ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Prof. Dr. Peter Thiemann
Manuel Geffken

05.02.2016
Abgabe bis spätestens Freitag 12.02.2016, 10 Uhr
in die Briefkästen in Gebäude 51

12. Übungsblatt zur Vorlesung

Theoretische Informatik

Mit Lösungsskizze für Tutoren

Dieses Blatt ist das letzte Übungsblatt und ist für die Zulassung relevant. Es findet kein Tutorat statt, in dem die Lösung für dieses Blatt besprochen wird. Daher wird für dieses Blatt nach dem 12. Februar eine Musterlösung auf der Webseite veröffentlicht. Ihre Korrektur können Sie sich ab dem 19. Februar am Lehrstuhl für Programmiersprachen (Gebäude 079, Obergeschoss) abholen. Alternativ können Sie mit Ihrem Tutor eine Abgabe per Email vereinbaren.

Hinweis: Wo Sie in den folgenden Aufgaben die Berechenbarkeit von Funktionen zeigen oder eine Laufzeitabschätzung angeben müssen, genügt jeweils eine intuitive Begründung. Sie müssen weder Turingmaschinen noch Pseudocode explizit angeben.

Aufgabe 1: Reduktion I — 3 Punkte

Welche der folgenden Aussagen gelten? Beweisen Sie Ihre Behauptungen.

(a) $\textsc{Sat} \preceq \mathrm{H}$

(b) $\mathrm{H} \preceq \textsc{Sat}$

(c) $\textsc{Sat} \preceq_p \mathrm{H}$

(d) $\mathrm{H} \preceq_p \textsc{Sat}$

Dabei ist H das allgemeine Halteproblem für Turingmaschinen und Sat das Erfüllbarkeitsproblem für boolesche Ausdrücke in konjunktiver Normalform.

.... Lösungsskizze ....

a), c) Es gilt $SAT \preceq_p H$, also auch $SAT \preceq H$.

Da SAT entscheidbar ist, existiert eine Turingmaschine M, die SAT entscheidet. Konstruiere eine Turingmaschine M', die zunächst M ausführt und hält, falls M die Eingabe akzeptiert, andernfalls in eine Endlosschleife übergeht.

Definiere $f(w) := \ulcorner M' \urcorner w$. f ist offensichtlich in Zeit $O(|w|)$, also mit polynomiellem Aufwand, berechenbar.

Nun gilt:

$$\begin{aligned} & w \in SAT \\ \iff & M \text{ akzeptiert } w \\ \iff & M' \text{ hält auf } w \\ \iff & f(w) = \ulcorner M \urcorner w \in H \end{aligned}$$

b), d) Es gilt nicht $H \preceq SAT$, also auch nicht $H \preceq_p SAT$.

Da SAT entscheidbar ist, würde aus $H \preceq SAT$ folgen, dass H entscheidbar ist. Dem ist bekanntermaßen nicht so.

Aufgabe 2: Reduktion II

3 Punkte

Das NP-vollständige Hamiltonpfadproblem HPATH lautet wie folgt:

Gegeben: ein ungerichteter Graph G.
Frage: Gibt es einen Pfad in G, der jeden Knoten genau einmal besucht?

Das Hamiltonpfadproblem für gerichtete Graphen DHPATH ist analog definiert, aber zusätzlich darf jede Kante nur in Richtung von ihrem Ausgangs- zu ihrem Zielknoten verwendet werden.
Zeigen Sie: HPATH $\preceq_p$ DHPATH.

.... Lösungsskizze ....

Sei $G := (V, E)$ ein ungerichteter Graph. Definiere die Reduktionsfunktion f durch $f(G) := (V, E')$ mit

$$E' := \{(u, v), (v, u) \mid \{u, v\} \in E\}.$$

$G' := (V, E')$ ist damit ein gerichteter Graph.
f ist in polynomieller Zeit berechenbar, da nur die Kanten von G durchlaufen werden müssen ($O(|E|)$), wobei für jede Kante zwei in E' eingefügt werden.
Zu zeigen bleibt: Es existiert ein Hamiltonpfad in G gdw. ein gerichteter Hamiltonpfad in G' existiert.

- „$\Rightarrow$":

  Seien

  $$\begin{aligned} p &:= (v_1, \{v_1, v_2\}, v_2, \ldots, \{v_{n-1}, v_n\}, v_n) \\ p' &:= (v_1, (v_1, v_2), v_2, \ldots, (v_{n-1}, v_n), v_n) \end{aligned}$$

  Angenommen, p ist ein Hamiltonpfad in G. p' ist ein Pfad in G', da nach Konstruktion jede Kante (v_i, v_j) in E' ist, sofern auch $\{v_i, v_j\}$ in E ist. p und p' besuchen die gleichen Knoten, und da G und G' die gleiche Knotenmenge V haben, ist p' ein Hamiltonpfad in G'.

- „$\Leftarrow$":

  Seien

  $$\begin{aligned} p' &:= (v_1, (v_1, v_2), v_2, \ldots, (v_{n-1}, v_n), v_n) \\ p &:= (v_1, \{v_1, v_2\}, v_2, \ldots, \{v_{n-1}, v_n\}, v_n) \end{aligned}$$

  Angenommen, p' ist ein Hamiltonpfad in G'. p ist ein Pfad in G, denn eine Kante (v_i, v_j) kann nach Konstruktion nur dann in E' sein, wenn auch $\{v_i, v_j\}$ in E ist. p besucht auch jeden Knoten; Begründung wie oben.

Aufgabe 3: NP-Vollständigkeit I

6 Punkte

Das NP-vollständige Problem 3Sat, eine Variante des Sat-Problems, ist wie folgt definiert:

Gegeben: eine aussagenlogische Formel F in konjunktiver Normalform, bei der jede Klausel höchstens drei Literale enthält.
Frage: Ist F erfüllbar?

Das Problem MSat ist wie folgt definiert:

Gegeben: eine aussagenlogische Formel F in konjunktiver Normalform.
Frage: Existiert eine Belegung der Variablen von F, sodass in jeder Klausel strikt mehr als die Hälfte der Literale wahr wird?

Zeigen Sie: MSat ist NP-vollständig.

.... Lösungsskizze ....

MSat ist in NP

Rate eine Belegung und prüfe für jede Klausel, ob die Mehrzahl der Literale bei dieser Belegung wahr wird. Bei geeigneter Repräsentation der Belegung, zum Beispiel als Array, benötigt dies Zeit $O(n)$.

MSat ist NP-hart

Wir zeigen: $3\text{Sat} \preceq_p \text{MSat}$.
Sei $F := C_1 \wedge \cdots \wedge C_n$ eine Formel in konjunktiver Normalform, bei der jede Klausel C_i höchstens drei Literale enthält. Definiere f durch

$$\begin{aligned} f(C_1 \wedge \cdots \wedge C_n) &:= g(C_1, 1) \wedge \cdots \wedge g(C_n, n) \\ g((l_1), i) &:= l_1 \vee a_{i,1} \\ g((l_1 \vee l_2), i) &:= l_1 \vee l_2 \vee a_{i,1} \\ g((l_1 \vee l_2 \vee l_3), i) &:= l_1 \vee l_2 \vee l_3 \vee a_{i,1} \vee a_{i,2} \end{aligned}$$

Dabei sind die $a_{i,j}$ Variablen, die von allen Variablen in F und einander verschieden sind.
$f(F)$ ist offensichtlich eine aussagenlogische Formel in konjunktiver Normalform, also eine Instanz von MSat. f ist polynomiell berechenbar, indem auf jede Klausel g angewandt wird ($O(n)$), wobei g in konstanter Zeit ($O(1)$) berechenbar ist.
Zu zeigen bleibt: $F \in 3\text{Sat} \iff f(F) \in \text{MSat}$.

- „$\Rightarrow$":
  Sei ϕ eine erfüllende Belegung von F und sei V die Menge der Variablen von F. Wähle die Belegung
  $$\phi'(v) := \begin{cases} \phi(v) & \mid v \in V \\ \text{True} & \mid \text{sonst} \end{cases}$$
  Unter ϕ' sind alle neuen Variablen $a_{i,j}$ wahr. Außerdem ist in jeder Klausel von F mindestens ein Literal wahr unter ϕ, denn sonst wäre ϕ keine erfüllende Belegung von F. Damit ist nach Konstruktion in jedem Literal von $f(F)$ die Mehrzahl der Literale wahr.

- „$\Leftarrow$“:

  Sei $F \notin 3\textsc{Sat}$, d.h. F unerfüllbar, d.h. für jede Belegung ϕ existiert eine Klausel C von F, deren Literale unter F alle falsch sind. Nach Konstruktion kann dann aber auch nicht die Mehrzahl der Literale in $g(C)$ wahr werden. Somit erfüllt $f(F)$ nicht die Bedingungen von $\textsc{MSat}$.

Aufgabe 4: NP-Vollständigkeit II 4 Bonuspunkte

Das Problem $\textsc{HSet}$ (Hitting-Set) ist wie folgt definiert:

> *Gegeben:* eine Menge M und eine endl. Menge von Teilmengen $\mathcal{S}$ (d.h. $\mathcal{S} := \{S_1, \ldots, S_n\}$; $\forall i \in \{1, \ldots, n\}.\ S_i \subseteq M$) sowie eine natürliche Zahl $k \leq n$.
>
> *Frage:* Gibt es eine Teilmenge $T \subseteq M$ mit $|T| \leq k$ und $\forall i \in \{1, \ldots, n\}.\ T \cap S_i \neq \emptyset$?

Das NP-vollständige Problem VC (Knotenüberdeckung; auch Vertex Cover) ist wie folgt definiert:

> *Gegeben:* ein ungerichteter Graph $G := (V, E)$ und eine natürliche Zahl $k \leq |E|$.
>
> *Frage:* Besitzt G eine überdeckende Knotenmenge der Größe höchstens k? Eine überdeckende Knotenmenge ist eine Teilmenge $V' \subseteq V$, sodass für alle Kanten $(u, v) \in E$ gilt: $u \in V'$ oder $v \in V'$.

(a) Begründen Sie, dass $\textsc{HSet}$ in NP liegt.

(b) Beweisen Sie, dass $\textsc{HSet}$ NP-schwer ist.

.... Lösungsskizze ....

(a) Rate eine Teilmenge $T \subseteq M$ mit $|T| = k$ sowie je ein Element $s_i \in S_i$ für jedes $S_i \in \mathcal{S}$. Diese potentielle Lösung kann überprüft werden, indem für alle $j \in \{1, \cdots, n\}$ getestet wird, ob $s_j \in T$ ist. Das ist mit Zeitaufwand $O(k \cdot n) = O(n)$ (mit k konstant) möglich.

(b) Instanzen von $\textsc{HSet}$ sind Tupel $(M, \mathcal{S}, k)$; Instanzen von VC sind Tupel (V, E, k). Wir zeigen $\text{VC} \preceq_p \textsc{HSet}$ (somit $\textsc{HSet}$ NP-schwer) mittels f wie folgt:

$$f(V, E, k) := (M := V, \mathcal{S} := \{\{v, u\} \mid (v, u) \in E\}, k := k)$$

$f(V, E, k)$ ist eine Instanz von $\textsc{HSet}$, denn $M = V$ ist eine endliche Menge; $\mathcal{S}$ eine endliche Menge von Teilmengen von V; $k \leq |E|$.

f ist offensichtlich in Zeit $O(1)$ berechenbar. (Wir sehen hier von Fragen der Kodierung von Graphen, Tupeln, Mengen etc. ab. Je nach Art der verwendeten Kodierung, z.B. bei bestimmten Binärkodierungen, kann der Aufwand zur Berechnung von f nichtkonstant sein, aber es existieren jedenfalls Kodierungen, die die Umwandlung in polynomieller Zeit ermöglichen.)

Nun ist $(V, E, k) \in \text{VC} \iff f(V, E, k) \in \textsc{HSet}$, denn:

- Sei $(V, E, k) \in \mathrm{VC}$. Dann existiert ein $V' \subseteq V$ mit $|V'| \leq k$ sodass für jedes $(u, v) \in E$ $u \in V'$ oder $v \in V'$. Wähle $T := V'$. Es ist $T \subseteq M = V$ und für jede Teilmenge $\{u, v\} \in \mathcal{S}$ ist $T \cap \{u, v\} \neq \emptyset$, denn sonst gälte für die entsprechende Kante (u, v): $u \notin V'$ und $v \notin V'$. Damit auch $f(V, E, k) \in \mathrm{HS{\small ET}}$.
- Sei $(M, \mathcal{S}, k) := f(V, E, k) \in \mathrm{HS{\small ET}}$. Dann existiert ein $T \subseteq M$ mit $|T| \leq k$ sodass $T \cap \{u, v\} \neq \emptyset$ für alle $\{u, v\} \in \mathcal{S}$. Wähle $V' := T$. Dann ist $|V'| \leq k$ und für jedes $(u, v) \in E$ ist $u \in V'$ oder $v \in V'$, denn sonst wäre $V' \cap \{u, v\} = \emptyset$. Damit auch $(V, E, k) \in \mathrm{VC}$.