Lehrstuhl für Informatik 1
Prof. Dr. Berthold Vöcking
Alexander Skopalik
Matthias Englert

WS 2007/08
14.1.2008

Übung zur Vorlesung
Berechenbarkeit und Komplexität
Lösung Blatt 9

Aufgabe 9.1: **(5+5+4 Punkte)**

(a) Sei $(G = (V, E), k)$ eine Eingabe von Clique, für die entschieden werden soll, ob G eine Clique C mit $|C| \geq k$ enthält. Aus (G, k) erzeugen wir in polynomieller Zeit eine Eingabe $(\bar{G}, \bar{k})$ für IndependentSet, so dass (G, k) genau dann eine Clique C mit $|C| \geq k$ enthält, wenn $(\bar{G}, \bar{k})$ ein Independent Set I mit $|I| \geq \bar{k}$ enthält.

Die Eingabe $(\bar{G}, \bar{k})$ konstruieren wir wie folgt. Sei

$$\bar{G} = (V, \{\{u, v\} \mid u \neq v, u, v \in V, \{u, v\} \notin E\})$$

der invertiere Graph G, der keine Kante aus G aber alle Kanten, die nicht in G sind, enthält. Außerdem sei $\bar{k} = k$. Diese Eingabe ist offensichtlich in polynomieller Zeit berechenbar.

O.B.d.A. sei $I = \{v_1, \ldots, v_l\}$ ein Independent Set mit $|I| = l \geq \bar{k}$ von $\bar{G}$. Dann enthält $\bar{G}$ keine Kante $\{v_i, v_j\}$ für $1 \leq i < j \leq l$. Dagegen enthält G aber alle diese Kanten. Also enthält G auch die Clique $C = \{v_1, \ldots, v_l\}$ mit $|C| = l \geq k$. Also

$$\text{Clique} \leq_p \text{IndependentSet}.$$

Mit dem gleichen Argument können wir auch zeigen, dass wenn G eine l-Clique enthält, auch $\bar{G}$ ein l-Independent Set enthält. Also

$$\text{IndependentSet} \leq_p \text{Clique}.$$

(b) Sei $(G = (V, E), k)$ eine Eingabe von IndependentSet, für die entschieden werden soll, ob G ein Independet Set I mit $|I| \geq k$ enthält. Aus (G, k) erzeugen wir in polynomieller Zeit eine Eingabe (G', k') für Vertex Cover, so dass (G, k) genau dann ein Independent Set I mit $|I| \geq k$ enthält, wenn (G', k') ein Vertex Cover VC mit $|VC| \leq k'$ enthält.

Die Eingabe (G', k') konstruieren wir wie folgt. Sei $G' = G$ und $k' = n - k$. Diese Eingabe ist offensichtlich in polynomieller Zeit berechenbar.

O.B.d.A. sei $VC = \{v_1, \ldots, v_l\}$ ein Vertex Cover VC mit $|VC| = l \leq k' = n - k$ von $G' = G$, d.h. jede Kante von G ist zu mindestens einem der Knoten aus VC inzident. Wir behaupten $I = V \backslash VC$ ist ein Independent Set der Größe mindestens k ist. Offensichtlich ist $|I| = n - l \geq k$. Außerdem enthält I keine zwei Knoten v, w so dass die Kante $\{v, w\}$ existiert. Anderenfalls wäre VC kein Vertex Cover. Also ist I ein $(n - l)$-Independent Set. Also

$$\text{IndependentSet} \leq_p \text{VertexCover}.$$

Mit dem gleichen Argument können wir auch zeigen, dass wenn G ein Independet Set I mit $|I| \geq k$ enthält, auch G' ein Vertex Cover VC mit $|VC| \leq n - k$ enthält. Also

$$\text{VertexCover} \leq_p \text{IndependentSet}.$$

(c) Es gilt nach (a)und (b)

$$\text{VertexCover} \leq_p \text{IndependentSet} \leq_p \text{Clique}.$$

Aufgabe 9.2: **(3+3+4 Punkte)**

(a) **Composite:** Wähle einen Faktor als Zertifikat.

Zertifikat: Ein Wort $y \in \{0,1\}^n$ der Länge höchstens $|w|$, das die Binärkodierung einer Zahl b darstellt.

Polynomialzeitverifizierer:

1. Prüfe, ob $y \in \{0,1\}^n$, ob y die Binärkodierung einer Zahl b darstellt, und ob $1 < b < k$.
2. Teile k mit Rest durch b.
3. Falls der Rest gleich 0 ist, dann akzeptiere.

Laufzeit: Der Test im ersten Schritt benötigt höchstens Zeit $O(|w|)$. Außerdem benötigt sowohl die Division als auch der Vergleich Zeit $O(|w|)$ auf der RAM bzgl. des logarithmischen Kostenmaßes. Insgesamt folgt eine Laufzeit von $O(|w|)$.

(b) **VertexCover:** Wähle eine Knotenteilmenge der Größe k als Zertifikat.

Sei $V = \{1, \ldots, n\}$, $|V| = n$, $|E| = m$.

Zertifikat: Ein Wort $y \in \{0,1\}^n$ der Länge n mit der folgenden Bedeutung: Falls $y_i = 1$, dann ist der Knoten i im VertexCover.

Polynomialzeitverifizierer:

1. Prüfe, ob y genau k Einsen enthält.
2. Prüfe für jede Kante $\{i, j\}$, ob $y_i = 1$ oder $y_j = 1$.

Laufzeit: Der Test in Schritt 1 benötigt höchstens Zeit $O(n)$ zum Lesen von y und Zeit $O(k^2) = O(n^2)$ zum Zählen der Einsen in y. Der Test im zweiten Schritt benötigt analog zur Analyse bzgl. des Problems Graphzusammenhang in der Vorlesung Zeit $O(\log n)$ pro Kante, insgesamt also $O(m \log n) = O(n^2 \log n)$. Als Gesamtlaufzeit folgt

$$O(n) + O(n^2) + O(n^2 \log n) = O(n^2 \log n).$$

(c) **k-kürzester Weg:** Es ist nicht bekannt, ob es in NP ist. Beachte: k kann exponentiell groß sein. Eine einfach Aufzählung von k verschiedenen Pfaden ist dann i.A. nicht polynomiel beschränkt.

Aufgabe 9.3: **(5+5 Punkte)**

(a) Wir zeigen, dass die nachfolgende Aussage gilt.

> Wenn für ein Entscheidungsproblem A ein Polynomialzeitverifizierer V existiert, der A mit Hilfe eines Zertifikats entscheidet, das nur logarithmisch in der Eingabelänge ist, dann gilt $A \in \mathsf{P}$.

Sei dazu x die Eingabe des Entscheidungsproblems A und sei $y \in \{0,1\}^*$ ein Zertifikat der Länge $m \in O(\log |x|)$. Die Laufzeit von V sei durch ein Polynom p beschränkt.

Ein Polynomialzeitalgorithmus für A kann nun alle Zertifikate bis zur Länge m generieren und jedes dieser Zertifikate mit Hilfe von V auf Gültigkeit überprüfen.

Die Laufzeit dieses Algorithmus ist in $O(p(|x|) \cdot (\sum_{i=0}^{m} 2^i))$. Da $\sum_{i=0}^{m} 2^i = 2^{m+1} - 1$ gilt, entspricht dies

$$O(p(|x|) \cdot 2^{m+1}) = O(p(|x|) \cdot 2^{O(\log |x|)}) = O(p(|x|) \cdot |x|^{O(1)})$$

einer polynomiellen Laufzeit.

(b) Das Halteproblem.