Grundlagen der Theoretischen Informatik

Komplexitätstheorie (III)

7.07.2021

Viorica Sofronie-Stokkermans

e-mail: sofronie@uni-koblenz.de

Bis jetzt

- DTIME($f(n)$), NTIME($f(n)$), DSPACE($f(n)$), NSPACE($f(n)$),
- Entscheidbarkeit / NTM vs. DTM / Zeit vs. Speicher
- P, NP, PSPACE; P $\subseteq$ NP $\subseteq$ PSPACE
- Polynomial-Zeit-Reduzibilität
- Vollständige und harte Probleme

  NP-vollständig, NP-hart; PSPACE-vollständig, PSPACE-hart

  Cook's Theorem: SAT ist NP-vollständig.
- Abgschlossenheit der Komplexitätsklassen

Beispiele

NP-vollständige Probleme

- Ist eine logische Formel erfüllbar? (**Satisfiability**)
- Ist ein (un-) gerichteter Graph hamiltonsch? (**Hamiltonian circle**)
- Gibt es in einem Graphen eine Clique der Größe k? (**Clique of size** k)
- Ist ein Graph mit drei Farben zu färben? (3-**colorability**)
- Gibt es in einer Menge von ganzen Zahlen eine Teilmenge mit der Gesamtsumme x? (**Subset Sum**)

NP-vollständige Probleme

- Ist eine logische Formel erfüllbar? (**Satisfiability**)
- Ist ein (un-) gerichteter Graph hamiltonsch? (**Hamiltonian circle**)
- Gibt es in einem Graphen eine Clique der Größe k? (**Clique of size** k)
- Ist ein Graph mit drei Farben zu färben? (3-**colorability**)
- Gibt es in einer Menge von ganzen Zahlen eine Teilmenge mit der Gesamtsumme x? (**Subset Sum**)

NP-vollständige Probleme

Definition[CNF, DNF]

DNF: Eine Formel ist in **disjunktiver Normalform**, wenn sie von folgender Form ist:

$$(l_{11} \wedge \ldots \wedge l_{1n_1}) \vee \ldots \vee (l_{m1} \wedge \ldots \wedge l_{mn_m})$$

CNF: Eine Formel ist in **konjunktiver Normalform**, wenn sie von folgender Form ist:

$$(l_{11} \vee \ldots \vee l_{1n_1}) \wedge \ldots \wedge (l_{m1} \vee \ldots \vee l_{mn_m})$$

.....

NP-vollständige Probleme

Definition[k-CNF, k-DNF]

k-DNF: Eine Formel ist in $\boldsymbol{k}$-*DNF* wenn sie in DNF ist und jede ihrer Konjuntionen genau $\boldsymbol{k}$ Literale hat.

k-CNF: Eine Formel ist in $\boldsymbol{k}$-*CNF* wenn sie in CNF ist und jede ihrer Disjunktion genau $\boldsymbol{k}$ Literale hat.

NP-vollständige Probleme

Definition[SAT, CNF-SAT, k-CNF-SAT]

- SAT $= L_{\text{sat}} = \{w \mid w$ ist eine erfüllbare aussagenlogische Formel$\}$
- CNF-SAT $= \{w \mid w$ ist eine erfüllbare aussagenlogische Formel in CNF$\}$
- $\boldsymbol{k}$-CNF-SAT$= \{w \mid w$ ist eine erfüllbare aussagenlogische Formel in k-CNF$\}$

Definition[DNF-SAT, k-DNF-SAT]

- DNF-SAT $= \{w \mid w$ ist eine erfüllbare aussagenlogische Formel in DNF$\}$
- $\boldsymbol{k}$-DNF-SAT$= \{w \mid w$ ist eine erfüllbare aussagenlogische Formel in k-DNF$\}$

NP-vollständige Probleme

Theorem [NP-vollständige Probleme]

Die folgenden Probleme liegen in **NP** und sind **NP**-vollständig:

- L_{sat} (SAT)
- CNF-SAT
- k-CNF-SAT für $k \geq 3$

NP-vollständige Probleme

Theorem [NP-vollständige Probleme]
Die folgenden Probleme liegen in **NP** und sind **NP**-vollständig:

- L_{sat} (SAT)
- CNF-SAT
- k-CNF-SAT für $k \geq 3$

Theorem [Probleme in P]
Die folgenden Probleme liegen in P:

- DNF-SAT
- k-DNF-SAT für alle k
- 2-CNF-SAT

NP-vollständige Probleme

Einige Beispiel-Reduktionen

- $L_{\mathsf{sat}} \preceq_{\mathsf{pol}} L_{\mathsf{3\text{-}CNF\text{-}SAT}}$,
- $L_{\mathsf{sat}} \preceq_{\mathsf{pol}} L_{\mathsf{CNF\text{-}SAT}}$,

NP-vollständige Probleme

Beispiel: SAT $\preceq_{\text{pol}}$ 3-CNF-SAT

1. Schritt: Wir eliminieren $\rightarrow$, $\leftrightarrow$ und ziehen $\neg$ ganz nach innen (NNF)

2. Schritt: Zusätzliche Klammern einführen ($\wedge$, $\vee$ binär)

3. Schritt: Wir ordnen jedem Klammerausdruck A op B (op $\in \{\vee, \wedge\}$) ein neues Atom $P_{A \text{ op} B}$ zu. Das $P_{A \text{ op } B}$ denselben Wahrheitswert erhält wie A op B erzwingen wir durch die Formel $P_{A \text{ op } B} \leftrightarrow (A \text{ op } B)$.

4. Schritt: Wir ersetzen:

$P_{A \vee B} \leftrightarrow (A \vee B)$ durch $(\neg P_{A \vee B} \vee A \vee B) \wedge (\neg A \vee P_{A \vee B}) \wedge (\neg B \vee P_{A \vee B})$

$P_{A \wedge B} \leftrightarrow (A \wedge B)$ durch $(\neg P_{A \wedge B} \vee A) \wedge (\neg P_{A \wedge B} \vee B) \wedge (\neg A \vee \neg B \vee P_{A \wedge B})$

$\mapsto P_F \wedge \text{Rename}(F) =: f(F)$

$F \in$ SAT gdw. F erfüllbare aussagenlogische Formel

gdw. $P_F \wedge \mathit{Rename}(F)$ erfüllbar

gdw. $f(F) \in$ 3-CNF-SAT

Beispiel

Sei F die Formel:

$$[(Q \wedge \neg P \wedge \neg(\neg(\neg Q \vee \neg R))) \vee (Q \wedge \neg P \wedge \neg(Q \wedge \neg P))] \wedge (P \vee R).$$

1. Schritt: Wir eliminieren $\rightarrow$, $\leftrightarrow$ und ziehen $\neg$ ganz nach innen (NNF)

$$F_1 = [(Q \wedge \neg P \wedge (\neg Q \vee \neg R)) \vee (Q \wedge \neg P \wedge (\neg Q \vee P))] \wedge (P \vee R)$$

2. Schritt: Zusätzliche Klammern einführen ($\wedge$, $\vee$ binär)

$$F_2 = [((Q \wedge \neg P) \wedge (\neg Q \vee \neg R)) \vee ((Q \wedge \neg P) \wedge (\neg Q \vee P))] \wedge (P \vee R)$$

3. Schritt: Wir ordnen jedem Klammerausdruck ein neues Atom:

$$\underbrace{\underbrace{[\underbrace{(\underbrace{(Q \wedge \neg P)}_{P_1} \wedge \underbrace{(\neg Q \vee \neg R)}_{P_2})}_{P_6} \vee \underbrace{(\underbrace{(Q \wedge \neg P)}_{P_1} \wedge \underbrace{(\neg Q \vee P)}_{P_4})}_{P_7}]}_{P_8} \wedge \underbrace{(P \vee R)}_{P_5}}_{P_F}.$$

Example

3. Schritt: Wir ordnen jedem Klammerausdruck ein neues Atom: inside).

$$\underbrace{\underbrace{[\underbrace{(\underbrace{(Q \wedge \neg P)}_{P_1} \wedge \underbrace{(\neg Q \vee \neg R)}_{P_2})}_{P_6} \vee \underbrace{(\underbrace{(Q \wedge \neg P)}_{P_1} \wedge \underbrace{(\neg Q \vee P)}_{P_4})}_{P_7}]}_{P_8} \wedge \underbrace{(P \vee R)}_{P_5}}_{P_F}.$$

F ist erfüllbar genau dann, wenn $P_F \wedge \mathrm{Rename}(F)$ erfüllbar:

$$\begin{array}{lllll}
P_F & \wedge & (P_F \leftrightarrow (P_8 \wedge P_5)) & \wedge & (P_1 \leftrightarrow (Q \wedge \neg P)) \\
 & \wedge & (P_8 \leftrightarrow (P_6 \vee P_7)) & \wedge & (P_2 \leftrightarrow (\neg Q \vee \neg R)) \\
 & \wedge & (P_6 \leftrightarrow (P_1 \wedge P_2)) & \wedge & (P_4 \leftrightarrow (\neg Q \vee P)) \\
 & \wedge & (P_7 \leftrightarrow (P_1 \wedge P_4)) & \wedge & (P_5 \leftrightarrow (P \vee R))
\end{array}$$

Example

F ist erfüllbar genau dann, wenn $P_F \wedge \text{Rename}(F)$ erfüllbar:

$$
\begin{array}{llll}
P_F & \wedge \quad (P_F \leftrightarrow (P_8 \wedge P_5) & \wedge & (P_1 \leftrightarrow (Q \wedge \neg P)) \\
 & \wedge \quad (P_8 \leftrightarrow (P_6 \vee P_7)) & \wedge & (P_2 \leftrightarrow (\neg Q \vee \neg R)) \\
 & \wedge \quad (P_6 \leftrightarrow (P_1 \wedge P_2)) & \wedge & (P_4 \leftrightarrow (\neg Q \vee P)) \\
 & \wedge \quad (P_7 \leftrightarrow (P_1 \wedge P_4)) & \wedge & (P_5 \leftrightarrow (P \vee R))
\end{array}
$$

Step 4: CNF berechnen:

$$
\begin{array}{llll}
P_F & \wedge \quad (\neg P_F \vee P_8) \wedge (\neg P_F \vee P_5) & \wedge & (\neg P_1 \vee Q) \wedge (\neg P_1 \vee \neg P) \\
 & \wedge \quad (\neg P_8 \vee \neg P_5 \vee P_F) & \wedge & (\neg Q \vee P \vee P_1) \\
 & \wedge \quad (\neg P_8 \vee P_6 \vee P_7) & \wedge & (\neg P_2 \vee \neg Q \vee \neg R) \\
 & \wedge \quad (\neg P_6 \vee P_8) \wedge (\neg P_7 \vee P_8) & \wedge & (Q \vee P_2) \wedge (R \vee P_2) \\
 & \wedge \quad (\neg P_6 \vee P_1) \wedge (\neg P_6 \vee P_2) & \wedge & (\neg P_4 \vee \neg Q \vee P) \\
 & \wedge \quad (\neg P_1 \vee \neg P_2 \vee P_6) & \wedge & (Q \vee P_4) \wedge (\neg P \vee P_4) \\
 & \wedge \quad (\neg P_7 \vee P_1) \wedge (\neg P_7 \vee P_4) & \wedge & (\neg P_5 \vee P \vee R) \\
 & \wedge \quad (\neg P_1 \vee \neg P_4 \vee P_7) & \wedge & (\neg P \vee P_5) \wedge (\neg R \vee P_5)
\end{array}
$$

NP-vollständige Probleme

- Ist eine logische Formel erfüllbar? (**Satisfiability**)
- Ist ein (un-) gerichteter Graph hamiltonsch? (**Hamiltonian circle**)
- Gibt es in einem Graphen eine Clique der Größe k? (**Clique of size** k)
- Ist ein Graph mit drei Farben zu färben? (3-**colorability**)
- Gibt es in einer Menge von ganzen Zahlen eine Teilmenge mit der Gesamtsumme x? (**Subset Sum**)

NP-vollständige Probleme

Definition [Hamilton Circle]

Hamilton-Kreis: Weg entlang der Kanten in einem Graphen, der jeden Knoten genau einmal besucht und wieder zum Ausgangspunkt zurückkehrt.

$L_{\mathbf{Ham}_{\mathrm{undir}}}$: Die Sprache, die aus allen ungerichteten Graphen besteht, in denen es einen Hamilton-Kreis gibt.

$L_{\mathbf{Ham}_{\mathrm{dir}}}$: Die Sprache, die aus allen gerichteten Graphen besteht, in denen es einen Hamilton-Kreis gibt.

NP-vollständige Probleme

- Ist eine logische Formel erfüllbar? (**Satisfiability**)
- Ist ein (un-) gerichteter Graph hamiltonsch? (**Hamiltonian circle**)
- Gibt es in einem Graphen eine Clique der Größe k? (**Clique of size** k)
- Ist ein Graph mit drei Farben zu färben? (3-**colorability**)
- Gibt es in einer Menge von ganzen Zahlen eine Teilmenge mit der Gesamtsumme x? (**Subset Sum**)

NP-vollständige Probleme

Definition[Maximale Clique: L_{Clique_k}]

Eine **Clique** in einem Graphen ist ein **vollständiger Teilgraph von G**.

Für $k \in \mathbb{N}$:

L_{Clique_k} Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe k enthalten.

$L_{\text{Clique}_{\leq k}}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe $\leq k$ enthalten.

$$L_{\text{Clique}} = \{(G, k) \mid G \text{ ungerichteter Graph, der eine Clique der Größe } k \text{ enthält.}\}$$

NP-vollständige Probleme

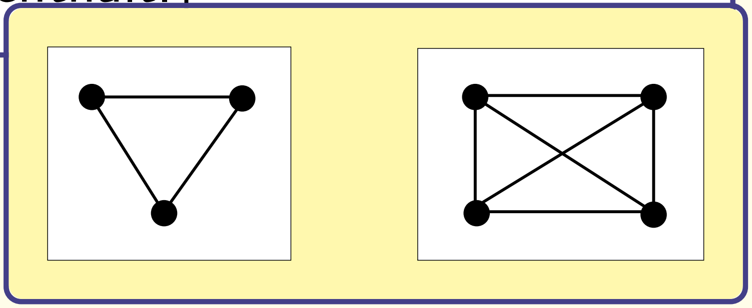
Definition[Maximale Clique: $L_{\textbf{Clique}_k}$]
Eine **Clique** in einem Graphen ist ein **vollständiger Teilgraph von G**.

Für $k \in \mathbb{N}$:

$L_{\textbf{Clique}_k}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe k enthalten.

$L_{\textbf{Clique}_{\leq k}}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe $\leq k$ enthalten.

$L_{\textbf{Clique}} = \{(G, k) \mid G$ ungerichteter Graph, der eine Clique der Größe k enthält.$\}$



NP-vollständige Probleme

Definition[Maximale Clique: $L_{\textbf{Clique}_k}$]

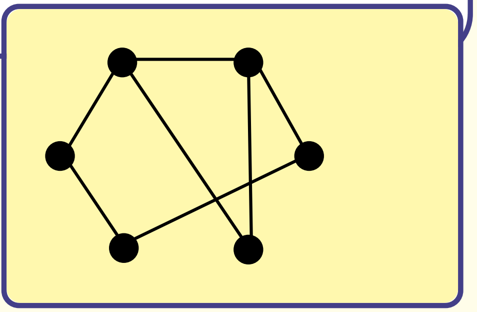
Eine **Clique** in einem Graphen ist ein **vollständiger Teilgraph von G**.

Für $k \in \mathbb{N}$:

$L_{\textbf{Clique}_k}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe k enthalten.

$L_{\textbf{Clique}_{\leq k}}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe $\leq k$ enthalten.

$L_{\textbf{Clique}} = \{(G, k) \mid G$ ungerichteter Graph, der eine Clique der Größe k enthält.$\}$



NP-vollständige Probleme

Definition[Maximale Clique: $L_{\textbf{Clique}_k}$]

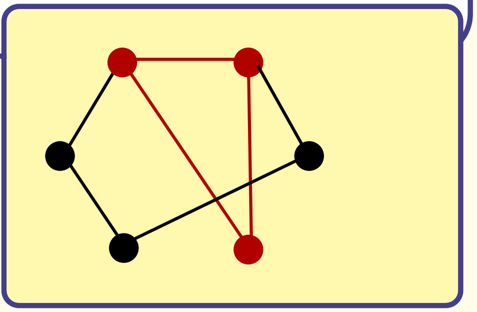
Eine **Clique** in einem Graphen ist ein **vollständiger Teilgraph von G**.

Für $k \in \mathbb{N}$:

$L_{\textbf{Clique}_k}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe k enthalten.

$L_{\textbf{Clique}_{\leq k}}$ Die Sprache, die aus allen ungerichteten Graphen besteht, die eine Clique der Größe $\leq k$ enthalten.

$L_{\textbf{Clique}} = \{(G, k) \mid G$ ungerichteter Graph, der eine Clique der Größe k enthält.$\}$



NP-vollständige Probleme

- Ist eine logische Formel erfüllbar? (**Satisfiability**)
- Ist ein (un-) gerichteter Graph hamiltonsch? (**Hamiltonian circle**)
- Gibt es in einem Graphen eine Clique der Größe k? (**Clique of size** k)
- Ist ein Graph mit drei Farben zu färben? (3-**colorability**)
- Gibt es in einer Menge von ganzen Zahlen eine Teilmenge mit der Gesamtsumme x? (**Subset Sum**)

NP-vollständige Probleme

Definition[k-colorability: $L_{\mathsf{Color}_{\leq k}}$]

Ein (ungerichteter) Graph heißt **k-färbbar**, falls jeder Knoten mit einer von k Farben so gefärbt werden kann, dass benachbarte Knoten verschiedene Farben haben.

Für $k \in \mathbb{N}$:

$L_{\mathsf{Color}_{\leq k}}$ Die Sprache, die aus allen ungerichteten, mit höchstens k Farben färbbaren Graphen besteht.

NP-vollständige Probleme

Einige Beispiel-Reduktionen

- $L_{\mathsf{SAT}} \preceq_{\mathsf{pol}} L_{\mathsf{3\text{-}CNF\text{-}SAT}}$,
- $L_{\mathsf{SAT}} \preceq_{\mathsf{pol}} L_{\mathsf{CNF\text{-}SAT}}$,
- $L_{\mathsf{CNF\text{-}SAT}} \preceq_{\mathsf{pol}} L_{\mathsf{Clique}}$,
- $L_{\mathsf{Ham}_{\mathsf{dir}}} \preceq_{\mathsf{pol}} L_{\mathsf{Ham}_{\mathsf{undir}}}$,
- $L_{\mathsf{3\text{-}CNF\text{-}SAT}} \preceq_{\mathsf{pol}} L_{\mathsf{Color}_{\leq 3}}$.

NP-vollständige Probleme

Beispiel: CNF-SAT $\preceq_{\text{pol}}$ Clique

Gegeben eine Instanz von CNF
(eine Konjunktion von Klauseln $C_1 \wedge C_2 \wedge \ldots \wedge C_k$)

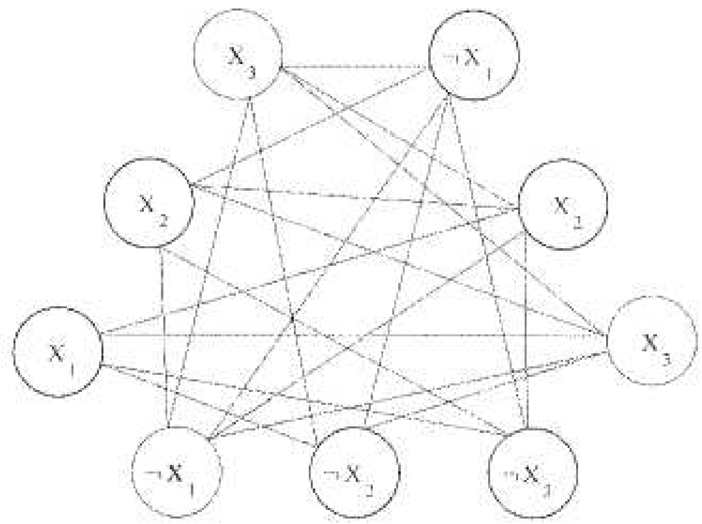
Wir konstruieren daraus einen Graphen G:

Knoten: die Paare (x, i), so dass x ein Literal ist, dass in der Klausel C_i vorkommt.

Kanten: Es gibt eine Kante zwischen (x, i) und (y, j) falls:
(1) $i \neq j$, und
(2) x, y sind nicht komplementär.

Es gilt dann: **Die CNF-Formel $C_1 \wedge C_2 \wedge \ldots \wedge C_k$ ist erfüllbar genau dann, wenn der zugeordnete Graph G eine Clique der Größe k hat genau dann, wenn $(G, k) \in$ Clique.**

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



NP-v

Beispiel: CNF-SAT $\preceq_{\text{pol}}$

Gegeben eine Instanz vo

(eine Konjunktion von K

Wir konstruieren daraus

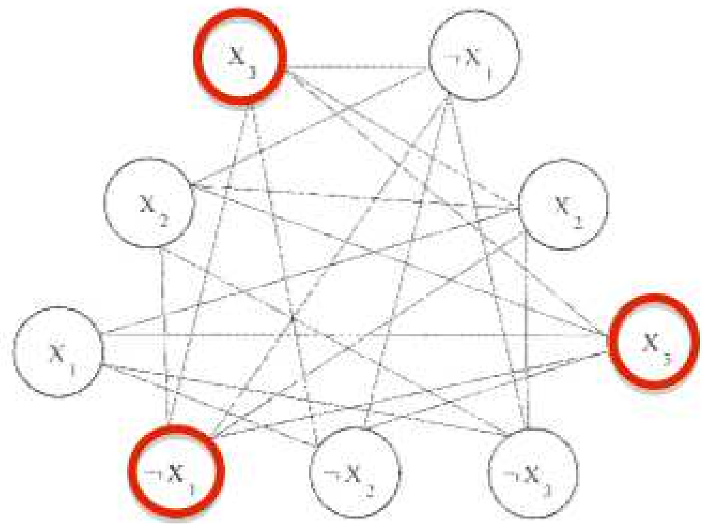
Knoten: die Paare (x, i), so dass x ein Literal ist, dass in der Klausel C_i vorkommt.

Kanten: Es gibt eine Kante zwischen (x, i) und (y, j) falls:
(1) $i \neq j$, und
(2) x, y sind nicht komplementär.

Es gilt dann: **Die CNF-Formel $C_1 \wedge C_2 \wedge \ldots \wedge C_k$ ist erfüllbar genau dann, wenn der zugeordnete Graph G eine Clique der Größe k hat genau dann, wenn $(G, k) \in$ Clique.**

NP-v

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



Beispiel: CNF-SAT $\preceq_{\text{pol}}$

Gegeben eine Instanz vo
(eine Konjunktion von K

Wir konstruieren daraus

Knoten: die Paare (x, i), so dass x ein Literal ist, dass in der Klausel C_i vorkommt.

Kanten: Es gibt eine Kante zwischen (x, i) und (y, j) falls:

(1) $i \neq j$, und

(2) x, y sind nicht komplementär.

Es gilt dann: **Die CNF-Formel $C_1 \wedge C_2 \wedge \ldots \wedge C_k$ ist erfüllbar genau dann, wenn der zugeordnete Graph G eine Clique der Größe k hat genau dann, wenn $(G, k) \in$ Clique.**

NP-vollständige Probleme

- Ist eine logische Formel erfüllbar? (**Satisfiability**)
- Ist ein (un-) gerichteter Graph hamiltonsch? (**Hamiltonian circle**)
- Gibt es in einem Graphen eine Clique der Größe k? (**Clique of size** k)
- Ist ein Graph mit drei Farben zu färben? (3-**colorability**)
- Gibt es in einer Menge von ganzen Zahlen eine Teilmenge mit der Gesamtsumme x? (**Subset Sum**)

Übersicht

1. Motivation
2. Terminologie
3. Endliche Automaten und reguläre Sprachen
4. Kellerautomaten und kontextfreie Sprachen
5. Turingmaschinen und rekursiv aufzählbare Sprachen
6. Berechenbarkeit, (Un-)Entscheidbarkeit
7. Komplexitätsklassen P und NP