Das Erfüllbarkeitsproblem der Aussagenlogik (SAT)

Problemstellung

Hier sollen nur 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 aussagenlogischer Ausdruck ist ein Wort über einem Alphabet *var* von aussagenlogischen Variablen sowie den Zeichen $(,), \neg, \wedge, \vee$.

- Ein *Literal* ist ein Wort der Form x bzw. $\neg x$, wobei x eine Variable ist.
- Eine *Alternative* ist ein Wort der Form $(\ell_1 \vee \ell_2 \vee \ldots \vee \ell_k)$, wobei $\ell_1, \ell_2, \ldots, \ell_k$ Literale sind.
- Ein *aussagenlogischer Ausdruck in konjunktiver Normalform* (kurz: Ausdruck in KNF) ist ein Wort der Form $A_1 \wedge A_2 \wedge \ldots \wedge A_m$, wobei $A_1, A_2, \ldots, A_m$ Alternativen sind.

Eine *Belegung* ist eine Abbildung $\beta : var \to \{0, 1\}$. Durch eine Belegung β wird für einen Ausdruck in KNF E wie folgt ein Wert $w_\beta(E) \in \{0, 1\}$ definiert.

- Für eine Variable x gilt $w_\beta(x) = \beta(x)$.
- Für ein Literal $\neg x$ ist $w_\beta(\neg x)$ genau dann 1 wenn $w_\beta(x) = 0$ gilt.
- Für eine Alternative $A = (\ell_1 \vee \ell_2 \vee \ldots \vee \ell_k)$ ist $w_\beta(A)$ genau dann 1, wenn $w_\beta(\ell_i) = 1$ für mindestens ein $i \in \{1, 2, \ldots, k\}$ gilt.
- Für einen Ausdruck in KNF $E = A_1 \wedge A_2 \wedge \ldots \wedge A_m$ ist $w_\beta(E)$ genau dann 1, wenn $w_\beta(A_j) = 1$ für alle $j \in \{1, 2, \ldots, m\}$ gilt.

Ein Ausdruck in KNF E heißt *erfüllbar*, wenn es eine Belegung β gibt, für die $w_\beta(E) = 1$ gilt.

Erfüllbarkeitsproblem **SAT**	
Eingabe:	Aussagenlogischer Ausdruck E in konjunktiver Normalform
Frage:	Ist E erfüllbar?

NP-Vollständigkeit von SAT

Offensichtlich liegt **SAT** in $\mathbb{NP}$. Ist der Ausdruck E erfüllbar, so rät man einfach eine erfüllende Belegung der in E vorkommenden Variablen und überprüft, dass diese Belegung tatsächlich E erfüllt. Beides kann in linearer Zeit bezüglich $|E|$ getan werden.

Um zu zeigen, dass **SAT** $\mathbb{NP}$-vollständig ist, beweisen wir **Domino** $\leq$ **SAT**. Wir werden also zu einer Instanz (Π, R) von **Domino** in Polynomialzeit einen Ausdruck E in konjunktiver Normalform konstruieren, so dass E genau dann erfüllbar ist, wenn (Π, R) eine korrekte Auslegung besitzt.

Es sei also Π ein Dominospiel über dem Alphabet Σ und R ein Rahmen mit den Randwörtern $o_1 o_2 \cdots o_n$, $u_1 u_2 \cdots u_n$, $l_1 l_2 \cdots l_m$ und $r_1 r_2 \cdots r_m$ am oberen, unteren, linken bzw. rechten Rand. Weiterhin bezeichnen wir für $a \in \Sigma$ mit $\Pi_{o,a}$, $\Pi_{u,a}$, $\Pi_{l,a}$ bzw. $\Pi_{r,a}$ die Menge aller Dominosteine aus Π, die in ihrem oberen, unteren, linken bzw. rechten Viertel das Symbol a besitzen.

Für jeden Dominostein $p \in \Pi$ sowie alle $1 \leq i \leq m, 1 \leq j \leq n$ führen wir die aussagenlogischen Variablen $B^p_{i,j}$ ein. Eine Belegung von $B^p_{i,j}$ mit dem Wert 1 wird einer Auslegung des Bildpunktes (i, j) mit dem Dominostein p entsprechen. Für jedes Symbol $a \in \Sigma$ sowie alle $1 \leq i \leq m, 1 \leq j \leq n$ führen wir die aussagenlogischen Variablen $O^a_j, U^a_j, L^a_i, R^a_i$ ein. Eine Belegung von O^a_j, U^a_j, L^a_i bzw. R^a_i mit dem Wert 1 wird $o_j = a$, $u_j = a$, $l_i = a$ bzw. $r_i = a$ entsprechen.

Der Ausdruck E entsteht durch Konjunktion der folgenden Alternativen:

- $O_j^{o_j}$, $U_j^{u_j}$, $L_i^{l_i}$, $R_i^{r_i}$ für $1 \leq i \leq m, 1 \leq j \leq n$.
  Damit wird erzwungen, dass die Variablen, die dem Rahmen entsprechen, mit 1 belegt werden.
- $\bigvee_{p \in \Pi} B_{i,j}^p$ für $1 \leq i \leq m, 1 \leq j \leq n$,
  $\neg B_{i,j}^p \vee \neg B_{i,j}^q$ für $p, q \in \Pi, p \neq q$, $1 \leq i \leq m, 1 \leq j \leq n$.
  Damit wird erzwungen, dass für alle (i, j) genau eine der Variablen $B_{i,j}^p$, $p \in \Pi$, mit 1 belegt wird.
- $\neg B_{i,j}^p \vee \bigvee_{q \in \Pi_{l,a}} B_{i,j+1}^q$ für $p \in \Pi_{r,a}$, $1 \leq i \leq m, 1 \leq j \leq n-1$.
  Ist die Variable $B_{i,j}^p$ mit 1 belegt und gilt $p \in \Pi_{r,a}$, so muss für die (einzige) Variable $B_{i,j+1}^q$ mit der Belegung 1 gelten: $q \in \Pi_{l,a}$. Das entspricht der Forderung, dass die Dominosteine an den Stellen (i, j) und $(i, j+1)$ zusammenpassen müssen.
- $\neg B_{i,j}^p \vee \bigvee_{q \in \Pi_{o,a}} B_{i+1,j}^q$ für $p \in \Pi_{r,a}$, $1 \leq i \leq m, 1 \leq j \leq n-1$.
  Das entspricht der Forderung, dass die Dominosteine an den Stellen (i, j) und $(i+1, j)$ zusammenpassen müssen.
- $\neg O_j^a \vee \bigvee_{q \in \Pi_{o,a}} B_{1,j}^q$ für $a \in \Sigma$, $1 \leq j \leq n$.
  Das entspricht der Forderung, dass die Dominosteine der ersten Zeile mit dem oberen Rand zusammenpassen müssen.
- $\neg U_j^a \vee \bigvee_{q \in \Pi_{u,a}} B_{m,j}^q$ für $a \in \Sigma$, $1 \leq j \leq n$.
  Das entspricht der Forderung, dass die Dominosteine der letzten Zeile mit dem unteren Rand zusammenpassen müssen.
- $\neg L_i^a \vee \bigvee_{q \in \Pi_{l,a}} B_{i,1}^q$ für $a \in \Sigma$, $1 \leq i \leq m$.
  Das entspricht der Forderung, dass die Dominosteine der ersten Spalte mit dem linken Rand zusammenpassen müssen.
- $\neg R_i^a \vee \bigvee_{q \in \Pi_{r,a}} B_{i,n}^q$ für $a \in \Sigma$, $1 \leq i \leq m$.
  Das entspricht der Forderung, dass die Dominosteine der letzten Spalte mit dem rechten Rand zusammenpassen müssen.

Wie man leicht sieht, ist die Länge von E polynomial in $m + n + |\Pi|$ und E kann auch in Polynomialzeit konstruiert werden. Durch die Konstruktion wird außerdem garantiert, dass eine korrekte Auslegung des Rahmens genau dann existiert, wenn E erfüllbar ist. Damit ist die polynomiale Reduktion von **Domino** auf **SAT** erbracht.

Das Problem 3SAT

Erfüllbarkeit mit höchstens 3 Literalen je Klausel (**3SAT**)	
Eingabe:	Ausdruck in KNF $E = A_1 \wedge A_2 \wedge \ldots \wedge A_m$, wobei jede Alternative höchstens 3 Literale enthält.
Frage:	Ist E erfüllbar?

3SAT ist offenbar ein Spezialfall von **SAT**, und damit gilt trivialerweise **3SAT** $\leq_p$ **SAT**. Wir werden zeigen, dass auch **SAT** $\leq_p$ **3SAT** gilt und folglich **3SAT** ebenfalls $\mathbb{NP}$-vollständig ist. **3SAT** ist von besonderem Interesse in der Komplexitätstheorie, da man die $\mathbb{NP}$-Vollständigkeit zahlreicher Probleme durch Reduktion von **3SAT** zeigen kann.

Zum Beweis der Reduzierbarkeit werden wir für eine Instanz E von **SAT** eine Instanz E' von **3SAT** derart konstruieren, dass E' genau dann erfüllbar ist, wenn E erfüllbar ist.
Zunächst sei $A = (\ell_1 \vee \ell_2 \vee \ldots \vee \ell_k)$ eine Alternative. Wir konstruieren eine Instanz $E'(A)$ wie

folgt. Ist $k \leq 3$, so ist $E'(A) = A$. Anderenfalls seien $y_{A,1}, y_{A,2}, \ldots, y_{A,k-1}$ neue Variablen, die nicht in A vorkommen. Dann ist $E'(A) = A'_1 \wedge A'_2 \wedge \ldots \wedge A'_k$ mit
$A'_1 = (\ell_1 \vee \neg y_{A,1})$,
$A'_i = (y_{A,i-1} \vee \ell_i \vee y_{A,i})$ für $2 \leq i \leq k-1$,
$A'_k = (y_{A,k-1} \vee \ell_k)$.

Es sei β eine Belegung der Variablen von A mit $w_\beta(A) = 1$. Dann gibt es ein minimales i mit $w_\beta(\ell_i) = 1$. Wir erweitern β wie folgt zu einer Belegung β' der Variablen von $E'(A)$: $\beta'(y_{A,j}) = 0$ genau dann, wenn $j < i$. Wie man leicht nachprüft, gilt $w_{\beta'}(A'_j) = 1$ für $1 \leq j \leq k$ und damit $w_{\beta'}(E'(A)) = 1$.

Umgekehrt sei β' eine Belegung der Variablen von $E'(A)$ mit $w_{\beta'}(E'(A)) = 1$ und β die Einschränkung von β' auf die Variablen von A. Gilt $\beta'(y_{A,j}) = 0$ für $1 \leq j \leq k-1$, so folgt $w_\beta(\ell_k) = w_{\beta'}(\ell_k) = 1$ und damit $w_\beta(A) = 1$. Anderenfalls gibt es ein i mit $\beta'(y_{A,i}) = 1$ und $\beta'(y_{A,i-1}) = 0$ oder $i = 1$. In beiden Fällen folgt $w_\beta(\ell_i) = w_{\beta'}(\ell_i) = 1$ und damit $w_\beta(A) = 1$.

Wir haben also gezeigt: $w_\beta(A) = 1$ genau dann, wenn eine Erweiterung β' von β auf die Variablen von $E'(A)$ existiert, für die $w_{\beta'}(E'(A)) = 1$ gilt.

Für einen Ausdruck in KNF $E = A_1 \wedge A_2 \wedge \ldots \wedge A_m$ konstruieren wir den Ausdruck in KNF $E' = E'(A_1) \wedge E'(A_2) \wedge \ldots \wedge E'(A_m)$, wobei alle neuen Variablen bei der Konstruktion der Ausdrücke $E'(A_i)$, $1 \leq i \leq m$, paarweise verschieden sind. Offensichtlich ist E' eine Instanz von **3SAT**, und es gilt für eine Belegung β der Variablen von E: $w_\beta(E) = 1$ genau dann, wenn eine Erweiterung β' von β auf die Variablen von E' existiert, für die $w_{\beta'}(E') = 1$ gilt. Das heißt, E ist genau dann erfüllbar, wenn E' erfüllbar ist. Da der Ausdruck E' in linearer Zeit bezüglich der Länge von E konstruiert werden kann, ist **SAT** $\leq_p$ **3SAT** bewiesen.

NP-Vollständigkeit des Clique-Problems

Cliquen-Problem (**Clique**)

Eingabe:	ungerichteter Graph G, $k \in \mathbb{N}$
Frage:	Enthält G einen vollständigen Teilgraphen mit k Knoten?

Die $\mathbb{NP}$-Vollständigkeit von **Clique** wird durch Reduktion von **SAT** gezeigt. Sei also $E = A_1 \wedge A_2 \wedge \ldots \wedge A_k$ ein Ausdruck in KNF mit den Alternativen $A_1, A_2, \ldots, A_k$. 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 E einen ungerichteten Graphen G wie folgt. Gibt es in der Alternativen 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 E 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. Damit 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. Das heißt: $E \in$ **SAT** genau dann, wenn $(G, k) \in$ **Clique**. Da die Anzahl der Knoten von G linear in $|E|$ ist, kann G aus E in Polynomialzeit konstruiert werden, d.h. **SAT** $\leq_p$ **Clique**.