Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik

Vorlesung am 30.11.2010

INSTITUT FÜR THEORETISCHE INFORMATIK

Das Problem EXACT COVER

Karlsruher Institut für Technologie

Problem EXACT COVER

Gegeben: Eine endliche Menge X und eine Familie $\mathcal{S}$ von Teilmengen von X.

Frage: Existiert eine Menge $\mathcal{S}' \subseteq \mathcal{S}$, so dass jedes Element aus X in genau einer Menge aus $\mathcal{S}'$ liegt?

Das Problem EXACT COVER

Karlsruher Institut für Technologie

Problem EXACT COVER

Gegeben: Eine endliche Menge X und eine Familie $\mathcal{S}$ von Teilmengen von X.

Frage: Existiert eine Menge $\mathcal{S}' \subseteq \mathcal{S}$, so dass jedes Element aus X in genau einer Menge aus $\mathcal{S}'$ liegt?

Beispiel:

$$X = \{1, 2, \ldots, 7\}$$
$$\mathcal{S} = \{\{1,2,3\}, \{1,2,4\}, \{2,3,4\}, \{1,3,4\}, \{1,5\}, \{3,5\}, \{1,3\}, \{5,6,7\}, \{4,5,6\}, \{4,5,7\}, \{4,6,7\}, \{5,6\}, \{5,7\}, \{6,7\}\}$$

Ist $(X, \mathcal{S})$ eine Ja-Instanz?

Das Problem EXACT COVER

Karlsruher Institut für Technologie

Problem EXACT COVER

Gegeben: Eine endliche Menge X und eine Familie $\mathcal{S}$ von Teilmengen von X.

Frage: Existiert eine Menge $\mathcal{S}' \subseteq \mathcal{S}$, so dass jedes Element aus X in genau einer Menge aus $\mathcal{S}'$ liegt?

Beispiel:

$$
\begin{aligned}
X &= \{1, 2, \ldots, 7\} \\
\mathcal{S} &= \{\{1,2,3\}, \{1,2,4\}, \{2,3,4\}, \{1,3,4\}, \{1,5\}, \{3,5\}, \{1,3\}, \\
&\quad \{5,6,7\}, \{4,5,6\}, \{4,5,7\}, \{4,6,7\}, \{5,6\}, \{5,7\}, \{6,7\}\} \\
\mathcal{S}' &= \{\{1,5\}, \{2,3,4\}, \{6,7\}\}
\end{aligned}
$$

Ja

Das Problem EXACT COVER

Karlsruher Institut für Technologie

Problem EXACT COVER

Gegeben: Eine endliche Menge X und eine Familie $\mathcal{S}$ von Teilmengen von X.

Frage: Existiert eine Menge $\mathcal{S}' \subseteq \mathcal{S}$, so dass jedes Element aus X in genau einer Menge aus $\mathcal{S}'$ liegt?

Satz:
Problem EXACT COVER ist $\mathcal{NP}$–vollständig.

Beweis: NP-Vollständigkeit von EXACT COVER

Karlsruher Institut für Technologie

EXACT COVER $\in \mathcal{NP}$

- Es kann in Polynomialzeit überprüft werden, ob eine Teilmenge $\mathcal{S}' \subseteq \mathcal{S}$ aus disjunkten Mengen besteht und X überdeckt.

Beweis: NP-Vollständigkeit von EXACT COVER

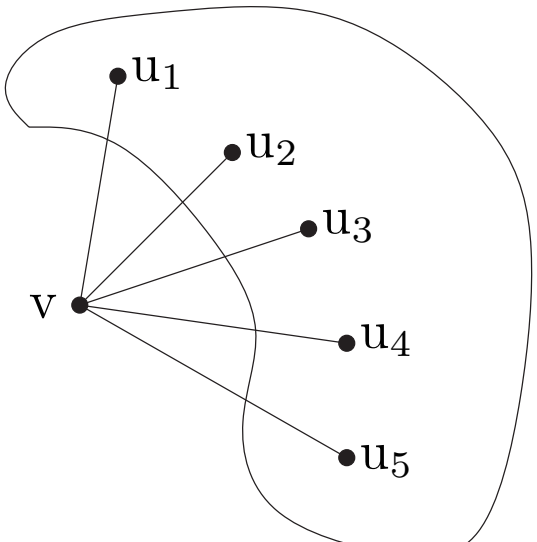
Karlsruher Institut für Technologie

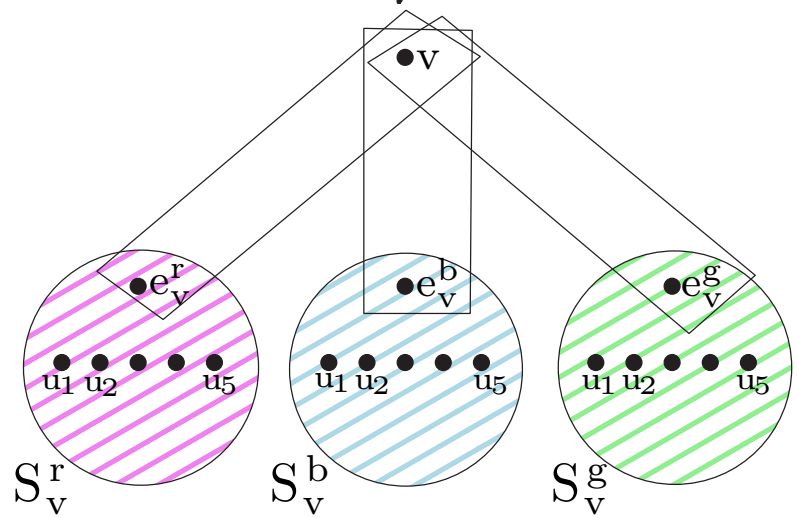
3COLOR $\propto$ EXACT COVER

- Sei $G = (V, E)$ eine 3COLOR-Instanz
- Wir konstruieren in Polynomialzeit eine EXACT COVER-Instanz $(X, \mathcal{S})$
- Es soll gelten: G ist 3-färbbar $\Leftrightarrow$ $(X, \mathcal{S})$ ist erfüllbar

Konstruktion von (X,S)

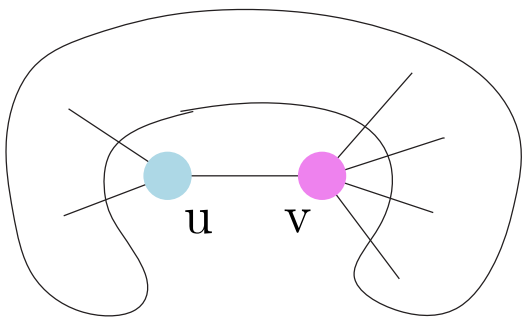
- Sei $C = \{r(ot), b(lau), g(rün)\}$
- Sei $N(v) := \{u \in V : \{u, v\} \in E\}$ die Nachbarschaft von v.
- Für jedes $v \in V$ enthalte X ein „Element“ v und jeweils $3 \cdot |N(v)| + 3$ zusätzliche Elemente.
- Zu jedem $v \in V$ gebe es in $\mathcal{S}$ drei disjunkte Mengen S_v^r, S_v^b, S_v^g mit jeweils $|N(v)| + 1$ Elementen.
- Außerdem enthalte $\mathcal{S}$ für jedes v drei zweielementige Mengen $\{v, e_v^r\}, \{v, e_v^b\}$ und $\{v, e_v^g\}$ mit $e_v^r \in S_v^r$, $e_v^b \in S_v^b$ und $e_v^g \in S_v^g$.
- **Interpretation:** S_v^r entspricht der „Farbe“ r, enthält für jeden Knoten aus $N(v)$ eine Kopie und einen zusätzlichen Knoten e_v^r.

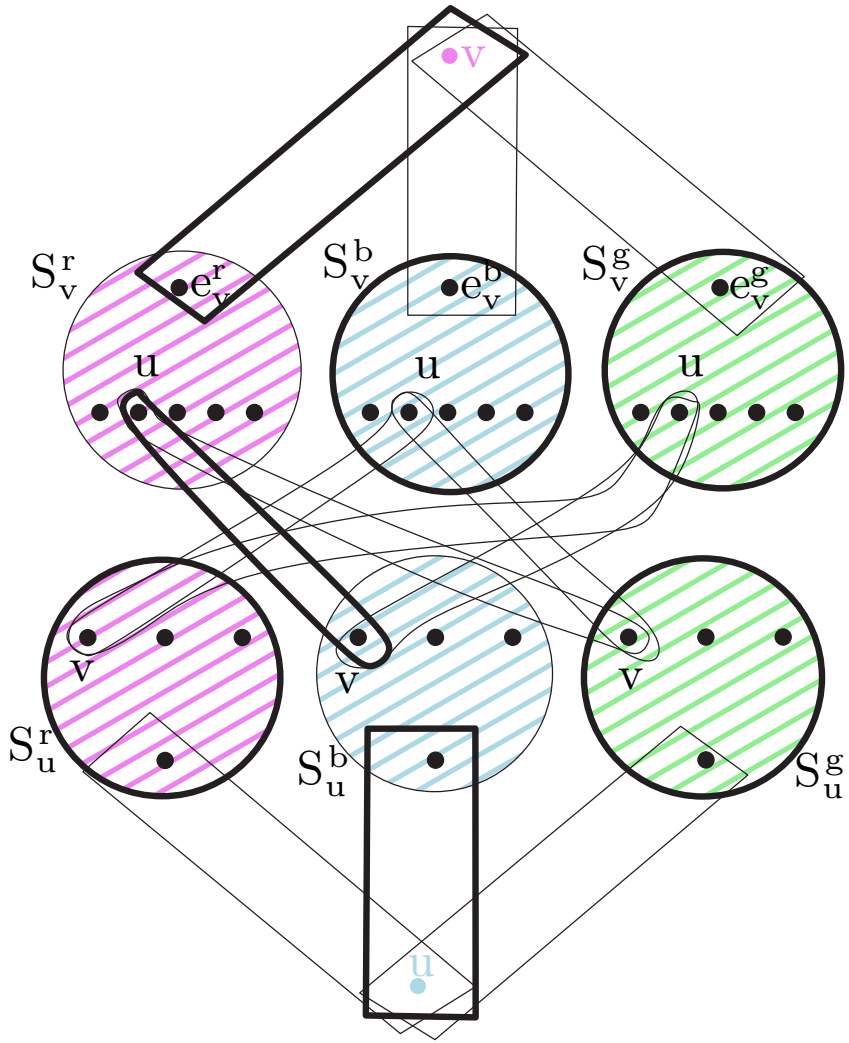




Konstruktion von (X,S)

- Außerdem enthält $\mathcal{S}$ für jede Kante $\{u, v\} \in E$ und je zwei $c, c' \in C$, $c \neq c'$, die zweielementigen Mengen $\{u_v^c, v_u^{c'}\}$, $u_v^c \in S_v^c$ „Kopie“ von u, $v_u^{c'} \in S_u^{c'}$ „Kopie“ von v.





Konstruktion von (X,S)

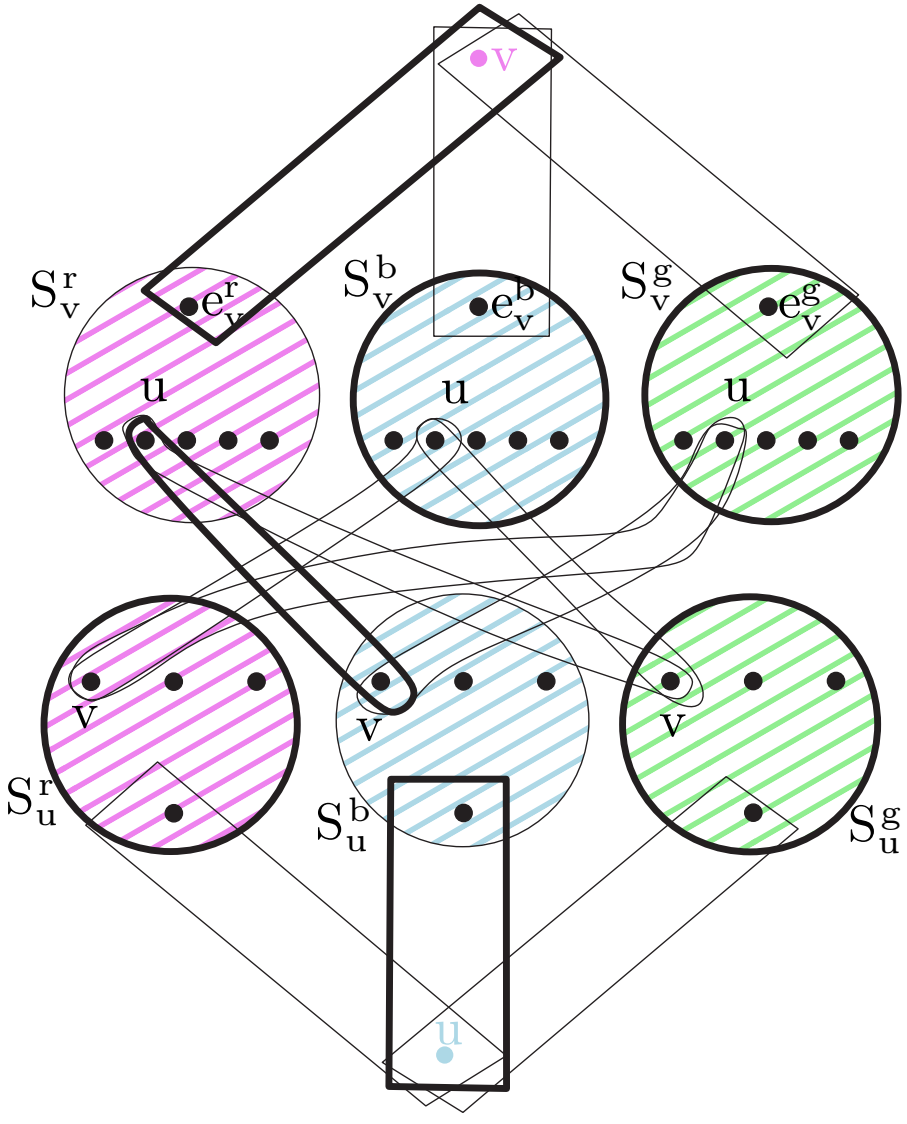
- Die Konstruktion ist polynomial.

Noch zu zeigen:

- G ist 3-färbbar $\Leftrightarrow$ $(X, \mathcal{S})$ ist erfüllbar

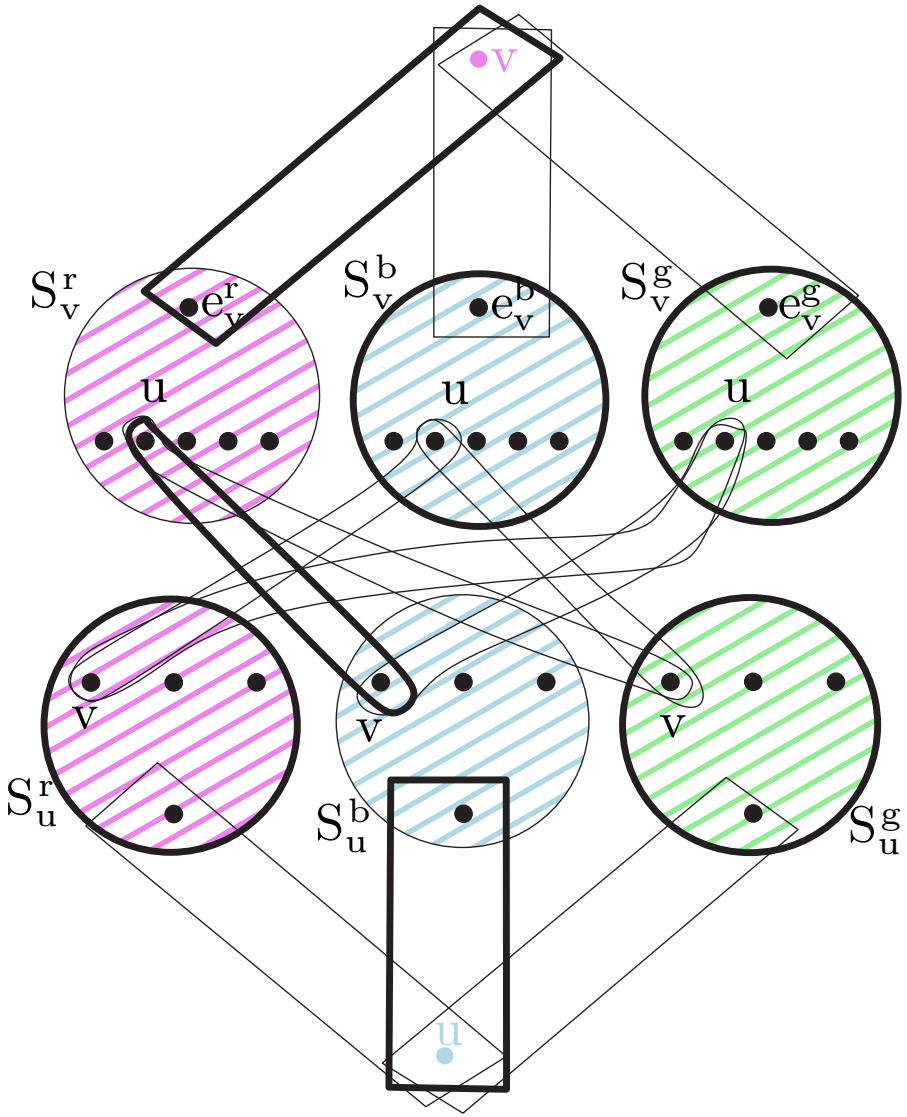
G dreifärbbar $\Rightarrow$ (X,S) hat exakte Überdeckung

- Sei $\chi : V \to C$ eine zulässige Dreifärbung.
- $\mathcal{S}'$ enthalte für jedes $v \in V$ die Mengen $\{v, e_v^{\chi(v)}\}$ und S_v^c mit $c \neq \chi(v)$.
- Diese Mengen überdecken alle Elemente exakt, außer den Elementen der Form $u_v^{\chi(v)}$, $v_u^{\chi(u)}$ für $\{u, v\} \in E$.
- Daher enthalte $\mathcal{S}'$ für jede Kante $\{u, v\} \in E$ die Menge $\{u_v^{\chi(v)}, v_u^{\chi(u)}\}$.
- Diese Menge existiert, da $\chi(u) \neq \chi(v)$, und damit überdeckt $\mathcal{S}'$ jedes Element aus X genau einmal.



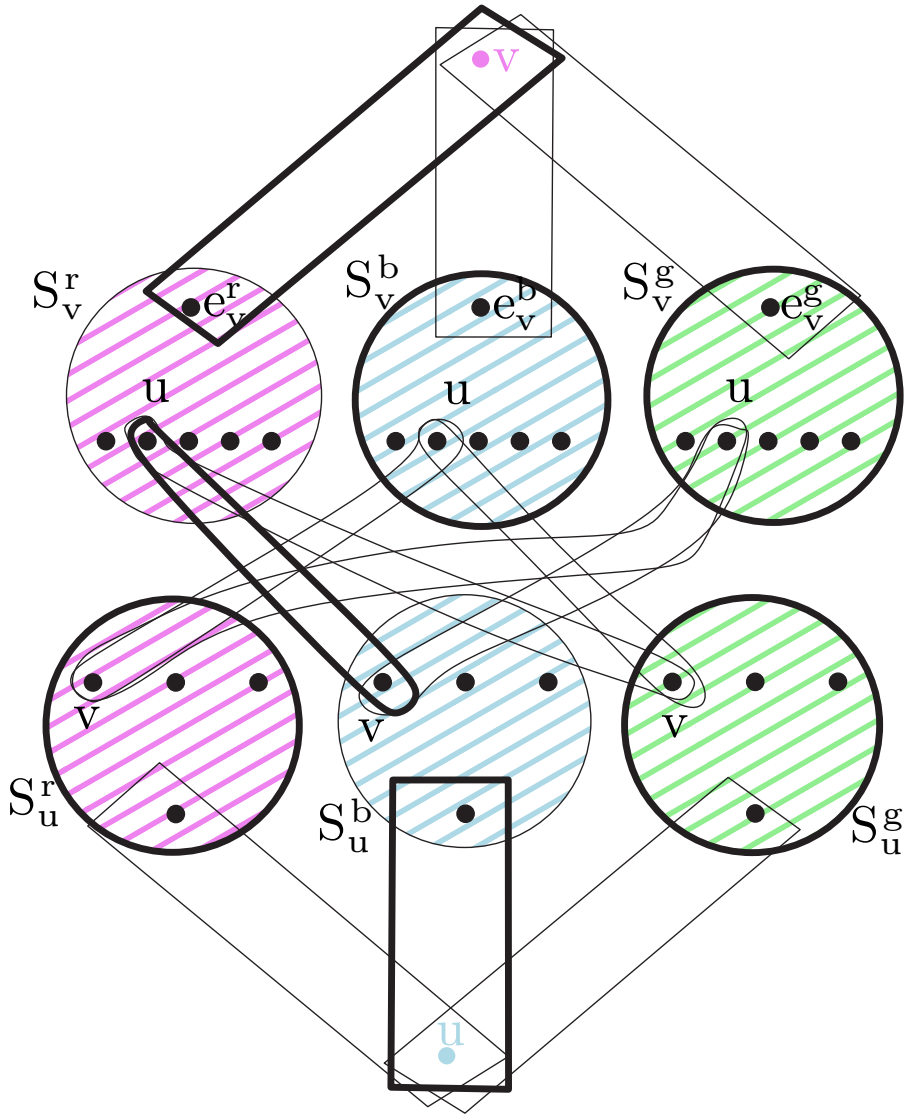
G dreifärbbar $\Leftarrow$ (X,S) hat exakte Überdeckung

- Sei also $\mathcal{S}'$ eine exakte Überdeckung.
- Jedes Element v muss von genau einer Menge der Form $\{v, e_v^c\}$ überdeckt sein.
- Dies induziert eine Färbung χ von G mit den Farben r, b und g.
- Wir müssen beweisen, dass diese Färbung zulässig ist
- Da für jedes v bereits $\{v, e_v^{\chi(v)}\} \in S'$, kann e_v^c mit $c \neq \chi(v)$ nur durch die Menge S_v^c überdeckt werden.



G dreifärbbar $\Leftarrow$ (X,S) hat exakte Überdeckung

- Da für jedes v bereits $\{v, e_v^{\chi(v)}\} \in S'$, kann e_v^c mit $c \neq \chi(v)$ nur durch die Menge S_v^c überdeckt werden.
- Da die Mengen der Form $\{v, e_v^{\chi(v)}\}$ und S_v^c, $c \neq \chi(v)$, alle Elemente außer den $u_v^{\chi(v)}$ mit $\{u, v\} \in E$ überdecken, müssen auch die Mengen $\{u_v^{\chi(v)}, v_u^{\chi(u)}\}$ für $\{u, v\} \in E$ in S' enthalten sein.
- Für diese gilt per Konstruktion $\chi(v) \neq \chi(u)$.



Das Problem SUBSET SUM

Karlsruher Institut für Technologie

Problem SUBSET SUM

Gegeben: Eine endliche Menge M, eine Gewichtsfunktion $w : M \to \mathbb{N}_0$ und $K \in \mathbb{N}_0$

Frage: Existiert eine Teilmenge $M' \subseteq M$ mit $\sum_{a \in M'} w(a) = K$?

Satz:
Problem SUBSET SUM ist $\mathcal{NP}$–vollständig.

NP-Vollständigkeit von SUBSET SUM

SUBSET SUM $\in \mathcal{NP}$.

- Es kann für eine gegebene Teilmenge $M' \subseteq M$ in Polynomialzeit der Wert $\sum_{a \in M'} w(a)$ ausgerechnet und mit K verglichen werden.

Beweis: NP-Vollständigkeit von SUBSET SUM

EXACT COVER $\propto$ SUBSET SUM

- Sei $(X = \{0, 1, \ldots, m-1\}, \mathcal{S})$ EXACT COVER-Instanz.
- Konstruiere SUBSET SUM Instanz (M, w, K)

$$
\begin{aligned}
M &:= \mathcal{S} \\
\#x &:= \left|\{Y \in \mathcal{S} : x \in Y\}\right| \\
p &:= \max_{x \in X} \#x + 1 \\
w(Y) &:= \sum_{x \in Y} p^x \\
K &:= \sum_{x=0}^{m-1} p^x
\end{aligned}
$$

- Die Konstruktion benötigt nur Polynomialzeit.

Beweis: NP-Vollständigkeit von SUBSET SUM

$$
\begin{aligned}
M &:= \mathcal{S} \\
\#x &:= |\{Y \in \mathcal{S} : x \in Y\}| \\
p &:= \max_{x \in X} \#x + 1 \\
w(Y) &:= \sum_{x \in Y} p^x \\
K &:= \sum_{x=0}^{m-1} p^x
\end{aligned}
$$

Veranschaulichung:

- Wir stellen die Mengenzugehörigkeiten als Zahlen zur Basis p dar.
- Kodiere $w(Y)$ für $Y \in \mathcal{S}$ als String aus Nullen und Einsen der Länge m, wobei an i-ter Stelle eine 1 steht genau dann, wenn $i \in Y$;
- entsprechend ist K ein String der Länge m aus Einsen

Beweis: NP-Vollständigkeit von SUBSET SUM

$$
\begin{aligned}
M &:= \mathcal{S} \\
\#x &:= |\{Y \in \mathcal{S} : x \in Y\}| \\
p &:= \max_{x \in X} \#x + 1 \\
w(Y) &:= \sum_{x \in Y} p^x \\
K &:= \sum_{x=0}^{m-1} p^x
\end{aligned}
$$

Veranschaulichung:

- Komponentenweise Addition der zu Teilmenge $Y_1, \ldots, Y_n$ von $\mathcal{S}$ gehörigen Strings $w(Y_1), \ldots, w(Y_n)$ ergibt einen String der Länge m, an dessen i-ter Stelle steht in wievielen der $Y_j (j = 1, \ldots, n)$ das Element i vorkommt.
- $\sum_{Y \in \mathcal{S}'} w(Y) = K$ bedeutet also, dass jedes $x \in X$ in genau einem $Y \in \mathcal{S}'$ vorkommt.

Beweis: NP-Vollständigkeit von SUBSET SUM

$$
\begin{aligned}
M &:= \mathcal{S} \\
\#x &:= |\{Y \in \mathcal{S} : x \in Y\}| \\
p &:= \max_{x \in X} \#x + 1 \\
w(Y) &:= \sum_{x \in Y} p^x \\
K &:= \sum_{x=0}^{m-1} p^x
\end{aligned}
$$

Beispiel:

$X = \{0, 1, 2, 3, 4, 5, 6\}$,
$\mathcal{S} = \{Y_1 = \{0, 1, 2, 3\}, Y_2 = \{2, 5\}, Y_3 = \{3, 4, 5\}, Y_4 = \{4, 5, 6\}\}$

$\#0 = 1, \#1 = 1, \#2 = 2, \#3 = 2, \#4 = 2, \#5 = 3, \#6 = 1, p = 4$
$w(Y_1) = 0001111_4$, $w(Y_2) = 0100100_4$,
$w(Y_3) = 0111000_4$, $w(Y_4) = 1110000_4$

Beweis: NP-Vollständigkeit von SUBSET SUM

$$
\begin{aligned}
M &:= \mathcal{S} \\
\#x &:= |\{Y \in \mathcal{S} : x \in Y\}| \\
p &:= \max_{x \in X} \#x + 1 \\
w(Y) &:= \sum_{x \in Y} p^x \\
K &:= \sum_{x=0}^{m-1} p^x
\end{aligned}
$$

- $(X, \mathcal{S})$ lösbar $\Rightarrow$ (M, w, K) lösbar.

Sei $\mathcal{S}' \subseteq \mathcal{S}$ exakte Überdeckung von $(X, \mathcal{S})$. Dann gilt

$$\sum_{Y \in \mathcal{S}'} w(Y) = \sum_{Y \in \mathcal{S}'} \sum_{x \in Y} p^x = \sum_{x=0}^{m-1} p^x = K$$

da jedes $x \in X$ genau einmal überdeckt wird.
$\mathcal{S}'$ erfüllt also die Bedingung für SUBSET SUM.

Beweis: NP-Vollständigkeit von SUBSET SUM

$$
\begin{aligned}
M &:= \mathcal{S} \\
\#x &:= |\{Y \in \mathcal{S} : x \in Y\}| \\
p &:= \max_{x \in X} \#x + 1 \\
w(Y) &:= \sum_{x \in Y} p^x \\
K &:= \sum_{x=0}^{m-1} p^x
\end{aligned}
$$

- $(X, \mathcal{S})$ lösbar $\Leftarrow (M, w, K)$ lösbar.

Ist $\mathcal{S}' \subseteq M = \mathcal{S}$ eine geeignete Menge für SUBSET SUM, so gilt

$$\sum_{Y \in \mathcal{S}'} w(Y) = K = \sum_{x=0}^{m-1} p^x.$$

Also kommt jedes $x \in X$ in genau einem $Y \in \mathcal{S}'$ vor.
Damit ist $\mathcal{S}'$ eine exakte Überdeckung.

Das Problem PARTITION

Problem PARTITION

Gegeben: Eine endliche Menge M und eine Gewichtsfunktion $w : M \to \mathbb{N}_0$.

Frage: Existiert eine Teilmenge $M' \subseteq M$ mit $\sum_{a \in M'} w(a) = \sum_{a \in M \setminus M'} w(a)$?

Satz:
Problem PARTITION ist $\mathcal{NP}$–vollständig.

Beweis: NP-Vollständigkeit von PARTITION

PARTITION $\in \mathcal{NP}$.

- Für eine Menge M' können in Polynomialzeit die Werte $\sum_{a \in M'} w(a)$ und $\sum_{a \in M \setminus M'} w(a)$ ausgerechnet und verglichen werden.

Beweis: NP-Vollständigkeit von PARTITION

Karlsruher Institut für Technologie

SUBSET SUM $\propto$ PARTITION.

- Sei (M, w, K) eine SUBSET SUM-Instanz
- Konstruiere PARTITION-Instanz (M^*, w^*)

$$
\begin{aligned}
N &:= \sum_{a \in M} w(a) + 1 \\
M^* &:= M \cup \{b, c\} \\
w^*(a) &= w(a) \qquad \text{für } a \in M \\
w^*(b) &:= N - K \\
w^*(c) &:= K + 1
\end{aligned}
$$

- Die Konstruktion benötigt nur Polynomialzeit.

Beweis: NP-Vollständigkeit von PARTITION

$$
\begin{aligned}
N &:= \sum_{a \in M} w(a) + 1 \\
M^* &:= M \cup \{b, c\} \\
w^*(a) &= w(a) \quad \text{für } a \in M \\
w^*(b) &:= N - K \\
w^*(c) &:= K + 1
\end{aligned}
$$

- (M, w, K) Ja-Instanz genau dann, wenn (M^*, w^*) Ja-Instanz:

$$\exists M' \subseteq M^* \text{ mit } \sum_{a \in M'} w^*(a) = \sum_{a \in M^* \setminus M'} w^*(a) \iff \exists M'' \subseteq M \text{ mit } w(M'') = K.$$

- Es können b und c nicht beide in M' bzw. $M^* \setminus M'$ enthalten sein
- o.B.d.A. $b \in M'$

Beweis: NP-Vollständigkeit von PARTITION

$$
\begin{aligned}
N &:= \sum_{a \in M} w(a) + 1 \\
M^* &:= M \cup \{b, c\} \\
w^*(a) &= w(a) \quad \text{für } a \in M \\
w^*(b) &:= N - K \\
w^*(c) &:= K + 1
\end{aligned}
$$

- (M, w, K) Ja-Instanz genau dann, wenn (M^*, w^*) Ja-Instanz:

$$\exists M' \subseteq M^* \text{ mit } \sum_{a \in M'} w^*(a) = \sum_{a \in M^* \setminus M'} w^*(a) \iff \exists M'' \subseteq M \text{ mit } w(M'') = K.$$

$\Rightarrow$

- Sei M', so dass $\sum_{a \in M'} w^*(a) = \sum_{a \in M^* \setminus M'} w^*(a)$
- Dann gilt $w(M') = N$, da $w(M^*) = 2N$
- Damit erfüllt $M'' := M' \setminus \{b\}$ die Bedingung für SUBSET SUM.

Beweis: NP-Vollständigkeit von PARTITION

$$
\begin{aligned}
N &:= \sum_{a \in M} w(a) + 1 \\
M^* &:= M \cup \{b, c\} \\
w^*(a) &= w(a) \quad \text{für } a \in M \\
w^*(b) &:= N - K \\
w^*(c) &:= K + 1
\end{aligned}
$$

- (M, w, K) Ja-Instanz genau dann, wenn (M^*, w^*) Ja-Instanz:

$$\exists M' \subseteq M^* \text{ mit } \sum_{a \in M'} w^*(a) = \sum_{a \in M^* \setminus M'} w^*(a) \iff \exists M'' \subseteq M \text{ mit } w(M'') = K.$$

$\Leftarrow$

- Sei M'', so dass $w(M'') = K$
- Dann erfüllt $M' := M'' \cup \{b\}$ die Bedingung für PARTITION.

Das Problem KNAPSACK

Karlsruher Institut für Technologie

Problem KNAPSACK

Gegeben: Eine endliche Menge M,
eine Gewichtsfunktion $w : M \to \mathbb{N}_0$,
eine Kostenfunktion $c : M \to \mathbb{N}_0$
$W, C \in \mathbb{N}_0$.

Frage: Existiert eine Teilmenge $M' \subseteq M$ mit $\sum_{a \in M'} w(a) \leq W$ und $\sum_{a \in M'} c(a) \geq C$?

Satz:
Problem KNAPSACK ist $\mathcal{NP}$–vollständig.

Beweis: NP-Vollständigkeit von KNAPSACK

KNAPSACK $\in \mathcal{NP}$.

- Für eine Menge M' kann in Polynomialzeit überprüft werden, ob
  - $\sum_{a \in M'} w(a) \leq W$ und
  - $\sum_{a \in M'} c(a) \geq C$

  gilt.

Beweis: NP-Vollständigkeit von KNAPSACK

PARTITION $\propto$ KNAPSACK.

- Sei (M, w) eine PARTITION-Instanz
- Konstruiere KNAPSACK-Instanz (M, w', c, W, C)

$$\begin{aligned} w' &:= 2w \\ c &:= 2w \\ W = C &:= \sum_{a \in M} w(a) \end{aligned}$$

- Die Konstruktion benötigt nur Polynomialzeit.
- Es ist (M, w) genau dann eine Ja-Instanz, wenn (M, w', c, W, C) eine Ja-Instanz ist (ohne Beweis)

Auswirkung auf die Frage $\mathcal{P}$=$\mathcal{NP}$

- Wir haben gesehen, dass es für je zwei $\mathcal{NP}$–vollständige Probleme eine polynomiale Transformation von einem zum anderen Problem gibt.
- Deshalb sind alle $\mathcal{NP}$–vollständigen Probleme im wesentlichen gleich schwer
- Dies hat Auswirkungen auf die Frage, ob $\mathcal{P} = \mathcal{NP}$ ist.

Satz:
Sei L $\mathcal{NP}$-vollständig, dann gilt:

- $L \in \mathcal{P} \Longrightarrow \mathcal{P} = \mathcal{NP}$
- $L \notin \mathcal{P} \Longrightarrow$ für jede $\mathcal{NP}$-vollständigen Sprache L' gilt $L' \notin \mathcal{P}$

Auswirkung auf die Frage $\mathcal{P}$=$\mathcal{NP}$

Beweis: L $\mathcal{NP}$**-vollständig,** $L \in \mathcal{P} \Longrightarrow \mathcal{P} = \mathcal{NP}$

- Sei $L \in \mathcal{P}$ und L $\mathcal{NP}$-vollständig.
- Dann existiert eine polynomiale deterministische TM M für L.
- Sei $L' \in \mathcal{NP}$
- Es gibt polynomiale Transformation $L' \propto L$
- Hintereinanderausführung von $L' \propto L$ und M liefert deterministische polynomielle TM-Berechnung für L'.
- Damit ist $L' \in \mathcal{P}$.

Auswirkung auf die Frage $\mathcal{P}$=$\mathcal{NP}$

Beweis: L $\mathcal{NP}$**-vollständig,** $L \notin \mathcal{P}$
$\Longrightarrow$ **für jede** $\mathcal{NP}$**-vollständigen Sprache** L' **gilt** $L' \notin \mathcal{P}$

- Sei $L \notin \mathcal{P}$ und L $\mathcal{NP}$-vollständig.
- Angenommen für eine $\mathcal{NP}$-vollständige Sprache L' gilt: $L' \in \mathcal{P}$
- Dann folgt aus Teil 1 des Satzes $\mathcal{P} = \mathcal{NP}$.
- Dies ist aber ein Widerspruch zur Voraussetzung $L \notin \mathcal{P}$.

Zusammenfassung

- Die Klasse $\mathcal{P}$ ist die Klasse aller Entscheidungsprobleme/Sprachen die mit einer **deterministischen** Turingmaschine in polynomieller Zeit gelöst werden können
- Die Klasse $\mathcal{NP}$ ist die Klasse aller Entscheidungsprobleme/Sprachen die mit einer **nicht-deterministischen** Turingmaschine in polynomieller Zeit gelöst werden können
- Informell ausgedrückt: Π gehört zu $\mathcal{NP}$, falls Π folgende Eigenschaft hat: Ist die Antwort bei Eingabe eines Beispiels *I* von Π Ja, dann kann die Korrektheit der Antwort in polynomialer Zeit überprüft werden.

Zusammenfassung

- Eine **polynomiale Transformation** einer Sprache $L_1 \subseteq \Sigma_1^*$ in eine Sprache $L_2 \subseteq \Sigma_2^*$ ist eine Funktion $f\colon \Sigma_1^* \to \Sigma_2^*$ mit den Eigenschaften:
  - es existiert eine polynomiale deterministische Turing-Maschine, die f berechnet;
  - für alle $x \in \Sigma_1^*$ gilt: $x \in L_1 \Leftrightarrow f(x) \in L_2$.

- Eine Sprache L heißt $\mathcal{NP}$**–vollständig**, falls gilt:
  - $L \in \mathcal{NP}$ und
  - für alle $L' \in \mathcal{NP}$ gilt $L' \propto L$ ($\mathcal{NP}$-Schwere).

- **Bedeutung**: Unter der Annahme $\mathcal{P} \neq \mathcal{NP}$ gibt es kein polynomielles Lösungsverfahren für ein $\mathcal{NP}$-vollständges Problem.

Zusammenfassung

- Mit dem Satz von Cook haben wir direkt gezeigt, dass Problem SAT $\mathcal{NP}$-schwer ist

- Bei allen anderen Problemen haben wir polynomielle Transformationen (Reduktionen) benutzt um die $\mathcal{NP}$-Schwere nachzuweisen:

$$\text{SAT} \propto \text{3SAT} \propto \text{3COLOR} \propto \text{EXACT COVER} \propto \text{SUBSET SUM} \propto \text{PARTITION} \propto \text{KNAPSACK}$$