathcal{NP}$ und
2. L ist \mathcal{NP} -schwer (manchmal auch \mathcal{NP} -hart genannt):
Für alle $L' \in \mathcal{NP}$ gilt $L' \leq_p L$

Beweistechnik für \mathcal{NP} -Schwere:

- ▶ Zeige $L_0 \leq_p L$ für ein bekanntes \mathcal{NP} -vollständiges Problem.
- ▶ Dann folgt die \mathcal{NP} -Schwere von L .

SAT-Problem

- ▶ Wir brauchen ein erstes Problem, dessen \mathcal{NP} -Vollständigkeit wir von Hand nachweisen müssen.
- ▶ Dafür nehmen wir das SAT-Problem.

Definition (SAT-Problem)

Das **Erfüllbarkeitsproblem der Aussagenlogik** (kurz **SAT**) ist:

gegeben: Eine aussagenlogische Formel F

gefragt: Ist F erfüllbar, d.h. gibt es eine erfüllende Belegung der Variablen mit den Wahrheitswerten 0 und 1, sodass F den Wert 1 erhält?

Als formale Sprache:

$$\text{SAT} = \{ \text{code}(F) \in \Sigma^* \mid F \text{ ist erfüllbare Formel der Aussagenlogik} \}$$

SAT \in NP

Lemma

SAT \in NP.

Lemma

SAT $\in \mathcal{NP}$.

Beweis:

- ▶ Konstruiere eine NTM M mit $code(F)$ als Eingabe.
- ▶ M berechnet, welche Variablen in F vorkommen. Seien diese $\{x_1, \dots, x_n\}$.
- ▶ M verwendet Nichtdeterminismus, um Belegung zu „raten“:

$$I : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$$

Lemma

SAT $\in \mathcal{NP}$.

Beweis:

- ▶ Konstruiere eine NTM M mit $code(F)$ als Eingabe.
- ▶ M berechnet, welche Variablen in F vorkommen. Seien diese $\{x_1, \dots, x_n\}$.
- ▶ M verwendet Nichtdeterminismus, um Belegung zu „raten“:

$$I : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$$

- ▶ Jede der 2^n nicht deterministischen Berechnungen berechnet Wert von $I(F)$.

Lemma

SAT $\in \mathcal{NP}$.

Beweis:

- ▶ Konstruiere eine NTM M mit $code(F)$ als Eingabe.
- ▶ M berechnet, welche Variablen in F vorkommen. Seien diese $\{x_1, \dots, x_n\}$.
- ▶ M verwendet Nichtdeterminismus, um Belegung zu „raten“:

$$I : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$$

- ▶ Jede der 2^n nicht deterministischen Berechnungen berechnet Wert von $I(F)$.
- ▶ Akzeptanz bei 1, sonst verwerfen.

Lemma

SAT $\in \mathcal{NP}$.

Beweis:

- ▶ Konstruiere eine NTM M mit $code(F)$ als Eingabe.
- ▶ M berechnet, welche Variablen in F vorkommen. Seien diese $\{x_1, \dots, x_n\}$.
- ▶ M verwendet Nichtdeterminismus, um Belegung zu „raten“:

$$I : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$$

- ▶ Jede der 2^n nicht deterministischen Berechnungen berechnet Wert von $I(F)$.
- ▶ Akzeptanz bei 1, sonst verwerfen.
- ▶ Da jede Belegung geprüft wird, gilt:

M akzeptiert eine Formel F g.d.w. $code(F) \in \text{SAT}$

Lemma

SAT $\in \mathcal{NP}$.

Beweis:

- ▶ Konstruiere eine NTM M mit $code(F)$ als Eingabe.
- ▶ M berechnet, welche Variablen in F vorkommen. Seien diese $\{x_1, \dots, x_n\}$.
- ▶ M verwendet Nichtdeterminismus, um Belegung zu „raten“:

$$I : \{x_1, \dots, x_n\} \rightarrow \{0, 1\}$$

- ▶ Jede der 2^n nicht deterministischen Berechnungen berechnet Wert von $I(F)$.
- ▶ Akzeptanz bei 1, sonst verwerfen.
- ▶ Da jede Belegung geprüft wird, gilt:

M akzeptiert eine Formel F g.d.w. $code(F) \in \text{SAT}$

- ▶ Jeder Berechnungspfad von M läuft in Polynomialzeit in $|code(F)|$, da die Anzahl der Variablen durch die Eingabegröße beschränkt ist. □

\mathcal{NP} = Polynomiell verifizierbar

Nachweis, dass Sprache in \mathcal{NP} liegt, geht oft so wie bei SAT:

- ▶ Verwende Nichtdeterminismus, um potentielle Lösung zu raten.
- ▶ Zeige, dass eine Lösung in Polynomialzeit verifiziert werden kann.

Hilfssatz für den \mathcal{NP} -Schwere-Beweis von SAT

Lemma

Für aussagenlogische Variablen $\{x_1, \dots, x_n\}$ gibt es eine aussagenlogische Formel $exactlyOne(x_1, \dots, x_n)$, sodass

$I(exactlyOne(x_1, \dots, x_n)) = 1$ g.d.w. I setzt genau eine der Variablen x_i auf 1
und alle anderen auf 0

Dabei ist die Größe der Formel $exactlyOne(x_1, \dots, x_n)$ in $O(n^2)$.

Hilfssatz für den \mathcal{NP} -Schwere-Beweis von SAT

Lemma

Für aussagenlogische Variablen $\{x_1, \dots, x_n\}$ gibt es eine aussagenlogische Formel $exactlyOne(x_1, \dots, x_n)$, sodass

$I(exactlyOne(x_1, \dots, x_n)) = 1$ g.d.w. I setzt genau eine der Variablen x_i auf 1 und alle anderen auf 0

Dabei ist die Größe der Formel $exactlyOne(x_1, \dots, x_n)$ in $O(n^2)$.

Beweis:

$$exactlyOne(x_1, \dots, x_n) := (x_1 \vee \dots \vee x_n) \wedge \bigwedge_{1 \leq i < j \leq n} \neg(x_i \wedge x_j)$$

- ▶ $(x_1 \vee \dots \vee x_n)$ sichert $atLeastOne(x_1, \dots, x_n)$ zu.
- ▶ $\bigwedge_{1 \leq i < j \leq n} \neg(x_i \wedge x_j)$ sichert $atMostOne(x_1, \dots, x_n)$ zu. □

\mathcal{NP} -Schwere von SAT: Idee

- ▶ Wir müssen zeigen:

$$L \leq_p \text{SAT für alle } L \in \mathcal{NP}$$

\mathcal{NP} -Schwere von SAT: Idee

- ▶ Wir müssen zeigen:

$$L \leq_p \text{SAT für alle } L \in \mathcal{NP}$$

- ▶ Da $L \in \mathcal{NP}$, gibt es polynomiell zeitbeschränkte NTM M , die L akzeptiert.

\mathcal{NP} -Schwere von SAT: Idee

- ▶ Wir müssen zeigen:

$$L \leq_p \text{SAT für alle } L \in \mathcal{NP}$$

- ▶ Da $L \in \mathcal{NP}$, gibt es polynomiell zeitbeschränkte NTM M , die L akzeptiert.
- ▶ Für Wort w erstelle Formel $f(w) = F$ (in determ. Polynomialzeit), sodass gilt:
 F ist erfüllbar g.d.w. M akzeptiert w

\mathcal{NP} -Schwere von SAT: Idee

- ▶ Wir müssen zeigen:

$$L \leq_p \text{SAT für alle } L \in \mathcal{NP}$$

- ▶ Da $L \in \mathcal{NP}$, gibt es polynomiell zeitbeschränkte NTM M , die L akzeptiert.
- ▶ Für Wort w erstelle Formel $f(w) = F$ (in determ. Polynomialzeit), sodass gilt:
 F ist erfüllbar g.d.w. M akzeptiert w
- ▶ Da die Laufzeit von M polynomiell beschränkt ist, beschränkt dies auch die Größe der Formel.

SAT ist \mathcal{NP} -schwer (1)

Lemma

SAT ist \mathcal{NP} -schwer.

SAT ist \mathcal{NP} -schwer (1)

Lemma

SAT ist \mathcal{NP} -schwer.

Beweis: Wir müssen zeigen: $L \leq_p \text{SAT}$

- ▶ Sei $L \in \mathcal{NP}$ beliebig.
- ▶ Sei M eine NTM mit $L(M) = L$, w eine Eingabe für M und $\text{ntime}_M(w) \leq p(|w|)$.

SAT ist \mathcal{NP} -schwer (1)

Lemma

SAT ist \mathcal{NP} -schwer.

Beweis: Wir müssen zeigen: $L \leq_p \text{SAT}$

- ▶ Sei $L \in \mathcal{NP}$ beliebig.
- ▶ Sei M eine NTM mit $L(M) = L$, w eine Eingabe für M und $\text{ntime}_M(w) \leq p(|w|)$.

Ziel: Konstruiere aussagenlogische Formel F , sodass gilt

$$w \in L \iff F \text{ ist erfüllbar}$$

Dabei muss F in Polynomialzeit konstruierbar sein.

D.h. wir geben eine in Polynomialzeit berechenbare Funktion $f(w)$ an, sodass

$$w \in L \iff f(w) \in \text{SAT}.$$

SAT ist \mathcal{NP} -schwer (2)

Notation:

Eingabe: $w = a_1 \cdots a_n \in \Sigma^*$

Bandalphabet: $\Gamma = \{b_1, \dots, b_\ell\}$

Zustände: $Z = \{z_0, \dots, z_k\}$

Startzustand: z_0

SAT ist \mathcal{NP} -schwer (2)

Eingabe: $w = a_1 \cdots a_n \in \Sigma^*$

Bandalphabet: $\Gamma = \{b_1, \dots, b_\ell\}$

Zustände: $Z = \{z_0, \dots, z_k\}$

Startzustand: z_0

SAT ist \mathcal{NP} -schwer (2)

Eingabe: $w = a_1 \cdots a_n \in \Sigma^*$
Bandalphabet: $\Gamma = \{b_1, \dots, b_\ell\}$
Zustände: $Z = \{z_0, \dots, z_k\}$
Startzustand: z_0

Aussagenlogische Variablen in der Formel F :

Variable	Index-Bereich	Bedeutung
$State_{t,z}$	$t = 0, 1, \dots, p(n)$ $z = z_0, \dots, z_k$	$State_{t,z} = 1$ g.d.w. nach t Schritten ist M im Zustand z .
$Pos_{t,i}$	$t = 0, 1, \dots, p(n)$ $i = -p(n), \dots, p(n)$	$Pos_{t,i} = 1$ g.d.w. nach t Schritten ist der Schreib-Lesekopf auf Position i
$Tape_{t,i,b}$	$t = 0, 1, \dots, p(n)$ $i = -p(n), \dots, p(n)$ $b = b_1, \dots, b_\ell$	$Tape_{t,i,b} = 1$ g.d.w. nach t Schritten steht in Position i das Zeichen b

SAT ist \mathcal{NP} -schwer (2)

Eingabe: $w = a_1 \cdots a_n \in \Sigma^*$
Bandalphabet: $\Gamma = \{b_1, \dots, b_\ell\}$
Zustände: $Z = \{z_0, \dots, z_k\}$
Startzustand: z_0

Aussagenlogische Variablen in der Formel F :

Variable	Index-Bereich	Bedeutung
$State_{t,z}$	$t = 0, 1, \dots, p(n)$ $z = z_0, \dots, z_k$	$State_{t,z} = 1$ g.d.w. nach t Schritten ist M im Zustand z .
$Pos_{t,i}$	$t = 0, 1, \dots, p(n)$ $i = -p(n), \dots, p(n)$	$Pos_{t,i} = 1$ g.d.w. nach t Schritten ist der Schreib-Lesekopf auf Position i
$Tape_{t,i,b}$	$t = 0, 1, \dots, p(n)$ $i = -p(n), \dots, p(n)$ $b = b_1, \dots, b_\ell$	$Tape_{t,i,b} = 1$ g.d.w. nach t Schritten steht in Position i das Zeichen b

- ▶ Bandpositionen: Position 0 am Anfang
- ▶ Bereiche reichen aus, da die TM nicht mehr als $p(n)$ Schritte macht

SAT ist \mathcal{NP} -schwer (3)

Aufbau der Formel F :

$$F = \text{Rand} \wedge \text{Anfang} \wedge \text{Übergang} \wedge \text{Ende}$$

- ▶ *Rand*: Randbedingungen
- ▶ *Anfang*: Anfangsbedingungen
- ▶ *Übergang*: Bedingungen für den Zustandsübergang
- ▶ *Ende*: Endbedingung

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k})$$

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k})$$

- ▶ ... ist der Kopf von M in genau einer Position auf dem Band:

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k})$$

- ▶ ... ist der Kopf von M in genau einer Position auf dem Band:

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{Pos}_{t, -p(n)}, \dots, \text{Pos}_{t, p(n)})$$

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k})$$

- ▶ ... ist der Kopf von M in genau einer Position auf dem Band:

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{Pos}_{t, -p(n)}, \dots, \text{Pos}_{t, p(n)})$$

- ▶ ... befindet sich in jeder Bandzelle genau ein Symbol aus Γ :

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k})$$

- ▶ ... ist der Kopf von M in genau einer Position auf dem Band:

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{Pos}_{t, -p(n)}, \dots, \text{Pos}_{t, p(n)})$$

- ▶ ... befindet sich in jeder Bandzelle genau ein Symbol aus Γ :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \bigwedge_{i \in \{-p(n), \dots, p(n)\}} \text{exactlyOne}(\text{Tape}_{t, i, b_1}, \dots, \text{Tape}_{t, i, b_\ell})$$

SAT ist \mathcal{NP} -schwer (4)

Randbedingungen:

Zu jedem Zeitpunkt t :

- ▶ ... ist M in genau einem Zustand z :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k})$$

- ▶ ... ist der Kopf von M in genau einer Position auf dem Band:

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \text{exactlyOne}(\text{Pos}_{t, -p(n)}, \dots, \text{Pos}_{t, p(n)})$$

- ▶ ... befindet sich in jeder Bandzelle genau ein Symbol aus Γ :

$$\bigwedge_{t \in \{0, \dots, p(n)\}} \bigwedge_{i \in \{-p(n), \dots, p(n)\}} \text{exactlyOne}(\text{Tape}_{t, i, b_1}, \dots, \text{Tape}_{t, i, b_\ell})$$

Daher:

$$\text{Rand} := \bigwedge_{t \in \{0, \dots, p(n)\}} \left(\begin{array}{l} \text{exactlyOne}(\text{State}_{t, z_0}, \dots, \text{State}_{t, z_k}) \\ \bigwedge \text{exactlyOne}(\text{Pos}_{t, -p(n)}, \dots, \text{Pos}_{t, p(n)}) \\ \bigwedge_{i \in \{-p(n), \dots, p(n)\}} \text{exactlyOne}(\text{Tape}_{t, i, b_1}, \dots, \text{Tape}_{t, i, b_\ell}) \end{array} \right)$$

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand:

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand: $State_{0,z_0}$

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand: $State_{0,z_0}$
- ▶ Der Schreib-Lesekopf ist auf Position 0:

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand: $State_{0,z_0}$
- ▶ Der Schreib-Lesekopf ist auf Position 0: $Pos_{0,0}$

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand: $State_{0,z_0}$
- ▶ Der Schreib-Lesekopf ist auf Position 0: $Pos_{0,0}$
- ▶ Die Eingabe $w = a_1 \dots a_n$ steht auf dem Band und alle anderen Zellen enthalten das Blank-Symbol:

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand: $State_{0,z_0}$
- ▶ Der Schreib-Lesekopf ist auf Position 0: $Pos_{0,0}$
- ▶ Die Eingabe $w = a_1 \dots a_n$ steht auf dem Band und alle anderen Zellen enthalten das Blank-Symbol:

$$\left(\bigwedge_{i \in \{0, \dots, n-1\}} Tape_{0,i,a_{i+1}} \right) \wedge \left(\bigwedge_{i \in \{-p(n), \dots, -1\}} Tape_{0,i,\square} \right) \wedge \left(\bigwedge_{i \in \{n, \dots, p(n)\}} Tape_{0,i,\square} \right)$$

SAT ist \mathcal{NP} -schwer (5)

Anfangsbedingungen:

Fixieren die Bedingungen zum Zeitpunkt $t = 0$:

- ▶ M ist im Startzustand: $State_{0,z_0}$
- ▶ Der Schreib-Lesekopf ist auf Position 0: $Pos_{0,0}$
- ▶ Die Eingabe $w = a_1 \dots a_n$ steht auf dem Band und alle anderen Zellen enthalten das Blank-Symbol:

$$\left(\bigwedge_{i \in \{0, \dots, n-1\}} Tape_{0,i,a_{i+1}} \right) \wedge \left(\bigwedge_{i \in \{-p(n), \dots, -1\}} Tape_{0,i,\square} \right) \wedge \left(\bigwedge_{i \in \{n, \dots, p(n)\}} Tape_{0,i,\square} \right)$$

Daher:

$$Anfang := State_{0,z_0} \wedge Pos_{0,0} \wedge \left(\bigwedge_{i \in \{0, \dots, n-1\}} Tape_{0,i,a_{i+1}} \right) \wedge \left(\bigwedge_{i \in \{-p(n), \dots, -1\}} Tape_{0,i,\square} \right) \wedge \left(\bigwedge_{i \in \{n, \dots, p(n)\}} Tape_{0,i,\square} \right)$$

SAT ist \mathcal{NP} -schwer (6)

Übergangsbedingungen:

SAT ist \mathcal{NP} -schwer (6)

Übergangsbedingungen:

- ▶ Für Übergang von t zu $t + 1$: Zustand, Bandinhalt, Position ändern.
Sei $dir(N) = 0$, $dir(L) = -1$, $dir(R) = 1$.

SAT ist \mathcal{NP} -schwer (6)

Übergangsbedingungen:

- Für Übergang von t zu $t + 1$: Zustand, Bandinhalt, Position ändern.
Sei $dir(N) = 0$, $dir(L) = -1$, $dir(R) = 1$.

$$\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, z \in Z, \\ i \in \{-p(n)+1, \dots, p(n)-1\}, b \in \Gamma}} \left(\left(State_{t,z} \wedge Pos_{t,i} \wedge Tape_{t,i,b} \right) \right. \\ \left. \implies \bigvee_{(z', b', y) \in \delta(z, b)} \left(State_{t+1, z'} \wedge Pos_{t+1, i+dir(y)} \wedge Tape_{t+1, i, b'} \right) \right)$$

SAT ist \mathcal{NP} -schwer (6)

Übergangsbedingungen:

- ▶ Für Übergang von t zu $t + 1$: Zustand, Bandinhalt, Position ändern.
Sei $dir(N) = 0$, $dir(L) = -1$, $dir(R) = 1$.

$$\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, z \in Z, \\ i \in \{-p(n)+1, \dots, p(n)-1\}, b \in \Gamma}} \left(\left(State_{t,z} \wedge Pos_{t,i} \wedge Tape_{t,i,b} \right) \implies \bigvee_{(z', b', y) \in \delta(z,b)} \left(State_{t+1,z'} \wedge Pos_{t+1,i+dir(y)} \wedge Tape_{t+1,i,b'} \right) \right)$$

- ▶ Zellen auf denen der Kopf nicht steht, bleiben unverändert.

SAT ist \mathcal{NP} -schwer (6)

Übergangsbedingungen:

- Für Übergang von t zu $t + 1$: Zustand, Bandinhalt, Position ändern.
Sei $dir(N) = 0$, $dir(L) = -1$, $dir(R) = 1$.

$$\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, z \in Z, \\ i \in \{-p(n)+1, \dots, p(n)-1\}, b \in \Gamma}} \left(\left(State_{t,z} \wedge Pos_{t,i} \wedge Tape_{t,i,b} \right) \implies \bigvee_{(z', b', y) \in \delta(z,b)} \left(State_{t+1,z'} \wedge Pos_{t+1,i+dir(y)} \wedge Tape_{t+1,i,b'} \right) \right)$$

- Zellen auf denen der Kopf nicht steht, bleiben unverändert.

$$\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, \\ i \in \{-p(n), \dots, p(n)\}, \\ b \in \Gamma}} \left((\neg Pos_{t,i} \wedge Tape_{t,i,b}) \implies Tape_{t+1,i,b} \right)$$

SAT ist \mathcal{NP} -schwer (7)

Übergangsbedingungen:

Ergibt zusammen:

$$\begin{aligned} \text{Übergang} := & \\ & \left(\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, \\ z \in Z, \\ i \in \{-p(n)+1, \dots, p(n)-1\}, \\ b \in \Gamma}} \left((State_{t,z} \wedge Pos_{t,i} \wedge Tape_{t,i,b}) \right. \right. \\ & \left. \left. \implies \bigvee_{(z',b',y) \in \delta(z,b)} (State_{t+1,z'} \wedge Pos_{t+1,i+dir(y)} \wedge Tape_{t+1,i,b'}) \right) \right) \\ & \wedge \left(\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, \\ i \in \{-p(n), \dots, p(n)\}, \\ b \in \Gamma}} ((\neg Pos_{t,i} \wedge Tape_{t,i,b}) \implies Tape_{t+1,i,b}) \right) \end{aligned}$$

SAT ist \mathcal{NP} -schwer (8)

Endbedingung: Ein akzeptierender Zustand wird erreicht:

SAT ist \mathcal{NP} -schwer (8)

Endbedingung: Ein akzeptierender Zustand wird erreicht:

$$Ende := \bigvee_{z \in E, t \in \{0, \dots, p(n)\}} State_{t,z}$$

SAT ist \mathcal{NP} -schwer (9)

$$\begin{aligned}
 F := & \bigwedge_{t \in \{0, \dots, p(n)\}} \left(\begin{array}{l} \text{exactlyOne}(\text{State}_{t,z_0}, \dots, \text{State}_{t,z_k}) \\ \wedge \text{exactlyOne}(\text{Pos}_{t,-p(n)}, \dots, \text{Pos}_{t,p(n)}) \\ \wedge \bigwedge_{i \in \{-p(n), \dots, p(n)\}} \text{exactlyOne}(\text{Tape}_{t,i,b_1}, \dots, \text{Tape}_{t,i,b_\ell}) \end{array} \right) \\
 & \wedge \text{State}_{0,z_0} \wedge \text{Pos}_{0,0} \wedge \left(\bigwedge_{i \in \{0, \dots, n-1\}} \text{Tape}_{0,i,a_{i+1}} \right) \wedge \left(\bigwedge_{i \in \{-p(n), \dots, -1\}} \text{Tape}_{0,i,\square} \right) \wedge \left(\bigwedge_{i \in \{n, \dots, p(n)\}} \text{Tape}_{0,i,\square} \right) \\
 & \wedge \left(\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, \\ z \in Z, \\ i \in \{-p(n)+1, \dots, p(n)-1\}, \\ b \in \Gamma}} \left(\begin{array}{l} (\text{State}_{t,z} \wedge \text{Pos}_{t,i} \wedge \text{Tape}_{t,i,b}) \\ \implies \bigvee_{(z',b',y) \in \delta(z,b)} (\text{State}_{t+1,z'} \wedge \text{Pos}_{t+1,i+\text{dir}(y)} \wedge \text{Tape}_{t+1,i,b'}) \end{array} \right) \right) \\
 & \wedge \left(\bigwedge_{\substack{t \in \{0, \dots, p(n)-1\}, \\ i \in \{-p(n), \dots, p(n)\}, \\ b \in \Gamma}} \left((\neg \text{Pos}_{t,i} \wedge \text{Tape}_{t,i,b}) \implies \text{Tape}_{t+1,i,b} \right) \right) \\
 & \wedge \bigvee_{z \in E, t \in \{0, \dots, p(n)\}} \text{State}_{t,z}
 \end{aligned}$$

SAT ist \mathcal{NP} -schwer (10)

- ▶ Wenn $w \in L$, dann $z_0 w \vdash_M^r uz_e v$ mit $z_e \in E$ und $r \leq p(n)$.
- ▶ Lauf liefert Belegung I der Variablen von F , sodass $I(F) = 1$.
- ▶ Umgekehrt: Wenn es eine erfüllende Belegung I gibt mit $I(F) = 1$, dann kann daraus ein akzeptierender Lauf für die TM auf Eingabe w konstruiert werden.
- ▶ Damit gilt $w \in L \iff F$ ist erfüllbar.

SAT ist \mathcal{NP} -schwer (10)

- ▶ Wenn $w \in L$, dann $z_0 w \vdash_M^r uz_e v$ mit $z_e \in E$ und $r \leq p(n)$.
- ▶ Lauf liefert Belegung I der Variablen von F , sodass $I(F) = 1$.
- ▶ Umgekehrt: Wenn es eine erfüllende Belegung I gibt mit $I(F) = 1$, dann kann daraus ein akzeptierender Lauf für die TM auf Eingabe w konstruiert werden.
- ▶ Damit gilt $w \in L \iff F$ ist erfüllbar.
- ▶ F kann in (deterministischer) Polynomialzeit berechnet werden:

Größe von F : (Anzahl an Variablenvorkommen):

Subformel	Größe
<i>Rand</i> :	$O(p(n)^3)$
<i>Anfang</i> :	$O(p(n))$
<i>Übergang</i> :	$O(p(n)^2)$
<i>Ende</i> :	$O(p(n))$
F	$O(p(n)^3)$



Insgesamt haben wir damit gezeigt:

Satz von Cook

Das Erfüllbarkeitsproblem der Aussagenlogik ist \mathcal{NP} -vollständig.