Weitere $\mathbb{NP}$-vollständige Probleme

Im folgenden soll die $\mathbb{NP}$-Vollständigkeit einiger weiterer Probleme nachgewiesen werden. Diese Probleme stammen aus der Aussagenlogik (Erfüllbarkeitsproblem **SAT** und sein Spezialfall **3SAT**), aus der Graphentheorie (**Clique**) sowie aus der Arithmetik (**SubsetSum**). Für alle diese Probleme ist es sehr einfach, die Zugehörigkeit zu $\mathbb{NP}$ zu beweisen (jeweils "Raten und Überprüfen"). Es sind deshalb in den Sätzen nur die Reduktionen angegeben.

Das Erfüllbarkeitsproblem der Aussagenlogik (SAT)

Zunächst sollen die für das Verständnis unmittelbar notwendigen Definitionen angegeben werden. Eine umfassende Einführung in die Aussagenlogik findet man z.B. in dem Buch *Logik für Informatiker* von Dassow, 2005.

- Ein *Literal* über der Menge von Variablen var ist ein Wort der Form x bzw. $\neg x$, mit $x \in var$.
- Eine *Klausel* über var ist eine endliche Menge von Literalen.
- Eine *Belegung* ist eine Abbildung $\beta : var \to \{0, 1\}$.
- Der *Wert* $w_\beta(\ell)$ eines Literals ℓ unter der Belegung β ist definiert als $\beta(x)$, falls $\ell = x$ für eine Variable x bzw. als $1 - \beta(x)$, falls $\ell = \neg x$ für eine Variable x.
- Eine Klausel K wird durch eine Belegung β erfüllt, wenn es ein Literal $\ell \in K$ mit $w_\beta(\ell) = 1$ gibt.
- Eine Menge $\mathcal{K}$ von Klauseln wird durch eine Belegung β erfüllt, wenn jede Klausel in $\mathcal{K}$ durch β erfüllt wird.
  $\mathcal{K}$ heißt *erfüllbar*, wenn es eine Belegung β gibt, die $\mathcal{K}$ erfüllt.

(Wie aus der Logik bekannt ist, sind Mengen von Klauseln und aussagenlogische Ausdrcke in konjunktiver Normalform äquivalent zueinander.)

Erfüllbarkeitsproblem **SAT**

Eingabe:	Endliche Menge $\mathcal{K}$ von Klauseln.
Frage:	Ist $\mathcal{K}$ erfüllbar?

Satz 1 **Domino** $\leq_p$ **SAT**.

Beweis. Es sei (Π, R) eine Eingabe für das Dominoproblem über dem Alphabet Σ, wobei R aus den Wörtern $o_1 o_2 \cdots o_n$, $u_1 u_2 \cdots u_n$, $l_1 l_2 \cdots l_m$ und $r_1 r_2 \cdots r_m$ am oberen, unteren, linken bzw. rechten Rand bestehe.

Für jeden Dominostein $p \in \Pi$ sowie alle $1 \leq i \leq m, 1 \leq j \leq n$ führen wir die aussagenlogischen Variablen $B_{i,j,p}$ ein. Aus (Π, R) wird die Menge $\mathcal{K}$ mit folgenden Klauseln konstruiert:

1. $\{B_{i,j,p} \mid p \in \Pi\}$ für $1 \leq i \leq m, 1 \leq j \leq n$.
2. $\{\neg B_{i,j,p}, \neg B_{i,j,q}\}$ für $p, q \in \Pi, p \neq q$, $1 \leq i \leq m, 1 \leq j \leq n$.
3. $\{B_{1,j,p} \mid p \in \Pi \text{ und } \mathrm{pr}_1(p) = o_j\}$ für $1 \leq j \leq n$.
4. $\{B_{m,j,p} \mid p \in \Pi \text{ und } \mathrm{pr}_3(p) = u_j\}$ für $1 \leq j \leq n$.
5. $\{B_{i,1,p} \mid p \in \Pi \text{ und } \mathrm{pr}_2(p) = l_i\}$ für $1 \leq i \leq m$.
6. $\{B_{i,n,p} \mid p \in \Pi \text{ und } \mathrm{pr}_4(p) = r_i\}$ für $1 \leq i \leq m$.
7. $\{\neg B_{i,j,p}\} \cup \{B_{i,j+1,q} \mid q \in \Pi \text{ und } \mathrm{pr}_4(p) = \mathrm{pr}_2(q)\}$ für $p \in \Pi$, $1 \leq i \leq m, 1 \leq j \leq n-1$.
8. $\{\neg B_{i,j,p}\} \cup \{B_{i+1,j,q} \mid q \in \Pi \text{ und } \mathrm{pr}_3(p) = \mathrm{pr}_1(q)\}$ für $p \in \Pi$, $1 \leq i \leq m-1, 1 \leq j \leq n$.

Es ist zu zeigen, dass die Konstruktion von $\mathcal{K}$ tatsächlich eine Reduktion darstellt, d.h. dass $\mathcal{K}$ genau dann erfüllbar ist, wenn (Π, R) eine Lösung besitzt. Sei zunächst $A_{i,j} \in \Pi(1 \leq i \leq m, 1 \leq j \leq n)$ eine korrekte Auslegung für (Π, R). Dann definieren wir die Belegung β vermöge: $\beta(B_{i,j,\alpha}) = 1$ genau dann, wenn $A_{i,j} = \alpha$.

Wir überprüfen im Folgenden, dass β eine erfüllende Belegung für $\mathcal{K}$ darstellt:

1. Jede Klausel $\{B_{i,j,p} \mid p \in \Pi\}$ wird erfüllt, da $\beta(B_{i,j,\alpha}) = 1$ für $\alpha = A_{i,j}$ gilt.
2. Jede Klausel $\{\neg B_{i,j,p}, \neg B_{i,j,q}\}$ mit $p, q \in \Pi, p \neq q$ wird erfüllt, da $p \neq A_{i,j}$ oder $q \neq A_{i,j}$ und folglich $\beta(\neg B_{i,j,p}) = 1$ oder $\beta(\neg B_{i,j,q}) = 1$ gilt.
3. Jede Klausel $\{B_{1,j,p} \mid p \in \Pi \text{ und } \mathrm{pr}_1(p) = o_j\}$ wird erfüllt, da für $p = A_{1,j}$ $\mathrm{pr}_1(p) = \mathrm{pr}_1(A_{1,j}) = o_j$ und $\beta(B_{1,j,p}) = 1$ gilt.
4. Jede Klausel $\{B_{m,j,p} \mid p \in \Pi \text{ und } \mathrm{pr}_3(p) = u_j\}$ wird erfüllt, da für $p = A_{m,j}$ $\mathrm{pr}_3(p) = \mathrm{pr}_3(A_{m,j}) = u_j$ und $\beta(B_{m,j,p}) = 1$ gilt.
5. Jede Klausel $\{B_{i,1,p} \mid p \in \Pi \text{ und } \mathrm{pr}_2(p) = l_i\}$ wird erfüllt, da für $p = A_{i,1}$ $\mathrm{pr}_2(p) = \mathrm{pr}_2(A_{i,1}) = l_i$ und $\beta(B_{i,1,p}) = 1$ gilt.
6. Jede Klausel $\{B_{i,n,p} \mid p \in \Pi \text{ und } \mathrm{pr}_4(p) = l_i\}$ wird erfüllt, da für $p = A_{i,n}$ $\mathrm{pr}_4(p) = \mathrm{pr}_4(A_{i,n}) = r_i$ und $\beta(B_{i,n,p}) = 1$ gilt.
7. Jede Klausel $\{\neg B_{i,j,p}\} \cup \{B_{i,j+1,q} \mid q \in \Pi \text{ und } \mathrm{pr}_4(p) = \mathrm{pr}_2(q)\}$ wird erfüllt, da für $p = A_{i,j}$ und $q = A_{i,j+1}$ $\quad \mathrm{pr}_4(p) = \mathrm{pr}_4(A_{i,j}) = \mathrm{pr}_2(A_{i,j+1}) = \mathrm{pr}_2(q)$ und $\beta(B_{i,j+1,q}) = 1$ gilt, während für $p \neq A_{i,j}$ $\quad \beta(\neg B_{i,j,p}) = 1$ gilt.
8. Jede Klausel $\{\neg B_{i,j,p}\} \cup \{B_{i+1,j,q} \mid q \in \Pi \text{ und } \mathrm{pr}_3(p) = \mathrm{pr}_1(q)\}$ wird erfüllt, da für $p = A_{i,j}$ und $q = A_{i+1,j}$ $\quad \mathrm{pr}_3(p) = \mathrm{pr}_3(A_{i,j}) = \mathrm{pr}_1(A_{i,j+1}) = \mathrm{pr}_1(q)$ und $\beta(B_{i+1,j,q}) = 1$ gilt, während für $p \neq A_{i,j}$ $\quad \beta(\neg B_{i,j,p}) = 1$ gilt.

Sei umgekehrt β eine Belegung, die $\mathcal{K}$ erfüllt. Wegen der Klauselmengen 1 und 2 gibt es für jedes (i,j) $(1 \leq i \leq m, 1 \leq j \leq n)$ genau ein $p \in \Pi$ mit $\beta(B_{i,j,p}) = 1$. Dann definieren wir eine Belegung $A_{i,j}$ $(1 \leq i \leq m, 1 \leq j \leq n)$ des Dominoproblems (Π, R) durch $A_{i,j} = p$ genau dann, wenn $\beta(B_{i,j,p}) = 1$. Es bleibt zu zeigen, dass die so definierte Belegung korrekt ist.

1. Da für $1 \leq j \leq n$ die Klausel $\{B_{1,j,p} \mid p \in \Pi \text{ und } \mathrm{pr}_1(p) = o_j\}$ erfüllt wird, gilt $\beta(B_{1,j,p}) = 1$ für ein p mit $\mathrm{pr}_1(p) = o_j$, und wegen der Definition von $A_{i,j}$ folgt $\mathrm{pr}_1(A_{1,j}) = o_j$.
2. Da für $1 \leq j \leq n$ die Klausel $\{B_{m,j,p} \mid p \in \Pi \text{ und } \mathrm{pr}_3(p) = u_j\}$ erfüllt wird, gilt $\beta(B_{m,j,p}) = 1$ für ein p mit $\mathrm{pr}_3(p) = u_j$, und wegen der Definition von $A_{i,j}$ folgt $\mathrm{pr}_3(A_{m,j}) = u_j$.
3. Da für $1 \leq i \leq m$ die Klausel $\{B_{i,1,p} \mid p \in \Pi \text{ und } \mathrm{pr}_2(p) = l_i\}$ erfüllt wird, gilt $\beta(B_{i,1,p}) = 1$ für ein p mit $\mathrm{pr}_2(p) = l_i$, und wegen der Definition von $A_{i,j}$ folgt $\mathrm{pr}_2(A_{i,1}) = l_i$.
4. Da für $1 \leq i \leq m$ die Klausel $\{B_{i,n,p} \mid p \in \Pi \text{ und } \mathrm{pr}_4(p) = r_i\}$ erfüllt wird, gilt $\beta(B_{i,n,p}) = 1$ für ein p mit $\mathrm{pr}_4(p) = r_i$, und wegen der Definition von $A_{i,j}$ folgt $\mathrm{pr}_4(A_{i,n}) = r_i$.
5. Für $1 \leq i < m$ und $1 \leq j \leq n$ sei $p = A_{i,j}$. Da die Klausel $\{\neg B_{i,j,p}\} \cup \{B_{i+1,j,q} \mid q \in \Pi \text{ und } \mathrm{pr}_3(p) = \mathrm{pr}_1(q)\}$ erfüllt wird und $\beta(B_{i,j,p}) = 1$ gilt, muss $\beta(B_{i+1,j,q}) = 1$ und damit $A_{i+1,j} = q$ für ein q mit $\mathrm{pr}_1(q) = \mathrm{pr}_3(p)$ gelten. Damit ist die Bedingung $\mathrm{pr}_3(A_{i,j}) = \mathrm{pr}_1(A_{i+1,j})$ für alle $1 \leq i < m, 1 \leq j \leq n$ erfüllt.
6. Für $1 \leq i \leq m$ und $1 \leq j < n$ sei $p = A_{i,j}$. Da die Klausel $\{\neg B_{i,j,p}\} \cup \{B_{i,j+1,q} \mid q \in \Pi \text{ und } \mathrm{pr}_4(p) = \mathrm{pr}_2(q)\}$ erfüllt wird und $\beta(B_{i,j,p}) = 1$ gilt, muss $\beta(B_{i,j+1,q}) = 1$ und damit $A_{i,j+1} = q$ für ein q mit $\mathrm{pr}_2(q) = \mathrm{pr}_4(p)$ gelten. Damit ist die Bedingung $\mathrm{pr}_4(A_{i,j}) = \mathrm{pr}_2(A_{i,j+1})$ für alle $1 \leq i \leq m, 1 \leq j < n$ erfüllt.

Damit ist der Beweis erbracht, dass die Konstruktion von $\mathcal{K}$ eine Reduktion darstellt. Um zu zeigen, dass es sich um eine Polynomialzeit-Reduktion handelt, schätzen wir die Gesamtzahl der in $\mathcal{K}$ auftretenden Literale ab. Von der Form 1 gibt es mn Klauseln mit je einem Literal, von der Form 2 mn Klauseln mit je zwei Literalen, von der Form 3 bzw. 4 je n Klauseln mit höchstens je $|\Pi|$ Literalen, von der Form 5 bzw. 6 je m Klauseln mit höchstens je $|\Pi|$ Literalen, von der Form

7 $(m-1)n$ Klauseln mit höchstens je $|\Pi|+1$ Literalen, von der Form 8 $m(n-1)$ Klauseln mit höchstens je $|\Pi|+1$ Literalen. Die Gesamtzahl der Literale beträgt also $O(mn|\Pi|)$. Jede Klausel kann in linearer Zeit bezüglich ihrer Länge konstruiert werden. Damit erfolgt die Konstruktion von $\mathcal{K}$ in Polynomialzeit. $\square$

Das Problem 3SAT

Erfüllbarkeit mit höchstens 3 Literalen je Klausel (**3SAT**)	
Eingabe:	endliche Klauselmenge $\mathcal{K}$, wobei jede Klausel aus $\mathcal{K}$ höchstens 3 Literale enthält.
Frage:	Ist $\mathcal{K}$ erfüllbar?

Satz 2 **SAT** $\leq_p$ **3SAT**.

Beweis. Zum Beweis der Reduzierbarkeit werden wir für eine Eingabe $\mathcal{K}$ von **SAT** eine Eingabe $\mathcal{K}'$ von **3SAT** derart konstruieren, dass $\mathcal{K}'$ genau dann erfüllbar ist, wenn $\mathcal{K}$ erfüllbar ist.
Zunächst sei $A = \{\ell_1, \ell_2, \ldots, \ell_k\}$ eine einzelne Klausel. Wir konstruieren eine Klauselmenge $\mathcal{K}'(A)$ mit höchstens 3 Variablen je Klausel wie folgt. Ist $k \leq 3$, so ist $\mathcal{K}'(A) = \{A\}$. Anderenfalls seien $y_{A,1}, y_{A,2}, \ldots, y_{A,k-1}$ neue Variablen, die nicht in A vorkommen. Dann ist $\mathcal{K}'(A) = \{A'_1, A'_2, \ldots, A'_k\}$ mit
$A'_1 = \{\ell_1, \neg y_{A,1}\}$,
$A'_i = \{y_{A,i-1}, \ell_i, \neg y_{A,i}\}$ für $2 \leq i \leq k-1$,
$A'_k = \{y_{A,k-1}, \ell_k\}$.

Wir zeigen, dass A genau dann von einer Belegung β erfüllt wird, wenn es eine Erweiterung von β auf die Variablen von $\mathcal{K}'(A)$ gibt, die $\mathcal{K}'(A)$ erfüllt.
Sei zunächst β eine Belegung der Variablen von A, die A erfüllt. Dann gibt es ein minimales i mit $w_\beta(\ell_i) = 1$. Wir erweitern β wie folgt zu einer Belegung β' der Variablen von $\mathcal{K}'(A)$: $\beta'(y_{A,j}) = 0$ genau dann, wenn $j < i$. Dann werden die Klauseln A_j mit $1 \leq j < i$ erfüllt, da sie das Literal $\neg y_{A,j}$ enthalten; die Klausel A_i wird erfüllt, da sie das Literal ℓ_i enthält; und die Klauseln A_j mit $i < j \leq k$ werden erfüllt, da sie das Literal $y_{A,j-1}$ enthalten.
Umgekehrt sei β' eine Belegung der Variablen von $\mathcal{K}'(A)$, die $\mathcal{K}'(A)$ erfüllt und β die Einschränkung von β' auf die Variablen von A. Gilt $\beta'(y_{A,1}) = 1$, so folgt $w_\beta(\ell_1) = w_{\beta'}(\ell_1) = 1$ und damit ist A durch β erfüllt. Gilt $\beta'(y_{A,k-1}) = 0$, so folgt $w_\beta(\ell_k) = w_{\beta'}(\ell_k) = 1$ und damit ist A durch β erfüllt. Anderenfalls gibt es ein i mit $\beta'(y_{A,i-1}) = 0$ und $\beta'(y_{A,i}) = 1$. Dann folgt $w_\beta(\ell_i) = w_{\beta'}(\ell_i) = 1$ und damit ist A durch β erfüllt.

Für eine Klauselmenge $\mathcal{K}$ konstruieren wir $\mathcal{K}' = \bigcup_{A \in \mathcal{K}} \mathcal{K}'(A)$, wobei die zusätzlichen Variablen bei der Konstruktion der Klauseln $\mathcal{K}'(A)$ paarweise verschieden sind. Offensichtlich ist $\mathcal{K}'$ eine Eingabe von **3SAT**, und eine Belegung β der Variablen von $\mathcal{K}$ erfüllt $\mathcal{K}$ genau dann, wenn eine Erweiterung β' von β auf die Variablen von $\mathcal{K}'$ existiert, die $\mathcal{K}'$ erfüllt. Das heißt, $\mathcal{K}$ ist genau dann erfüllbar, wenn $\mathcal{K}'$ erfüllbar ist.

Da die Klauselmenge $\mathcal{K}'$ in linearer Zeit bezüglich der Länge von $\mathcal{K}$ konstruiert werden kann, ist **SAT** $\leq_p$ **3SAT** bewiesen. $\square$

3SAT ist von besonderem Interesse in der Komplexitätstheorie, da man die $\mathbb{NP}$-Vollständigkeit zahlreicher Probleme durch Reduktion von **3SAT** zeigen kann.

Das Clique-Problem

Cliquen-Problem (**Clique**)	
Eingabe:	ungerichteter Graph G, $k \in \mathbb{N}$
Frage:	Enthält G einen vollständigen Teilgraphen mit k Knoten?

Satz 3 **SAT** $\leq_p$ **Clique**.

Beweis. Es sei $\mathcal{K} = \{A_1, A_2, \ldots, A_k\}$ ein Klauselmenge. Für ein Literal ℓ sei $\overline{\ell}$ das zu ℓ komplementäre Literal; d.h. $\overline{x} = \neg x$ und $\overline{\neg x} = x$ für eine Variable x.

Wir konstruieren aus $\mathcal{K}$ einen ungerichteten Graphen G wie folgt. Gibt es in der Klausel A_i das Literal ℓ, so enthält G den Knoten (ℓ, i). Eine Kante zwischen zwei Knoten (ℓ, i) und (ℓ', j) existiert genau dann, wenn $\overline{\ell} \neq \ell'$ und $i \neq j$ gilt.

Eine Clique in G kann höchstens die Größe k haben, da für je zwei Knoten (ℓ, i), (ℓ', j) der Clique $i \neq j$ gelten muss. Ist $\mathcal{K}$ erfüllbar, so gibt es eine Belegung β und für alle $1 \leq i \leq k$ ein Literal ℓ_i aus A_i derart, dass $w_\beta(\ell_i) = 1$ gilt. Nach Definition von w_β muss $\overline{\ell_i} \neq \ell_j$ für alle $i \neq j$ gelten. Nach der Konstruktion von G bildet die Knotenmenge $\{(\ell_i, i) \mid 1 \leq i \leq k\}$ eine Clique in G.

Gibt es umgekehrt in G eine Clique der Größe k, so hat sie die Form $\{(\ell_i, i) \mid 1 \leq i \leq k\}$ mit $\overline{\ell_i} \neq \ell_j$ für alle $i \neq j$. Man kann dann eine Belegung β derart konstruieren, dass $w_\beta(\ell_i) = 1$ für alle $1 \leq i \leq k$ gilt. Damit erfüllt β die Klauselmenge $\mathcal{K}$.

Da die Anzahl der Knoten von G gleich der Anzahl der Literale in $\mathcal{K}$ ist, kann G aus $\mathcal{K}$ in Polynomialzeit konstruiert werden, d.h. **SAT** $\leq_p$ **Clique**. $\square$

Die Probleme SubsetSum und Knapsack

Das Problem der Teilmengensumme (**SubsetSum**)

Eingabe:	endliche Menge $U \subseteq \mathbb{N}$, $b \in \mathbb{N}$
Frage:	Existiert eine Teilmenge $A \subseteq U$ mit $\sum\limits_{a \in A} a = b$?

Satz 4 **3SAT** $\leq_p$ **SubsetSum**.

Beweis. Es sei $\mathcal{K} = \{K_1, K_2, \ldots, K_k\}$ eine Menge von k Klauseln mit höchstens 3 Literalen je Klausel. Die in $\mathcal{K}$ vorkommenden Variablen seien $x_1, x_2, \ldots, x_m$, die Anzahl der Klauseln von $\mathcal{K}$ sei k.

Aus $\mathcal{K}$ konstruieren wir eine Eingabe (U, b) für **SubsetSum** wie folgt. Die auftretenden Zahlen sind alle kleiner als 10^{k+m}. Zur besseren Übersicht werden sie alle durch $k+m$ Dezimalstellen mit führenden Nullen dargestellt. Die (von links) i-te Dezimalstelle einer Zahl steht für die Klausel K_i, die $(k+i)$-te Dezimalstelle steht für die Variable x_i.

Die Zahl b besteht in ihrer Dezimaldarstellung k-mal aus der Ziffer 4, gefolgt von m-mal der Ziffer 1, formal:

$$b = 4 \cdot \sum_{i=1}^{k} 10^{k+m-i} + \sum_{j=1}^{m} 10^{m-j}.$$

Für $k = 6$ und $m = 10$ erhält man also z.B. $b = 4444441111111111$.

Für jede Variable x_j, $1 \leq j \leq m$, enthält U zwei Zahlen a_j und $\overline{a_j}$. In beiden Zahlen ist die $(k+j)$-te Dezimalstelle 1. Für $1 \leq i \leq k$ ist die i-te Dezimalstelle in a_j (bzw. in a_j) genau dann gleich 1, wenn $x_j \in K_i$ (bzw. $\neg x_j \in K_i$) gilt. Alle anderen Dezimalstellen sind Null, formal:

$$a_j = \sum_{i : x_j \in K_i} 10^{k+m-i} + 10^{m-j}, \qquad \overline{a_j} = \sum_{i : \neg x_j \in K_i} 10^{k+m-i} + 10^{m-j}.$$

Kommen z.B. für $k = 6$ und $m = 10$ das Literal x_2 in den Klauseln K_1, K_4, K_5 und das Literal $\neg x_2$ in den Klauseln K_3, K_6 vor, so erhält man die Zahlen $a_2 = 1001100100000000$ und $\overline{a_2} = 0010010100000000$.

Wir setzen $U' := \{a_j \mid 1 \leq j \leq m\} \cup \{\overline{a_j} \mid 1 \leq j \leq m\}$. Offensichtlich gibt es in U' für jedes $j \in \{1, 2, \ldots, m\}$ genau 2 Zahlen, deren $(k+j)$-te Dezimalstelle gleich 1 ist, nämlich a_j und $\overline{a_j}$. Weiterhin enthält U' für jedes $i \in \{1, 2, \ldots, k\}$ höchstens 3 Zahlen, deren i-te Dezimalstelle gleich 1 ist, weil K_i höchstens 3 Literale enthält.

Die Menge U entsteht, indem man zu U' noch die Zahlen c_i und d_i mit $1 \leq i \leq k$ hinzufügt, wobei bei c_i (bzw. bei d_i) die i-te Dezimalstelle 1 (bzw. 2) ist und alle anderen Dezimalstellen Null sind, formal:

$$c_i = 10^{k+m-i}, \qquad d_i = 2 \cdot 10^{k+m-i}.$$

Sei nun $\beta : \{x_1, x_2, \ldots, x_m\} \to \{0,1\}$ eine erfüllende Belegung für $\mathcal{K}$. Dann wählen wir aus U' die Teilmenge $U'_\beta = \{a_j \mid \beta(x_j) = 1\} \cup \{\overline{a_j} \mid \beta(x_j) = 0\}$. Mit b_β bezeichnen wir die Summe der Zahlen in U'_β. Da U'_β für jedes $j \in \{1, 2, \ldots, m\}$ genau eine der Zahlen $a_j, \overline{a_j}$ enthält, sind die letzten m Ziffern von b_β jeweils 1. Da β eine erfüllende Belegung für $\mathcal{K}$ ist, gibt es für jedes $i \in \{1, 2, \ldots, k\}$ ein $j \in \{1, 2, \ldots, m\}$ mit $\beta(x_j) = 1$ und $x_j \in K_i$ oder $\beta(x_j) = 0$ und $\neg x_j \in K_i$. Im ersten Fall ist die i-te Dezimalstelle von a_i gleich 1 und $a_i \in U'_\beta$; im zweiten Fall ist die i-te Dezimalstelle von $\overline{a_i}$ gleich 1 und $\overline{a_i} \in U'_\beta$. In jedem Fall enthält U_β für jedes $i \in \{1, 2, \ldots, k\}$ mindestens eine Zahl, deren i-te Dezimalstelle gleich 1 ist. Damit ist die i-te Dezimalstelle von b_β eine Zahl aus der Menge $\{1, 2, 3\}$.

Die Menge U'_β wird schließlich zu einer Menge $U_\beta \subseteq U$ wie folgt erweitert: Ist die i-te Dezimalstelle ($1 \leq i \leq k$) von b_β gleich 3, so wird c_i hinzugefügt; ist sie 2, so wird d_i hinzugefügt; ist sie 1, so werden c_i und d_i hinzugefügt. Offensichtlich ist die Summe der Zahlen aus U_β gleich b.

Umgekehrt sei $A \subseteq U$ eine Menge mit $\sum\limits_{a \in A} a = b$. Da die letzten m Dezimalstellen von b jeweils 1 sind, enthält A für alle $j \in \{1, 2, \ldots, m\}$ genau eine der Zahlen $a_j, \overline{a_j}$. Wir wählen für die Variablen in $\mathcal{K}$ die Belegung β_A mit $\beta_A(x_j) = 1$ genau dann, wenn $a_j \in A$. Weiterhin seien $A' = A \cap U'$ und b' die Summe aller Zahlen aus A'. Da die ersten k Dezimalstellen von b jeweils gleich 4 sind, ist jede der ersten k Dezimalstellen von b' eine Zahl größer gleich 1. Also gibt es für jedes $1 \leq i \leq k$ in A' eine Zahl $z(i)$, deren i-te Dezimalstelle gleich 1 ist. Gilt $z(i) = a_j$ für ein $j \in \{1, 2, \ldots, m\}$, so sind $\beta_A(x_j) = 1$ und $x_j \in K_i$. Gilt $z(i) = \overline{a_j}$ für ein $j \in \{1, 2, \ldots, m\}$, so sind $\beta_A(x_j) = 0$ und $\neg x_j \in K_i$. In beiden Fällen wird K_i durch β_A erfüllt. Damit ist β_A eine erfüllende Belegung von $\mathcal{K}$. Die Konstruktion von (U, b) aus $\mathcal{K}$ stellt also tatsächlich eine Reduktion von **3SAT** auf **SubsetSum** dar. Der Zeitaufwand beträgt $O(m+k)$ für die Bestimmung von b und $O(m(m+k))$ für die Bestimmung von U, ist also polynomial. □

Das Rucksackproblem (**Knapsack**) ist eng mit dem Problem der Teilmengensumme verwandt. Gegeben sind eine endliche Menge von Gegenständen U und ein Rucksack mit einer Tragfähigkeit von b. Jeder Gegenstand $u \in U$ hat einen Wert $v(u)$ und ein Gewicht $w(u)$. Gesucht ist eine Teilmenge von U mit maximalem Wert und einem Gesamtgewicht von höchstens b. In der Entscheidungsvariante gibt es eine Konstante c und es wird gefragt, ob eine Teilmenge mit einem Wert von mindestens c und einem Gewicht von höchstens b existiert.

Rucksackproblem (**Knapsack**)

Eingabe: endliche Menge U, Abbildungen $v : U \to \mathbb{N}, w : U \to \mathbb{N}$, $b, c \in \mathbb{N}$

Frage: Existiert eine Teilmenge $A \subseteq U$ mit $\sum\limits_{a \in A} w(a) \leq b$ und $\sum\limits_{a \in A} v(a) \geq c$?

Satz 5 **SubsetSum** $\leq_p$ **Knapsack**.

Beweis. Übungsaufgabe. □