

# Berechenbarkeit

## Vorlesung 12: NP-Vollständigkeit

10. Juli 2025

# Termine — Modul Berechenbarkeit

---

ÜBUNGEN	PRÜFUNG	VORLESUNG
8.7. Abschlussübung beide Wochen	9.7. _____	10.7. NP-Vollständigkeit
15.7. _____	16.7. Prüfung ab 13:30 Uhr in AudiMax & Hs. 9	17.7. _____

# NP-Vollständigkeit

---

Definition (§11.7 *nondeterministically polynomially decidable*)

Problem  $L \subseteq \Sigma^*$  **nichtdeterministisch polynomiell entscheidbar** falls Alphabet  $\Gamma$ , Relation  $R \subseteq \Sigma^* \times \Gamma^*$  und  $k \in \mathbb{N}$  existieren mit

- $\{w\#z \mid (w, z) \in R\} \in \mathbf{P}$  polynomiell entscheidbar und
- $w \in L$  gdw.  $(w, z) \in R$  existiert mit  $|z| \leq |w|^k$  für alle  $w \in \Sigma^*$

# NP-Vollständigkeit

---

Definition (§11.7 *nondeterministically polynomially decidable*)

Problem  $L \subseteq \Sigma^*$  **nichtdeterministisch polynomiell entscheidbar** falls Alphabet  $\Gamma$ , Relation  $R \subseteq \Sigma^* \times \Gamma^*$  und  $k \in \mathbb{N}$  existieren mit

- $\{w\#z \mid (w, z) \in R\} \in \mathbf{P}$  polynomiell entscheidbar und
- $w \in L$  gdw.  $(w, z) \in R$  existiert mit  $|z| \leq |w|^k$  für alle  $w \in \Sigma^*$

## Komplexitätsklassen

$\mathbf{P} = \{L \mid L \text{ ist polynomiell entscheidbar}\}$

$\mathbf{NP} = \{L \mid L \text{ ist nichtdeterministisch polynomiell entscheidbar}\}$

# Determinismus vs. Nichtdeterminismus

---

$P \subseteq NP$  gilt, aber

Beweis  $NP \subseteq P$  oder  $P \subsetneq NP$  1 Million USD wert

- Wichtigstes Problem der theoretischen Informatik
- 1 der 7 Millenniumprobleme der Mathematik

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextsensitiver Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextsensitiver Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextsensitiver Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextsensitiver Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
  
- Entscheidbarkeit von  $L(G)$

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextsensitiver Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextsensitiver Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
  
- Entscheidbarkeit von  $L(G)$  **entscheidbar**
- Polynomielle Entscheidbarkeit von  $L(G)$



# Polynomielle Berechenbarkeit

---

## Wortproblem kontextsensitiver Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextsensitiver Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
- Entscheidbarkeit von  $L(G)$  **entscheidbar**
- Polynomielle Entscheidbarkeit von  $L(G)$  **unklar**
- Nichtdet. polynomielle Entscheidbarkeit von  $L(G)$

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextsensitiver Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextsensitiver Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
- Entscheidbarkeit von  $L(G)$  **entscheidbar**
- Polynomielle Entscheidbarkeit von  $L(G)$  **unklar**
- Nichtdet. polynomielle Entscheidbarkeit von  $L(G)$  **unklar**

# Polynomielle Berechenbarkeit

---

Sei  $G = (N, \Sigma, S, P)$  kontextsensitive Grammatik

1. Setze  $\mathcal{F} = \{S\}$  (nur Startsymbol)

# Polynomielle Berechenbarkeit

---

Sei  $G = (N, \Sigma, S, P)$  kontextsensitive Grammatik

1. Setze  $\mathcal{F} = \{S\}$  (nur Startsymbol)
2. Setze  $\mathcal{F}' = \mathcal{F} \cup \{v \in (N \cup \Sigma)^{\leq |w|} \mid \exists u \in \mathcal{F}: u \Rightarrow_G v\}$   
(füge Nachfolger der Länge höchstens  $|w|$  hinzu)

# Polynomielle Berechenbarkeit

---

Sei  $G = (N, \Sigma, S, P)$  kontextsensitive Grammatik

1. Setze  $\mathcal{F} = \{S\}$  (nur Startsymbol)
2. Setze  $\mathcal{F}' = \mathcal{F} \cup \{v \in (N \cup \Sigma)^{\leq |w|} \mid \exists u \in \mathcal{F}: u \Rightarrow_G v\}$   
(füge Nachfolger der Länge höchstens  $|w|$  hinzu)
3. Falls  $\mathcal{F} \subsetneq \mathcal{F}'$ , dann setze  $\mathcal{F} = \mathcal{F}'$  und gehe zu 2.

# Polynomielle Berechenbarkeit

---

Sei  $G = (N, \Sigma, S, P)$  kontextsensitive Grammatik

1. Setze  $\mathcal{F} = \{S\}$  (nur Startsymbol)
2. Setze  $\mathcal{F}' = \mathcal{F} \cup \{v \in (N \cup \Sigma)^{\leq |w|} \mid \exists u \in \mathcal{F}: u \Rightarrow_G v\}$   
(füge Nachfolger der Länge höchstens  $|w|$  hinzu)
3. Falls  $\mathcal{F} \subsetneq \mathcal{F}'$ , dann setze  $\mathcal{F} = \mathcal{F}'$  und gehe zu 2.
4. Liefere Wahrheitswert von  $w \in \mathcal{F}'$

# Polynomielle Berechenbarkeit

---

Sei  $G = (N, \Sigma, S, P)$  kontextsensitive Grammatik

1. Setze  $\mathcal{F} = \{S\}$  (nur Startsymbol)
2. Setze  $\mathcal{F}' = \mathcal{F} \cup \{v \in (N \cup \Sigma)^{\leq |w|} \mid \exists u \in \mathcal{F}: u \Rightarrow_G v\}$   
(füge Nachfolger der Länge höchstens  $|w|$  hinzu)
3. Falls  $\mathcal{F} \subsetneq \mathcal{F}'$ , dann setze  $\mathcal{F} = \mathcal{F}'$  und gehe zu 2.
4. Liefere Wahrheitswert von  $w \in \mathcal{F}'$

## Komplexität

- Potentiell  $\sum_{i=0}^{|w|} (|N| + |\Sigma|)^i$  Elemente; exponentiell

# Polynomielle Berechenbarkeit

---

Sei  $G = (N, \Sigma, S, P)$  kontextsensitive Grammatik

1. Setze  $\mathcal{F} = \{S\}$  (nur Startsymbol)
2. Setze  $\mathcal{F}' = \mathcal{F} \cup \{v \in (N \cup \Sigma)^{\leq |w|} \mid \exists u \in \mathcal{F}: u \Rightarrow_G v\}$   
(füge Nachfolger der Länge höchstens  $|w|$  hinzu)
3. Falls  $\mathcal{F} \subsetneq \mathcal{F}'$ , dann setze  $\mathcal{F} = \mathcal{F}'$  und gehe zu 2.
4. Liefere Wahrheitswert von  $w \in \mathcal{F}'$

## Komplexität

- Potentiell  $\sum_{i=0}^{|w|} (|N| + |\Sigma|)^i$  Elemente; exponentiell
- Ableitung als Zertifikat potentiell zu lang



# Polynomielle Berechenbarkeit

---

## Wortproblem kontextfreier Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextfreier Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextfreier Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextfreier Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
  
- Entscheidbarkeit von  $L(G)$

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextfreier Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextfreier Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
- Entscheidbarkeit von  $L(G)$  **entscheidbar**
- Polynomielle Entscheidbarkeit von  $L(G)$

# Polynomielle Berechenbarkeit

---

## Wortproblem kontextfreier Sprache

- Ist geg.  $w \in \Sigma^*$  in Sprache  $L(G)$   
kontextfreier Grammatik  $G = (N, \Sigma, S, P)$ ?
- Problem  $L(G)$
- Entscheidbarkeit von  $L(G)$  **entscheidbar**
- Polynomielle Entscheidbarkeit von  $L(G)$  **in P**
- CYK-Algorithmus  $\mathcal{O}(|w|^3)$

# Polynomielle Berechenbarkeit

---

## Problem des Handelsreisenden

- Hat geg. Distanzmatrix  $D \in \mathbb{N}^{n \times n}$   
Rundreise der Länge höchstens  $k$ ?
- Problem  $\text{TSP} = \{\langle D, k \rangle \mid D \text{ hat Rundreise der Länge höchstens } k\}$

# Polynomielle Berechenbarkeit

---

## Problem des Handelsreisenden

- Hat geg. Distanzmatrix  $D \in \mathbb{N}^{n \times n}$   
Rundreise der Länge höchstens  $k$ ?
- Problem  $TSP = \{\langle D, k \rangle \mid D \text{ hat Rundreise der Länge höchstens } k\}$
- Entscheidbarkeit von  $TSP$

# Polynomielle Berechenbarkeit

---

## Problem des Handelsreisenden

- Hat geg. Distanzmatrix  $D \in \mathbb{N}^{n \times n}$   
Rundreise der Länge höchstens  $k$ ?
- Problem  $TSP = \{\langle D, k \rangle \mid D \text{ hat Rundreise der Länge höchstens } k\}$
- Entscheidbarkeit von  $TSP$     **entscheidbar**
- Polynomielle Entscheidbarkeit von  $TSP$

# Polynomielle Berechenbarkeit

---

## Problem des Handelsreisenden

- Hat geg. Distanzmatrix  $D \in \mathbb{N}^{n \times n}$   
Rundreise der Länge höchstens  $k$ ?
- Problem  $TSP = \{\langle D, k \rangle \mid D \text{ hat Rundreise der Länge höchstens } k\}$
- Entscheidbarkeit von  $TSP$     **entscheidbar**
- Polynomielle Entscheidbarkeit von  $TSP$     **unklar**
- Nichtdet. polynomielle Entscheidbarkeit von  $TSP$



# Polynomielle Berechenbarkeit

---

## Problem des Handelsreisenden

- Hat geg. Distanzmatrix  $D \in \mathbb{N}^{n \times n}$   
Rundreise der Länge höchstens  $k$ ?
- Problem  $TSP = \{\langle D, k \rangle \mid D \text{ hat Rundreise der Länge höchstens } k\}$
- Entscheidbarkeit von  $TSP$     **entscheidbar**
- Polynomielle Entscheidbarkeit von  $TSP$     **unklar**
- Nichtdet. polynomielle Entscheidbarkeit von  $TSP$     **ja, in NP**

# Polynomielle Berechenbarkeit

---

## Problem des Handelsreisenden

- Hat geg. Distanzmatrix  $D \in \mathbb{N}^{n \times n}$   
Rundreise der Länge höchstens  $k$ ?
- Problem  $TSP = \{\langle D, k \rangle \mid D \text{ hat Rundreise der Länge höchstens } k\}$
- Entscheidbarkeit von  $TSP$     **entscheidbar**
- Polynomielle Entscheidbarkeit von  $TSP$     **unklar**
- Nichtdet. polynomielle Entscheidbarkeit von  $TSP$     **ja, in NP**
- Zertifikat ist Rundreise der Länge höchstens  $k$

# Polynomielle Problemreduktion

---

## §12.1 Definition (polynomielle Reduktion; *polynomial reduction*)

Problem  $L \subseteq \Sigma^*$  **polynomiell reduzierbar** auf  $L' \subseteq \Gamma^*$ , kurz  $L \preceq_p L'$ , falls polyn. ber. totale Funktion  $f: \Sigma^* \rightarrow \Gamma^*$  mit  $L = f^{-1}(L')$  existiert

# Polynomielle Problemreduktion

---

## §12.1 Definition (polynomielle Reduktion; *polynomial reduction*)

Problem  $L \subseteq \Sigma^*$  **polynomiell reduzierbar** auf  $L' \subseteq \Gamma^*$ , kurz  $L \preceq_P L'$ , falls polyn. ber. totale Funktion  $f: \Sigma^* \rightarrow \Gamma^*$  mit  $L = f^{-1}(L')$  existiert

### Konsequenzen

- Seien  $L \subseteq \Sigma^*$  und  $L' \subseteq \Gamma^*$  mit  $L \preceq_P L'$
- $L$  polynomiell entscheidbar falls  $L'$  polynomiell entscheidbar  
( $L \in \mathbf{P}$  falls  $L' \in \mathbf{P}$ )

# Polynomielle Problemreduktion

## §12.1 Definition (polynomielle Reduktion; *polynomial reduction*)

Problem  $L \subseteq \Sigma^*$  **polynomiell reduzierbar** auf  $L' \subseteq \Gamma^*$ , kurz  $L \preceq_P L'$ , falls polyn. ber. totale Funktion  $f: \Sigma^* \rightarrow \Gamma^*$  mit  $L = f^{-1}(L')$  existiert

### Konsequenzen

- Seien  $L \subseteq \Sigma^*$  und  $L' \subseteq \Gamma^*$  mit  $L \preceq_P L'$
- $L$  polynomiell entscheidbar falls  $L'$  polynomiell entscheidbar  
( $L \in \mathbf{P}$  falls  $L' \in \mathbf{P}$ )
- $L$  nichtdet. polyn. entscheidbar  
falls  $L'$  nichtdet. polyn. entscheidbar  
( $L \in \mathbf{NP}$  falls  $L' \in \mathbf{NP}$ )

# Polynomielle Problemreduktion

---

## Problem

- Keine untere Schranke per Reduktion
- Wie erhalten wir untere Schranken?

## Stephen Arthur Cook (\* 1939)

- Amer.-kan. Mathematiker & Informatiker
- Polynomielle Reduktion & **NP**-Vollständigkeit
- Turing-Preisträger



© Jiří Janíček

# NP-Schwere & NP-Vollständigkeit

---

## §12.2 Definition (**NP**-schwer, -vollständig; *NP-hard*, -complete)

Problem  $L$

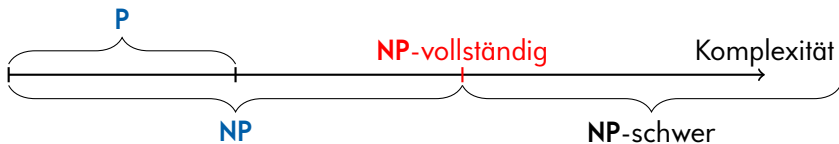
- **NP-schwer** falls  $L' \preceq_p L$  für alle  $L' \in \mathbf{NP}$

# NP-Schwere & NP-Vollständigkeit

## §12.2 Definition (NP-schwer, -vollständig; NP-hard, -complete)

Problem  $L$

- **NP-schwer** falls  $L' \preceq_P L$  für alle  $L' \in \mathbf{NP}$
- **NP-vollständig** falls  $L$  **NP-schwer** und  $L \in \mathbf{NP}$



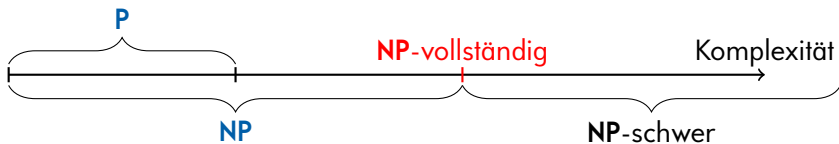


# NP-Schwere & NP-Vollständigkeit

## §12.2 Definition (NP-schwer, -vollständig; NP-hard, -complete)

Problem  $L$

- **NP-schwer** falls  $L' \preceq_P L$  für alle  $L' \in \text{NP}$
- **NP-vollständig** falls  $L$  NP-schwer und  $L \in \text{NP}$



Notizen

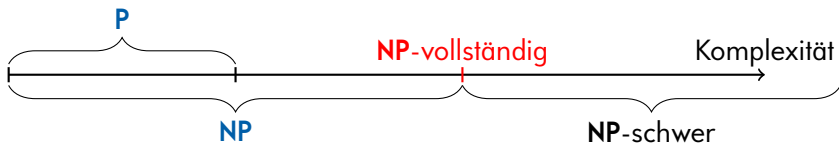
- **NP-schwer** = mind. so schwer wie alle Probleme in **NP**  
(untere Schranke)

# NP-Schwere & NP-Vollständigkeit

## §12.2 Definition (NP-schwer, -vollständig; NP-hard, -complete)

Problem  $L$

- **NP-schwer** falls  $L' \preceq_P L$  für alle  $L' \in \mathbf{NP}$
- **NP-vollständig** falls  $L$  NP-schwer und  $L \in \mathbf{NP}$



Notizen

- **NP-schwer** = mind. so schwer wie alle Probleme in **NP**  
(untere Schranke)
- **NP-vollständig** = passende untere & obere Schranke **NP**

# NP-Schwere & NP-Vollständigkeit

---

## §12.3 Theorem

Sei  $L$  NP-vollständig. Dann  $L \in P$  gdw.  $P = NP$

# NP-Schwere & NP-Vollständigkeit

---

## §12.3 Theorem

Sei  $L$  NP-vollständig. Dann  $L \in P$  gdw.  $P = NP$

### Beweis

Falls  $P = NP$ , dann  $L \in P = NP$ , da  $L \in NP$  (da NP-vollständig).

# NP-Schwere & NP-Vollständigkeit

## §12.3 Theorem

Sei  $L$  **NP**-vollständig. Dann  $L \in \mathbf{P}$  gdw.  $\mathbf{P} = \mathbf{NP}$

### Beweis

Falls  $\mathbf{P} = \mathbf{NP}$ , dann  $L \in \mathbf{P} = \mathbf{NP}$ , da  $L \in \mathbf{NP}$  (da **NP**-vollständig).

Umgekehrt sei  $L \in \mathbf{P}$  und  $L' \in \mathbf{NP}$  beliebig. Da  $L$  **NP**-vollständig und damit **NP**-schwer, gilt  $L' \preceq_{\mathbf{P}} L$ . Zusammen mit  $L \in \mathbf{P}$  folgt  $L' \in \mathbf{P}$  und damit  $\mathbf{NP} \subseteq \mathbf{P}$ . Per Theorem §11.8  $\mathbf{P} \subseteq \mathbf{NP}$  und damit  $\mathbf{P} = \mathbf{NP}$ .  $\square$

# NP-Schwere & NP-Vollständigkeit

---

## Notizen

- Nachweis **NP**-Schwere schwierig  
(polynomielle Reduktion von jedem Problem aus **NP**)
- Mitgliedschaft in **NP** per nichtdet. polynomielle Entscheidbarkeit  
(Angabe geeigneter Zertifikatrelation)

# NP-Schwere & NP-Vollständigkeit

---

## §12.4 Theorem

Problem  $L$  **NP**-schwer, falls **NP**-schweres Problem  $L'$  mit  $L' \preceq_P L$  existiert

# NP-Schwere & NP-Vollständigkeit

---

## §12.4 Theorem

Problem  $L$  **NP**-schwer, falls **NP**-schweres Problem  $L'$  mit  $L' \preceq_P L$  existiert

### Beweis

Sei  $L'$  **NP**-schwer und  $L' \preceq_P L$ . Dann  $L'' \preceq_P L' \preceq_P L$  für alle  $L'' \in \mathbf{NP}$ .



# NP-Schwere & NP-Vollständigkeit

---

## §12.4 Theorem

Problem  $L$  **NP**-schwer, falls **NP**-schweres Problem  $L'$  mit  $L' \preceq_P L$  existiert

### Beweis

Sei  $L'$  **NP**-schwer und  $L' \preceq_P L$ . Dann  $L'' \preceq_P L' \preceq_P L$  für alle  $L'' \in \mathbf{NP}$ .

Transitivität  $\preceq_P$  liefert  $L'' \preceq_P L$  für alle  $L'' \in \mathbf{NP}$ , womit  $L$  **NP**-schwer  $\square$

# NP-Schwere & NP-Vollständigkeit

## §12.4 Theorem

Problem  $L$  **NP**-schwer, falls **NP**-schweres Problem  $L'$  mit  $L' \preceq_P L$  existiert

### Beweis

Sei  $L'$  **NP**-schwer und  $L' \preceq_P L$ . Dann  $L'' \preceq_P L' \preceq_P L$  für alle  $L'' \in \mathbf{NP}$ .

Transitivität  $\preceq_P$  liefert  $L'' \preceq_P L$  für alle  $L'' \in \mathbf{NP}$ , womit  $L$  **NP**-schwer  $\square$

### Schwierigkeit

- Bisher kein **NP**-schweres Problem

# NP-Vollständigkeit

---

## Erfüllbarkeit Aussagenlogik

- Geg. aussagenlogische Formel  $F$
- $F$  erfüllbar? (d.h. existiert Modell der Formel?)
- Problem  $\text{SAT} = \{F \mid F \text{ erfüllbare Formel Aussagenlogik}\}$

## Erfüllbarkeit Aussagenlogik

- Geg. aussagenlogische Formel  $F$
- $F$  erfüllbar? (d.h. existiert Modell der Formel?)
- Problem  $\text{SAT} = \{F \mid F \text{ erfüllbare Formel Aussagenlogik}\}$
  
- Entscheidbarkeit  $\text{SAT}$

# NP-Vollständigkeit

---

## Erfüllbarkeit Aussagenlogik

- Geg. aussagenlogische Formel  $F$
- $F$  erfüllbar? (d.h. existiert Modell der Formel?)
- Problem  $\text{SAT} = \{F \mid F \text{ erfüllbare Formel Aussagenlogik}\}$
  
- Entscheidbarkeit  $\text{SAT}$  **entscheidbar**
- Polynomielle Entscheidbarkeit  $\text{SAT}$

# NP-Vollständigkeit

---

## Erfüllbarkeit Aussagenlogik

- Geg. aussagenlogische Formel  $F$
- $F$  erfüllbar? (d.h. existiert Modell der Formel?)
- Problem  $SAT = \{F \mid F \text{ erfüllbare Formel Aussagenlogik}\}$
  
- Entscheidbarkeit  $SAT$  **entscheidbar**
- Polynomielle Entscheidbarkeit  $SAT$  **unklar**
- Nichtdet. polynomielle Entscheidbarkeit  $SAT$

# NP-Vollständigkeit

---

## Erfüllbarkeit Aussagenlogik

- Geg. aussagenlogische Formel  $F$
- $F$  erfüllbar? (d.h. existiert Modell der Formel?)
- Problem  $\text{SAT} = \{F \mid F \text{ erfüllbare Formel Aussagenlogik}\}$
  
- Entscheidbarkeit  $\text{SAT}$  **entscheidbar**
- Polynomielle Entscheidbarkeit  $\text{SAT}$  **unklar**
- Nichtdet. polynomielle Entscheidbarkeit  $\text{SAT}$  **ja, in NP**

# NP-Vollständigkeit

---

## Beispiele

- Erfüllbare Formel

$$F_1 = (x_2 \vee (x_1 \wedge \neg x_3) \vee x_4) \wedge x_1$$

Modell  $I = \{x_1, x_2\}$ , kurz 1100

$$x_1 = 1; x_2 = 1; x_3 = 0; x_4 = 0$$



# NP-Vollständigkeit

---

## Beispiele

- Erfüllbare Formel

$$F_1 = (x_2 \vee (x_1 \wedge \neg x_3) \vee x_4) \wedge x_1 \quad F_1' = (1 \vee (1 \wedge \neg 0) \vee 0) \wedge 1 = 1$$

Modell  $I = \{x_1, x_2\}$ , kurz 1100       $x_1 = 1; x_2 = 1; x_3 = 0; x_4 = 0$

- Unerfüllbare Formel

$$F_2 = ((\neg x_1 \wedge \neg x_3) \vee x_2) \wedge x_1 \wedge \neg x_2$$

# NP-Vollständigkeit

---

## Beispiele

- Erfüllbare Formel

$$F_1 = (x_2 \vee (x_1 \wedge \neg x_3) \vee x_4) \wedge x_1 \quad F_1' = (1 \vee (1 \wedge \neg 0) \vee 0) \wedge 1 = 1$$

Modell  $I = \{x_1, x_2\}$ , kurz 1100       $x_1 = 1; x_2 = 1; x_3 = 0; x_4 = 0$

- Unerfüllbare Formel

$$F_2 = ((\neg x_1 \wedge \neg x_3) \vee x_2) \wedge x_1 \wedge \neg x_2$$

- Erfüllbare Formel

$$F_3 = (\neg x_1 \vee x_3 \vee x_2) \wedge x_1 \wedge \neg x_2$$

Modell  $I = \{x_1, x_3\}$ , kurz: 101       $x_1 = 1; x_2 = 0; x_3 = 1$

# NP-Vollständigkeit

---

## Beispiele

- Erfüllbare Formel

$$F_1 = (x_2 \vee (x_1 \wedge \neg x_3) \vee x_4) \wedge x_1 \quad F_1' = (1 \vee (1 \wedge \neg 0) \vee 0) \wedge 1 = 1$$

Modell  $I = \{x_1, x_2\}$ , kurz 1100       $x_1 = 1; x_2 = 1; x_3 = 0; x_4 = 0$

- Unerfüllbare Formel

$$F_2 = ((\neg x_1 \wedge \neg x_3) \vee x_2) \wedge x_1 \wedge \neg x_2$$

- Erfüllbare Formel

$$F_3 = (\neg x_1 \vee x_3 \vee x_2) \wedge x_1 \wedge \neg x_2 \quad F_3' = (\neg 1 \vee 1 \vee 0) \wedge 1 \wedge \neg 0 = 1$$

Modell  $I = \{x_1, x_3\}$ , kurz: 101       $x_1 = 1; x_2 = 0; x_3 = 1$

# NP-Vollständigkeit

---

## §12.5 Theorem

SAT  $\in$  NP

### Beweis

Sei  $F$  aussagenlogische Formel mit  $k$  Atomen  $\{x_1, \dots, x_k\}$ . Wir setzen  $R = \{(F, I) \mid I \models F\}$ ; Zertifikat ist Modell.

# NP-Vollständigkeit

---

## §12.5 Theorem

SAT  $\in$  NP

### Beweis

Sei  $F$  aussagenlogische Formel mit  $k$  Atomen  $\{x_1, \dots, x_k\}$ . Wir setzen  $R = \{(F, I) \mid I \models F\}$ ; Zertifikat ist Modell. Repräsentation  $R$  polynomiell entscheidbar, denn While-Programm kann  $F$  dekodieren, Atome gemäß Interpretation  $I$  auswerten und Wahrheitswert von  $I \models F$  bestimmen.

# NP-Vollständigkeit

## §12.5 Theorem

SAT  $\in$  NP

### Beweis

Sei  $F$  aussagenlogische Formel mit  $k$  Atomen  $\{x_1, \dots, x_k\}$ . Wir setzen  $R = \{(F, I) \mid I \models F\}$ ; Zertifikat ist Modell. Repräsentation  $R$  polynomiell entscheidbar, denn While-Programm kann  $F$  dekodieren, Atome gemäß Interpretation  $I$  auswerten und Wahrheitswert von  $I \models F$  bestimmen. Zertifikat hat Länge  $k \leq |F|$  (Interpretation = Teilmenge repräsentiert als  $\{0, 1\}^k$ ) und  $F \in \text{SAT}$  gdw.  $(F, I) \in R$  für  $I \subseteq \{x_1, \dots, x_k\}$ , wobei  $(F, I) \in R$  gdw.  $I \models F$ . □

## §12.6 Theorem

Existiert Formel  $U$  polynomieller Größe in  $k$  mit Atomen  $x_1, \dots, x_k$  und  $|I| = 1$  für jedes Modell  $I \models U$  mit  $I \subseteq \{x_1, \dots, x_k\}$

# NP-Vollständigkeit

## §12.6 Theorem

Existiert Formel  $U$  polynomieller Größe in  $k$  mit Atomen  $x_1, \dots, x_k$  und  $|I| = 1$  für jedes Modell  $I \models U$  mit  $I \subseteq \{x_1, \dots, x_k\}$

## Beweis

Sei

$$U = \left( \bigvee_{i=1}^k x_i \right) \wedge \left( \bigwedge_{1 \leq m < \ell \leq k} \neg(x_m \wedge x_\ell) \right)$$



# NP-Vollständigkeit

## §12.6 Theorem

Existiert Formel  $U$  polynomieller Größe in  $k$  mit Atomen  $x_1, \dots, x_k$  und  $|I| = 1$  für jedes Modell  $I \models U$  mit  $I \subseteq \{x_1, \dots, x_k\}$

## Beweis

Sei

$$U = \left( \bigvee_{i=1}^k x_i \right) \wedge \left( \bigwedge_{1 \leq m < \ell \leq k} \neg(x_m \wedge x_\ell) \right)$$

Formel hat Größe in  $\mathcal{O}(k^2)$  und Teil  $\bigvee_{i=1}^k x_i$  erzwingt mind. 1 Atom in  $I$ .

# NP-Vollständigkeit

## §12.6 Theorem

Existiert Formel  $U$  polynomieller Größe in  $k$  mit Atomen  $x_1, \dots, x_k$  und  $|I| = 1$  für jedes Modell  $I \models U$  mit  $I \subseteq \{x_1, \dots, x_k\}$

## Beweis

Sei

$$U = \left( \bigvee_{i=1}^k x_i \right) \wedge \left( \bigwedge_{1 \leq m < \ell \leq k} \neg(x_m \wedge x_\ell) \right)$$

Formel hat Größe in  $\mathcal{O}(k^2)$  und Teil  $\bigvee_{i=1}^k x_i$  erzwingt mind. 1 Atom in  $I$ . Verbleibender Teil genau dann falsch, wenn  $|I| \geq 2$ . Also  $|I| = 1$  für alle Modelle  $I \models U$  □

# NP-Vollständigkeit

---

## §12.7 Theorem (Satz von Cook)

SAT NP-vollständig

# NP-Vollständigkeit

---

## §12.7 Theorem (Satz von Cook)

SAT **NP**-vollständig

### Beweis (1/6)

SAT  $\in$  **NP** bekannt; zu zeigen **NP**-Schwere

# NP-Vollständigkeit

## §12.7 Theorem (Satz von Cook)

SAT NP-vollständig

### Beweis (1/6)

SAT  $\in$  NP bekannt; zu zeigen NP-Schwere

Sei  $L \subseteq \Sigma^*$  Problem aus NP. Dann existieren Alphabet  $\Gamma$ ,  $k \geq 1$  und polynomiell entscheidbare Zertifikatrelation  $R \subseteq \Sigma^* \times \Gamma^*$  mit

$$w \in L \text{ gdw. } (w, z) \in R \text{ und } |z| \leq |w|^k \text{ für ein } z \in \Gamma^*$$

# NP-Vollständigkeit

## §12.7 Theorem (Satz von Cook)

SAT NP-vollständig

### Beweis (1/6)

SAT  $\in$  NP bekannt; zu zeigen NP-Schwere

Sei  $L \subseteq \Sigma^*$  Problem aus NP. Dann existieren Alphabet  $\Gamma$ ,  $k \geq 1$  und polynomiell entscheidbare Zertifikatrelation  $R \subseteq \Sigma^* \times \Gamma^*$  mit

$$w \in L \text{ gdw. } (w, z) \in R \text{ und } |z| \leq |w|^k \text{ für ein } z \in \Gamma^*$$

Sei  $M = (Q, \Sigma', \Gamma', \Delta, \square, q_0, q_+, q_-)$  det. TM, die  $R$  polynomiell berechnet und beschränkendes Polynom  $P$ .

# NP-Vollständigkeit

## §12.7 Theorem (Satz von Cook)

### SAT NP-vollständig

#### Beweis (1/6)

SAT  $\in$  NP bekannt; zu zeigen NP-Schwere

Sei  $L \subseteq \Sigma^*$  Problem aus NP. Dann existieren Alphabet  $\Gamma$ ,  $k \geq 1$  und polynomiell entscheidbare Zertifikatrelation  $R \subseteq \Sigma^* \times \Gamma^*$  mit

$$w \in L \text{ gdw. } (w, z) \in R \text{ und } |z| \leq |w|^k \text{ für ein } z \in \Gamma^*$$

Sei  $M = (Q, \Sigma', \Gamma', \Delta, \square, q_0, q_+, q_-)$  det. TM, die  $R$  polynomiell berechnet und beschränkendes Polynom  $P$ . O.B.d.A.

- $Q = \{1, \dots, k'\}$  und  $\Gamma' = \{1, \dots, k''\}$
- $(w, z) \in R$  impliziert  $|z| = |w|^k$  (Zertifikate mit uniformer Länge)
- $t_{\max}(w) = P(1 + |w| + |w|^k)$  (ob. Schranke Laufzeit auf  $w$ )

# NP-Vollständigkeit

---

## Beweis (2/6)

Sei  $w = \sigma_1 \cdots \sigma_\ell$ . Konstruiere aussagenlogische Formel  $F(w)$  mit folgenden Atomen für alle  $0 \leq t \leq t_{\max}(w)$ ,  $-t_{\max}(w) \leq i \leq t_{\max}(w)$ ,  $q \in Q$  und  $\gamma \in \Gamma'$

- $\text{InState}_{t,q}$ : Ist  $M$  bei Schritt  $t$  in Zustand  $q$ ?



# NP-Vollständigkeit

## Beweis (2/6)

Sei  $w = \sigma_1 \cdots \sigma_\ell$ . Konstruiere aussagenlogische Formel  $F(w)$  mit folgenden Atomen für alle  $0 \leq t \leq t_{\max}(w)$ ,  $-t_{\max}(w) \leq i \leq t_{\max}(w)$ ,  $q \in Q$  und  $\gamma \in \Gamma'$

- $\text{InState}_{t,q}$ : Ist  $M$  bei Schritt  $t$  in Zustand  $q$ ?
- $\text{AtPos}_{t,i}$ : Ist Kopf von  $M$  bei Schritt  $t$  an Bandposition  $i$ ?

# NP-Vollständigkeit

## Beweis (2/6)

Sei  $w = \sigma_1 \cdots \sigma_\ell$ . Konstruiere aussagenlogische Formel  $F(w)$  mit folgenden Atomen für alle  $0 \leq t \leq t_{\max}(w)$ ,  $-t_{\max}(w) \leq i \leq t_{\max}(w)$ ,  $q \in Q$  und  $\gamma \in \Gamma'$

- $\text{InState}_{t,q}$ : Ist  $M$  bei Schritt  $t$  in Zustand  $q$ ?
- $\text{AtPos}_{t,i}$ : Ist Kopf von  $M$  bei Schritt  $t$  an Bandposition  $i$ ?
- $\text{OnTape}_{t,i,\gamma}$ : Steht Zeichen  $\gamma$  bei Schritt  $t$  an Bandposition  $i$ ?

# NP-Vollständigkeit

## Beweis (2/6)

Sei  $w = \sigma_1 \cdots \sigma_\ell$ . Konstruiere aussagenlogische Formel  $F(w)$  mit folgenden Atomen für alle  $0 \leq t \leq t_{\max}(w)$ ,  $-t_{\max}(w) \leq i \leq t_{\max}(w)$ ,  $q \in Q$  und  $\gamma \in \Gamma'$

- $\text{InState}_{t,q}$ : Ist  $M$  bei Schritt  $t$  in Zustand  $q$ ?
- $\text{AtPos}_{t,i}$ : Ist Kopf von  $M$  bei Schritt  $t$  an Bandposition  $i$ ?
- $\text{OnTape}_{t,i,\gamma}$ : Steht Zeichen  $\gamma$  bei Schritt  $t$  an Bandposition  $i$ ?

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

(wir geben offensichtliche Quantifikation nicht an)

Endbedingung  $E(w) = \bigvee_t \text{InState}_{t,q_+}$

(akzeptierender Zustand erreicht)

# NP-Vollständigkeit

---

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

$$Q = \{1, \dots, k'\} \text{ und } \Gamma' = \{1, \dots, k''\}$$

## Beweis (3/6)

### Randbedingungen

$$\begin{aligned} A(w) = & \bigwedge_t U(\text{InState}_{t,1}, \dots, \text{InState}_{t,k'}) \wedge \\ & \bigwedge_t U(\text{AtPos}_{t,-t_{\max}(w)}, \dots, \text{AtPos}_{t,t_{\max}(w)}) \wedge \\ & \bigwedge_{t,i} U(\text{OnTape}_{t,i,1}, \dots, \text{OnTape}_{t,i,k'') \end{aligned}$$

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

$$Q = \{1, \dots, k'\} \text{ und } \Gamma' = \{1, \dots, k''\}$$

## Beweis (3/6)

### Randbedingungen

$$A(w) = \bigwedge_t U(\text{InState}_{t,1}, \dots, \text{InState}_{t,k'}) \wedge \\ \bigwedge_t U(\text{AtPos}_{t,-t_{\max}(w)}, \dots, \text{AtPos}_{t,t_{\max}(w)}) \wedge \\ \bigwedge_{t,i} U(\text{OnTape}_{t,i,1}, \dots, \text{OnTape}_{t,i,k''})$$

- Zu jedem Schritt in genau 1 Zustand

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

$$Q = \{1, \dots, k'\} \text{ und } \Gamma' = \{1, \dots, k''\}$$

## Beweis (3/6)

### Randbedingungen

$$A(w) = \bigwedge_t U(\text{InState}_{t,1}, \dots, \text{InState}_{t,k'}) \wedge$$
$$\bigwedge_t U(\text{AtPos}_{t,-t_{\max}(w)}, \dots, \text{AtPos}_{t,t_{\max}(w)}) \wedge$$
$$\bigwedge_{t,i} U(\text{OnTape}_{t,i,1}, \dots, \text{OnTape}_{t,i,k''})$$

- Zu jedem Schritt in genau 1 Zustand
- Zu jedem Schritt an genau 1 Position

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

$$Q = \{1, \dots, k'\} \text{ und } \Gamma' = \{1, \dots, k''\}$$

## Beweis (3/6)

### Randbedingungen

$$\begin{aligned} A(w) = & \bigwedge_t U(\text{InState}_{t,1}, \dots, \text{InState}_{t,k'}) \wedge \\ & \bigwedge_t U(\text{AtPos}_{t,-t_{\max}(w)}, \dots, \text{AtPos}_{t,t_{\max}(w)}) \wedge \\ & \bigwedge_{t,i} U(\text{OnTape}_{t,i,1}, \dots, \text{OnTape}_{t,i,k'') \end{aligned}$$

- Zu jedem Schritt in genau 1 Zustand
- Zu jedem Schritt an genau 1 Position
- Zu jedem Schritt steht genau 1 Zeichen an Position

# NP-Vollständigkeit

---

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (4/6)

### Initialbedingungen

$$I(w) = \text{InState}_{0,q_0} \wedge \text{AtPos}_{0,0} \wedge \left( \bigwedge_{m \notin \{0, \dots, \ell^k + \ell\}} \text{OnTape}_{0,m,\square} \right) \wedge \\ \left( \bigwedge_{m=1}^{\ell} \text{OnTape}_{0,m-1,\sigma_m} \right) \wedge \text{OnTape}_{0,\ell,\#} \wedge \left( \bigwedge_{m=\ell+1}^{\ell^k + \ell} \neg \text{OnTape}_{0,m,\square} \right)$$



# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (4/6)

### Initialbedingungen

$$I(w) = \text{InState}_{0,q_0} \wedge \text{AtPos}_{0,0} \wedge \left( \bigwedge_{m \notin \{0, \dots, \ell^k + \ell\}} \text{OnTape}_{0,m,\square} \right) \wedge$$
$$\left( \bigwedge_{m=1}^{\ell} \text{OnTape}_{0,m-1,\sigma_m} \right) \wedge \text{OnTape}_{0,\ell,\#} \wedge \left( \bigwedge_{m=\ell+1}^{\ell^k + \ell} \neg \text{OnTape}_{0,m,\square} \right)$$

- Initial im Zustand  $q_0$  und an Position 0

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (4/6)

### Initialbedingungen

$$I(w) = \text{InState}_{0,q_0} \wedge \text{AtPos}_{0,0} \wedge \left( \bigwedge_{m \notin \{0, \dots, \ell^k + \ell\}} \text{OnTape}_{0,m,\square} \right) \wedge \\ \left( \bigwedge_{m=1}^{\ell} \text{OnTape}_{0,m-1,\sigma_m} \right) \wedge \text{OnTape}_{0,\ell,\#} \wedge \left( \bigwedge_{m=\ell+1}^{\ell^k + \ell} \neg \text{OnTape}_{0,m,\square} \right)$$

- Initial im Zustand  $q_0$  und an Position 0
- Außerhalb Eingabe steht  $\square$  auf Band

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (4/6)

### Initialbedingungen

$$I(w) = \text{InState}_{0,q_0} \wedge \text{AtPos}_{0,0} \wedge \left( \bigwedge_{m \notin \{0, \dots, \ell^k + \ell\}} \text{OnTape}_{0,m,\square} \right) \wedge$$
$$\left( \bigwedge_{m=1}^{\ell} \text{OnTape}_{0,m-1,\sigma_m} \right) \wedge \text{OnTape}_{0,\ell,\#} \wedge \left( \bigwedge_{m=\ell+1}^{\ell^k + \ell} \neg \text{OnTape}_{0,m,\square} \right)$$

- Initial im Zustand  $q_0$  und an Position 0
- Außerhalb Eingabe steht  $\square$  auf Band
- Auf Band steht  $w\#z$  für beliebiges  $z \in \Gamma^{\ell^k}$

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (5/6)

Übergangsbedingungen mit  $\diamond = 0$ ,  $\triangleleft = -1$  und  $\triangleright = 1$

$$\begin{aligned} T(w) = & \bigwedge_{\substack{t,i,\gamma \\ t \neq t_{\max}(w)}} \left( (\neg \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \text{OnTape}_{t+1,i,\gamma} \right) \wedge \\ & \bigwedge_{\substack{t,q,i,\gamma \\ t \neq t_{\max}(w), q \notin \{q_+, q_-\}}} \left( (\text{InState}_{t,q} \wedge \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \right. \\ & \quad \left. \bigvee_{((q,\gamma) \rightarrow (q',\gamma',d)) \in \Delta'} (\text{InState}_{t+1,q'} \wedge \text{AtPos}_{t+1,i+d} \wedge \text{OnTape}_{t+1,i,\gamma'}) \right) \end{aligned}$$

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (5/6)

Übergangsbedingungen mit  $\diamond = 0$ ,  $\triangleleft = -1$  und  $\triangleright = 1$

$$\begin{aligned} T(w) = & \bigwedge_{\substack{t,i,\gamma \\ t \neq t_{\max}(w)}} \left( (\neg \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \text{OnTape}_{t+1,i,\gamma} \right) \wedge \\ & \bigwedge_{\substack{t,q,i,\gamma \\ t \neq t_{\max}(w), q \notin \{q_+, q_-\}}} \left( (\text{InState}_{t,q} \wedge \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \right. \\ & \quad \left. \bigvee_{((q,\gamma) \rightarrow (q',\gamma',d)) \in \Delta'} (\text{InState}_{t+1,q'} \wedge \text{AtPos}_{t+1,i+d} \wedge \text{OnTape}_{t+1,i,\gamma'}) \right) \end{aligned}$$

- Band außerhalb aktueller Position erhalten

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (5/6)

Übergangsbedingungen mit  $\diamond = 0$ ,  $\triangleleft = -1$  und  $\triangleright = 1$

$$\begin{aligned} T(w) = & \bigwedge_{\substack{t,i,\gamma \\ t \neq t_{\max}(w)}} \left( (\neg \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \text{OnTape}_{t+1,i,\gamma} \right) \wedge \\ & \bigwedge_{\substack{t,q,i,\gamma \\ t \neq t_{\max}(w), q \notin \{q_+, q_-\}}} \left( (\text{InState}_{t,q} \wedge \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \right. \\ & \quad \left. \bigvee_{((q,\gamma) \rightarrow (q',\gamma',d)) \in \Delta'} (\text{InState}_{t+1,q'} \wedge \text{AtPos}_{t+1,i+d} \wedge \text{OnTape}_{t+1,i,\gamma'}) \right) \end{aligned}$$

- Band außerhalb aktueller Position erhalten
- Prüfe Vorbedingungen Übergang

# NP-Vollständigkeit

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (5/6)

Übergangsbedingungen mit  $\diamond = 0$ ,  $\triangleleft = -1$  und  $\triangleright = 1$

$$\begin{aligned} T(w) = & \bigwedge_{\substack{t,i,\gamma \\ t \neq t_{\max}(w)}} \left( (\neg \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \text{OnTape}_{t+1,i,\gamma} \right) \wedge \\ & \bigwedge_{\substack{t,q,i,\gamma \\ t \neq t_{\max}(w), q \notin \{q_+, q_-\}}} \left( (\text{InState}_{t,q} \wedge \text{AtPos}_{t,i} \wedge \text{OnTape}_{t,i,\gamma}) \rightarrow \right. \\ & \quad \left. \bigvee_{((q,\gamma) \rightarrow (q',\gamma',d)) \in \Delta'} (\text{InState}_{t+1,q'} \wedge \text{AtPos}_{t+1,i+d} \wedge \text{OnTape}_{t+1,i,\gamma'}) \right) \end{aligned}$$

- Band außerhalb aktueller Position erhalten
- Prüfe Vorbedingungen Übergang
- Für jeden Schritt führe passenden Übergang aus

# NP-Vollständigkeit

---

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (6/6)

Teilformeln polynomieller Länge in  $|w|$  und  $F(w)$  polynomiell berechenbar.



# NP-Vollständigkeit

---

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (6/6)

Teilformeln polynomieller Länge in  $|w|$  und  $F(w)$  polynomiell berechenbar. Sei  $w \in L$  mit Zertifikat  $z \in \Gamma^{\ell^k}$ . Dann  $F(w)$  für Band  $w\#z$  erfüllbar, da Berechnung von  $M$  simuliert und  $M$  akzeptiert.

# NP-Vollständigkeit

---

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (6/6)

Teilformeln polynomieller Länge in  $|w|$  und  $F(w)$  polynomiell berechenbar. Sei  $w \in L$  mit Zertifikat  $z \in \Gamma^{\ell^k}$ . Dann  $F(w)$  für Band  $w\#z$  erfüllbar, da Berechnung von  $M$  simuliert und  $M$  akzeptiert. Umgekehrt sei  $F(w)$  erfüllbar. Dann liefert Modell Zertifikat  $z$  und akzeptierende Berechnung det. TM  $M$ . Folglich  $w \in L$ .

# NP-Vollständigkeit

---

$$F(w) = A(w) \wedge I(w) \wedge T(w) \wedge E(w)$$

## Beweis (6/6)

Teilformeln polynomieller Länge in  $|w|$  und  $F(w)$  polynomiell berechenbar. Sei  $w \in L$  mit Zertifikat  $z \in \Gamma^{\ell^k}$ . Dann  $F(w)$  für Band  $w\#z$  erfüllbar, da Berechnung von  $M$  simuliert und  $M$  akzeptiert. Umgekehrt sei  $F(w)$  erfüllbar. Dann liefert Modell Zertifikat  $z$  und akzeptierende Berechnung det. TM  $M$ . Folglich  $w \in L$ . Also  $w \in L$  gdw.  $F(w)$  erfüllbar gdw.  $F(w) \in \text{SAT}$ . Damit  $L \leq_p \text{SAT}$ , womit SAT **NP**-schwer und **NP**-vollständig. □

# NP-vollständige Probleme

---

## §12.8 Definition (konjunktive Normalform mit 3 Literalen)

Aussagenlogische Formel  $F$  in **konjunktiver Normalform mit 3 Literalen** (3KNF) falls  $F = F_1 \wedge \dots \wedge F_k$  für Formeln  $F_1, \dots, F_k$  mit  $F_i = L_{i1} \vee L_{i2} \vee L_{i3}$  für alle  $1 \leq i \leq k$  und Literale  $L_{i1}, L_{i2}, L_{i3}$   
(Literal = Atom oder negiertes Atom)

# NP-vollständige Probleme

---

## §12.8 Definition (konjunktive Normalform mit 3 Literalen)

Aussagenlogische Formel  $F$  in **konjunktiver Normalform mit 3 Literalen** (3KNF) falls  $F = F_1 \wedge \dots \wedge F_k$  für Formeln  $F_1, \dots, F_k$  mit  $F_i = L_{i1} \vee L_{i2} \vee L_{i3}$  für alle  $1 \leq i \leq k$  und Literale  $L_{i1}, L_{i2}, L_{i3}$   
(Literal = Atom oder negiertes Atom)

### Beispiele

- $x_1 \vee x_2 \vee x_3$  in 3KNF

# NP-vollständige Probleme

---

## §12.8 Definition (konjunktive Normalform mit 3 Literalen)

Aussagenlogische Formel  $F$  in **konjunktiver Normalform mit 3 Literalen** (3KNF) falls  $F = F_1 \wedge \dots \wedge F_k$  für Formeln  $F_1, \dots, F_k$  mit  $F_i = L_{i1} \vee L_{i2} \vee L_{i3}$  für alle  $1 \leq i \leq k$  und Literale  $L_{i1}, L_{i2}, L_{i3}$   
(Literal = Atom oder negiertes Atom)

### Beispiele

- $x_1 \vee x_2 \vee x_3$  in 3KNF
- $(x_1 \wedge x_2) \vee x_4$  nicht in 3KNF

# NP-vollständige Probleme

---

## §12.8 Definition (konjunktive Normalform mit 3 Literalen)

Aussagenlogische Formel  $F$  in **konjunktiver Normalform mit 3 Literalen** (3KNF) falls  $F = F_1 \wedge \dots \wedge F_k$  für Formeln  $F_1, \dots, F_k$  mit  $F_i = L_{i1} \vee L_{i2} \vee L_{i3}$  für alle  $1 \leq i \leq k$  und Literale  $L_{i1}, L_{i2}, L_{i3}$   
(Literal = Atom oder negiertes Atom)

### Beispiele

- $x_1 \vee x_2 \vee x_3$  in 3KNF
- $(x_1 \wedge x_2) \vee x_4$  nicht in 3KNF
- $x_1 \wedge (x_2 \vee x_1 \vee \neg x_3)$  nicht in 3KNF

# NP-vollständige Probleme

## §12.8 Definition (konjunktive Normalform mit 3 Literalen)

Aussagenlogische Formel  $F$  in **konjunktiver Normalform mit 3 Literalen** (3KNF) falls  $F = F_1 \wedge \dots \wedge F_k$  für Formeln  $F_1, \dots, F_k$  mit  $F_i = L_{i1} \vee L_{i2} \vee L_{i3}$  für alle  $1 \leq i \leq k$  und Literale  $L_{i1}, L_{i2}, L_{i3}$   
(Literal = Atom oder negiertes Atom)

### Beispiele

- $x_1 \vee x_2 \vee x_3$  in 3KNF
- $(x_1 \wedge x_2) \vee x_4$  nicht in 3KNF
- $x_1 \wedge (x_2 \vee x_1 \vee \neg x_3)$  nicht in 3KNF
- $(x_1 \vee x_1 \vee x_1) \wedge (x_2 \vee \neg x_1 \vee \neg x_3)$  in 3KNF  
(erlauben auch  $\leq 3$  Literale; dann 3. Beispiel in 3KNF)



# NP-vollständige Probleme

---

## Erfüllbarkeit 3KNF-Formel

- Geg. aussagenlogische Formel  $F$  in 3KNF
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $3\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 3KNF}\}$

# NP-vollständige Probleme

---

## Erfüllbarkeit 3KNF-Formel

- Geg. aussagenlogische Formel  $F$  in 3KNF
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $3\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 3KNF}\}$
- Entscheidbarkeit  $3\text{-SAT}$

# NP-vollständige Probleme

---

## Erfüllbarkeit 3KNF-Formel

- Geg. aussagenlogische Formel  $F$  in 3KNF
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $3\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 3KNF}\}$
- Entscheidbarkeit  $3\text{-SAT}$  **entscheidbar**
- Polynomielle Entscheidbarkeit  $3\text{-SAT}$

# NP-vollständige Probleme

---

## Erfüllbarkeit 3KNF-Formel

- Geg. aussagenlogische Formel  $F$  in 3KNF
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $3\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 3KNF}\}$
- Entscheidbarkeit  $3\text{-SAT}$  **entscheidbar**
- Polynomielle Entscheidbarkeit  $3\text{-SAT}$  **unklar**
- Nichtdet. polynomielle Entscheidbarkeit  $3\text{-SAT}$

# NP-vollständige Probleme

---

## Erfüllbarkeit 3KNF-Formel

- Geg. aussagenlogische Formel  $F$  in 3KNF
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $3\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 3KNF}\}$
  
- Entscheidbarkeit  $3\text{-SAT}$  **entscheidbar**
- Polynomielle Entscheidbarkeit  $3\text{-SAT}$  **unklar**
- Nichtdet. polynomielle Entscheidbarkeit  $3\text{-SAT}$  **ja, in NP**  
(denn  $3\text{-SAT} \preceq_p \text{SAT}$  mittels Identität; also  $3\text{-SAT} \in \text{NP}$ )

# NP-vollständige Probleme

---

## §12.9 Theorem

3-SAT NP-vollständig

### Beweis (1/2)

Da 3-SAT  $\in$  NP nur NP-Schwere per SAT  $\preceq_p$  3-SAT zu zeigen.

# NP-vollständige Probleme

---

## §12.9 Theorem

### 3-SAT NP-vollständig

#### Beweis (1/2)

Da  $3\text{-SAT} \in \text{NP}$  nur NP-Schwere per  $\text{SAT} \preceq_p 3\text{-SAT}$  zu zeigen. Sei  $F$  aussagenlogische Formel. Transformiere  $F$  in Polynomialzeit in Negationsnormalform (Negationen nur vor Atomen).

# NP-vollständige Probleme

## §12.9 Theorem

### 3-SAT NP-vollständig

#### Beweis (1/2)

Da  $3\text{-SAT} \in \text{NP}$  nur NP-Schwere per  $\text{SAT} \preceq_p 3\text{-SAT}$  zu zeigen. Sei  $F$  aussagenlogische Formel. Transformiere  $F$  in Polynomialzeit in Negationsnormalform (Negationen nur vor Atomen). Sei  $T$  Syntaxbaum der erhaltenen Formel  $F'$  und für jeden Knoten  $w$  dieses Baumes sei

- $v(w) = T(w)$  falls Knotenbeschriftung  $T(w)$  Literal
- sonst  $v(w) = y$  für neues Atom  $y$ .



# NP-vollständige Probleme

## §12.9 Theorem

### 3-SAT NP-vollständig

#### Beweis (1/2)

Da  $3\text{-SAT} \in \mathbf{NP}$  nur  $\mathbf{NP}$ -Schwere per  $\text{SAT} \preceq_p 3\text{-SAT}$  zu zeigen. Sei  $F$  aussagenlogische Formel. Transformiere  $F$  in Polynomialzeit in Negationsnormalform (Negationen nur vor Atomen). Sei  $T$  Syntaxbaum der erhaltenen Formel  $F'$  und für jeden Knoten  $w$  dieses Baumes sei

- $v(w) = T(w)$  falls Knotenbeschriftung  $T(w)$  Literal
- sonst  $v(w) = y$  für neues Atom  $y$ .

Konstruiere Formel  $f(F) = v(\varepsilon) \wedge \bigwedge_{w \text{ innere Position in } T} F'_w$ , in der für jedes  $w$  Formel  $F'_w$  durch Formel  $v(w) \leftrightarrow (v(w_1) T(w) v(w_2))$  in 3KNF gegeben ist, wobei  $T(w)$  Symbol ( $\vee$  oder  $\wedge$ ) an Position  $w$  und  $w_1/w_2$  erste/zweite Kindposition von  $w$  (Tseitin-Transformation)

# NP-vollständige Probleme

---

## Beweis (2/2)

3KNF Teilformel  $F'_w$  gegeben durch

$$(L_1 \leftrightarrow (L_2 \vee L_3)) \quad \text{äq. zu} \quad (L_1 \vee \neg L_2) \wedge (\neg L_1 \vee L_2 \vee L_3) \wedge (L_1 \vee \neg L_3)$$

$$(L_1 \leftrightarrow (L_2 \wedge L_3)) \quad \text{äq. zu} \quad (\neg L_1 \vee L_2) \wedge (L_1 \vee \neg L_2 \vee \neg L_3) \wedge (\neg L_1 \vee L_3)$$

# NP-vollständige Probleme

---

## Beweis (2/2)

3KNF Teilformel  $F'_w$  gegeben durch

$$(L_1 \leftrightarrow (L_2 \vee L_3)) \quad \text{äq. zu} \quad (L_1 \vee \neg L_2) \wedge (\neg L_1 \vee L_2 \vee L_3) \wedge (L_1 \vee \neg L_3)$$

$$(L_1 \leftrightarrow (L_2 \wedge L_3)) \quad \text{äq. zu} \quad (\neg L_1 \vee L_2) \wedge (L_1 \vee \neg L_2 \vee \neg L_3) \wedge (\neg L_1 \vee L_3)$$

Offenbar  $f(F)$  in 3KNF und

$F$  erfüllbar gdw.  $f(F)$  erfüllbar

Damit  $\text{SAT} \preceq_p \text{3-SAT}$ , womit **3-SAT NP-vollständig**.

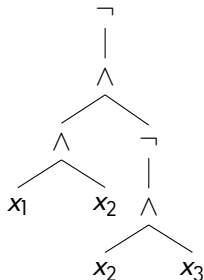


# NP-vollständige Probleme

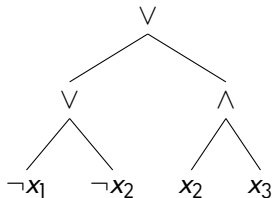
Beispiel

$$F = \neg((x_1 \wedge x_2) \wedge \neg(x_2 \wedge x_3))$$

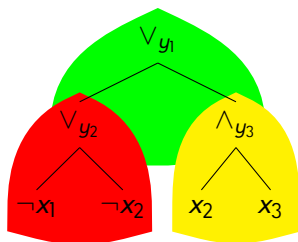
Syntaxbaum von  $F$



Syntaxbaum NNF  $F'$



Zuweisung

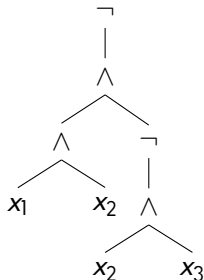


# NP-vollständige Probleme

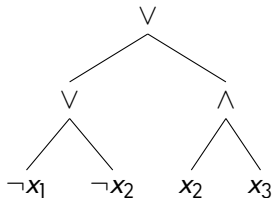
Beispiel

$$F = \neg((x_1 \wedge x_2) \wedge \neg(x_2 \wedge x_3))$$

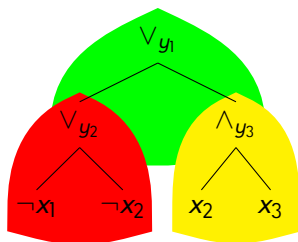
Syntaxbaum von  $F$



Syntaxbaum NNF  $F'$



Zuweisung



Konstruierte Formel  $f(F)$

$$y_1 \wedge (y_1 \leftrightarrow (y_2 \vee y_3)) \wedge (y_2 \leftrightarrow (\neg x_1 \vee \neg x_2)) \wedge (y_3 \leftrightarrow (x_2 \wedge x_3))$$

# NP-vollständige Probleme

---

## Konjunktive Normalform mit 2 Literalen

- Geg. aussagenlogische Formel  $F$  in 2KNF (max. 2 Literale)
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem 2-SAT =  $\{F \mid F \text{ erfüllbare Formel in 2KNF}\}$

# NP-vollständige Probleme

---

## Konjunktive Normalform mit 2 Literalen

- Geg. aussagenlogische Formel  $F$  in 2KNF (max. 2 Literale)
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem 2-SAT =  $\{F \mid F \text{ erfüllbare Formel in 2KNF}\}$
  
- Entscheidbarkeit 2-SAT

# NP-vollständige Probleme

---

## Konjunktive Normalform mit 2 Literalen

- Geg. aussagenlogische Formel  $F$  in 2KNF (max. 2 Literale)
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem 2-SAT =  $\{F \mid F \text{ erfüllbare Formel in 2KNF}\}$
- Entscheidbarkeit 2-SAT entscheidbar
- Polynomielle Entscheidbarkeit 2-SAT



# NP-vollständige Probleme

---

## Konjunktive Normalform mit 2 Literalen

- Geg. aussagenlogische Formel  $F$  in 2KNF (max. 2 Literale)
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $2\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 2KNF}\}$
- Entscheidbarkeit 2-SAT entscheidbar
- Polynomielle Entscheidbarkeit 2-SAT ja, in P
- Nichtdet. polynomielle Entscheidbarkeit 2-SAT

# NP-vollständige Probleme

---

## Konjunktive Normalform mit 2 Literalen

- Geg. aussagenlogische Formel  $F$  in 2KNF (max. 2 Literale)
- Ist  $F$  erfüllbar? (Existiert Modell?)
- Problem  $2\text{-SAT} = \{F \mid F \text{ erfüllbare Formel in 2KNF}\}$
  
- Entscheidbarkeit 2-SAT    **entscheidbar**
- Polynomielle Entscheidbarkeit 2-SAT    **ja, in P**
- Nichtdet. polynomielle Entscheidbarkeit 2-SAT    **ja, in NP**

# NP-vollständige Probleme

---

## Algorithmus für polynomielle Entscheidbarkeit

- Resolution für Unerfüllbarkeit (Resolution korrekt & vollständig)
- Resolventen haben höchstens 2 Literale
- Höchstens  $(2|F|)^2$  Resolventen bildbar

# Zusammenfassung

---

- Polynomielle Reduktionen & Zertifikate
- NP-Schwere & NP-Vollständigkeit
- NP-vollständiges Problem SAT (aussagenlogische Erfüllbarkeit)
- Weitere NP-vollständige Probleme

Sechste Übungsserie bereits im Moodle