Übungsstunde 11

Dienstag, 5. Dezember 2023 21:03

Recall: - $VP = NP$, d.h. wenn wir $\in NP$ zeigen wollen, so reicht es aus folgendes zu tun:
1. Angenommen w ist eine Lösung des Problems
2. Die Überprüfung von w muss in poly. Zeit zur Eingabe möglich sein

Intuition zu polynomiellen Reduktionen: $\leq_p \iff \leq_{EE}$ + Reduktion muss effizient sein (poly. Algo [A ist poly. Algo., falls $Time_A(n) \in \mathcal{O}(n^c)$ für eine Konstante c])

Es gilt $NP \subseteq \mathcal{L}_R \subseteq \mathcal{L}_{RE}$.

Konjunktive Normalform ≡ Formeln in der Form $(x_1 \vee x_2) \wedge (x_3 \vee \neg x_4)$

$SAT = \{\Phi \mid \Phi$ ist eine erfüllbare KNF$\}$

$VC = \{(G,k) \mid G$ ist ein ungerichteter Graph mit einer Knotenüberdeckung der Mächtigkeit $\leq k\}$

Menge von Knoten $U \subseteq V$ s.d. jede Kante mind. 1 Endknoten in U hat

$SCP = \{(X,S,k) \mid X$ hat ein Set-Cover $C \subseteq S$ mit $|C| \leq k\}$

Def.: Sei X eine Menge, $S \subseteq \mathcal{P}(X)$ mit $\bigcup_{s \in S} s = X$. Dann heißt $C \subseteq S$ Set-Cover von X, falls $X = \bigcup_{s \in C} s$.

Beh.: $VC \leq_p SCP$

Beweis: Sei $G = (V,E)$ eine Eingabe für VC und $k \in \mathbb{N}$. Wir definieren eine Eingabe für SCP wie folgt: Sei $E_v = \{e \in E \mid v$ inzident zu $e\}$ die Menge der mit $v \in V$ inzidenten Kanten und sei $S_G = \{E_v \mid v \in V\}$. Dann ist (E, S_G, k) unsere Eingabe für k.

Die Transformation ist offensichtlich in poly. Zeit durchführbar ($\mathcal{O}(|V|^{|V|-1})$)

Beh.: $(G,k) \in VC \iff (E, S_G, k) \in SCP$

Beweis:

"⇒" Sei $U \subseteq V$ ein Vertex-cover mit $|U| \leq k$. Sei $\{v_1, \dots, v_k\} = U$. Dann sind $\bigcup_{i=1}^{k} E_{v_i}$ die von U überdeckten Kanten. Klar gilt: $E_{v_i} \in S_G$ und $\bigcup_{i=1}^{k} E_{v_i} = E$. Also haben wir ein Set-cover der Größe $\leq k$ für (E, S_G, k)

"⇐" Angenommen $C \subseteq S_G$ sei ein Set-Cover, $|C| \leq k$. Also $\bigcup_{s \in C} s = E$. Damit bilden alle Knoten $v \in V$ s.d. $E_v \in C$ zusammen ein Vertex-Cover der Größe $\leq k$ in G. □

Problem $\in P$ oder $\in NP$?

Large-Clique $= \{(G,k) \mid G=(V,E)$ ist ungerichteter Graph, der eine k-Clique der Größe $k \geq |V|/3$ enthält$\}$

Very-Large-Clique $= \{(G,k) \mid G=(V,E)$ " $k \geq |V|-3$ "$\}$

Lösung: Ob das Entscheidungsproblem $\in P$ oder $\in NP$ liegt, hängt davon ab wie viele Kandidaten (hier Mengen) wir überprüfen müssen. Intuitiv:

$\binom{n}{n-3} = \frac{1}{6}(n-2)(n-1)n \in \mathcal{O}(n^3)$

$\binom{n}{n/3} = n \cdot \ldots \cdot (\frac{2}{3}n+1) \approx n! \rightsquigarrow$ exponentiell, da $e^n \in \mathcal{O}(n!)$

Also $LC \in NP$, $VLC \in P$

Beh.: $VLC \in P$.

Beweis: Für einen Graphen mit n Knoten können wir einfach alle $\sum_{j=0}^{3} \binom{n}{n-j} \in \mathcal{O}(n^3)$ möglichen Teilmengen von min. $n-3$ Knoten darauf überprüfen, ob diese eine Clique bilden. Diese Überprüfung ist für jede der Teilmengen in Zeit $\mathcal{O}(n^2)$ möglich ($< n^2$ Kanten). Also poly. LZ von $\mathcal{O}(n^5)$ $\square$

Beh.: $LC \in NP$

Beweis: Angenommen $w=(G,k) \in LC$. D.h. G hat eine k-Clique, $k \geq |V|/3$.
Wir prüfen ob w tatsächlich eine Lösung ist, indem wir sukzessive alle Knoten durchlaufen und prüfen, ob es min. $|V|/3$ Knoten gibt, die paarweise miteinander verbunden sind. Diese Überprüfung ist in poly. LZ möglich, da wir max. n^2 Vergleiche durchführen. Somit ist $LC \in NP$ $\square$

Beh.: Vertex Cover ist NP vollständig.

Beweis: Angenommen Independent Set ist NP complete, Ind.Set = ist in einem ungerichteten Graphen $G=(V,E)$ ein kantenloser Teilgraph, also $V' \subseteq V$, s.d. $\forall v,w \in V' : \{v,w\} \notin E$.

Independent Set $= \{(G,k) \mid G$ hat ein Ind.Set der Größe $\geq k\}$ (Komplement zu VC)

- Vertex Cover $\in NP$: Sei (G,k) eine Eingabe, welche in Vertex Cover liegt. Dann gibt es k' Knoten V' in G, welche ein Vertex Cover bilden. Klar: $|V'| \leq |G|$. Gegeben V', so können wir alle Kanten in G durchlaufen und prüfen, ob jede davon min. einen Endpunkt in V' hat. Dies hat Laufzeit $|E| \cdot |V'|$, was polynomiell in $|G|$ ist.

- Independent Set $\leq_p$ Vertex Cover

  Sei (G, k) eine Eingabe für Independent Set. Dann ist (G', k') eine Eingabe für Vertex Cover, wobei $G' = G$ und $k' = n - k$. $(n = |V|)$

  <u>Beh.</u>: $(G, k) \in$ Independent Set $\Leftrightarrow$ $(G', k') \in$ VertexCover

  <u>Beweis</u>: "$\Rightarrow$" G hat ein Ind.Set S, $|S| = k$. Dann ist $V' = V \setminus S$ ein VC, da keine Kante in G beide Eckpunkte in S haben kann

  "$\Leftarrow$" G' hat ein VC V', $|V'| = n - k$. Dann gibt es keine Kante in $V \setminus V' =: S$, $|S| = k$ $\square$

  Da die Konstruktion in poly. LZ möglich ist, folgt die Behauptung. $\square$

Beh.: Sei

Undirected Hamilton Cycle = $\{ G = (V, E) \mid$ Gibt es einen Kreis, der jeden Knoten in G genau einmal besucht ? $\}$
UHC

gerichteter Graph

Directed Hamilton Cycle $= \{ D = (V, A) \mid$ " gerichteten Kreis, " $\}$
DHC

Dann ist UHC $\leq_p$ DHC

Beweis: Sei G eine Eingabe für UHC. Wir konstruieren G' wie folgt:
$V(G') = V(G)$. Für jede Kante $\{v, w\} \in E(G)$ fügen wir die gerichteten Kanten (v, w) und (w, v) in $A = E(G')$ ein. Die Konstruktion ist sicher in poly. LZ in $|G|$ möglich.

"$\Rightarrow$" Angenommen $(u_1, \ldots, u_n)$ ist ein UHC in G. So ist dies auch ein DHC.

"$\Leftarrow$" Jeder DHC ist auch ein UHC. $\square$ $\square$

Beh.: Dreifach-SAT ist NP-vollständig (Dreifach-SAT $\equiv$ alle KNF mit min. 3 versch. erfüllenden Belegungen)

Beweis: 1. Da Dreifech-SAT $\subseteq$ SAT, folgt: Dreifach-SAT $\in NP$

2. Wir zeigen SAT $\leq_p$ Dreifach-SAT

Sei $F = C_1 \wedge \ldots \wedge C_m$ eine KNF über $\{x_1, \ldots, x_n\}$, $C_i = L_{i_1} \vee \ldots \vee L_{i_k}$

Wir definieren $\Phi = F \wedge D_1 \wedge D_2 \wedge D_3$, wobei $D_1 = y_1 \vee y_2$, $D_2 = y_1 \vee \bar{y}_2$, $D_3 = \bar{y}_1 \vee y_2$

mit y_1, y_2 neuen Variablen, welche nicht in F vorkommen. Die Konstruktion ist sicherlich in poly. LZ möglich.

Beh.: $F \in SAT \iff \Phi \in$ Dreifach-SAT

Beweis: "$\Rightarrow$" Angenommen $F \in SAT$. D.h. es existiert eine erfüllende Belegung α für F. Dann sind $(\alpha, \overset{y_1}{1}, \overset{y_2}{0})$, $(\alpha, 0, 1)$, $(\alpha, 1, 1)$ drei erfüllende Belegungen für Φ, also $\Phi \in$ Dreifach-SAT.

"$\Leftarrow$" Angenommen $\Phi \in$ Dreifach-SAT. D.h. es existiert eine erfüllende Belegung β für Φ. Aber falls Φ erfüllt ist, so <u>muss</u> F auch erfüllt sein über $\{x_1, \ldots, x_n\}$. Also $F \in SAT$ $\square$

Da SAT NP-Schwer ist, folgt Dreifach-SAT ist NP-complete $\blacksquare$

ETH zürich
Departement Informatik

Theoretische Informatik

Prof. Dr. Juraj Hromkovič
Dr. Hans-Joachim Böckenhauer
Prof. Dr. Dennis Komm

Lösungsvorschläge – Blatt 10

Zürich, 8. Dezember 2023

Lösung zu Aufgabe 27

(a) Die Idee unserer Reduktion ist es, SCP als eine Verallgemeinerung von VC anzusehen.

Die Eingabe für VC ist ein Graph $G = (V, E)$ und eine natürliche Zahl k. Jede solche Eingabe bilden wir wie folgt auf eine Eingabe für SCP ab. Sei $E_v := \{e \in E \mid v \text{ ist inzident zu } e\}$ die Menge der mit dem Knoten v inzidenten Kanten und sei $\mathcal{S}_G = \{E_v \mid v \in V\}$. Dann ist

$$(E, \mathcal{S}_G, k)$$

unsere Eingabe für SCP. Die Mengenfamilie $\mathcal{S}_G$ enthält also für jeden Knoten v die Menge aller Kanten, die inzident mit v sind. Man beachte, dass zwei Knoten v und w dieselbe Menge $E_v = E_w$ inzidenter Kanten haben können; in diesem Fall ist E_v nur einmal in $\mathcal{S}$ enthalten.

Die Transformation ist offensichtlich in polynomieller Zeit durchführbar. Es bleibt noch zu zeigen, dass (G, k) genau dann eine zu akzeptierende Eingabe für VC ist, wenn $(E, \mathcal{S}_G, k)$ eine zu akzeptierende Eingabe für SCP ist.

Angenommen, es gibt ein Vertex-Cover der Grösse k in G. Dann gibt es eine Menge von k Knoten $\{v_1, v_2, \ldots, v_k\}$, die alle Kanten in G überdeckt. Wir können die überdeckten Kanten zudem durch $\bigcup_{i=1}^{k} E_{v_i}$ beschreiben. Jede Menge E_{v_i} ist in $\mathcal{S}_G$. Dementsprechend gibt es ein Set-Cover der Grösse höchstens k für $(E, \mathcal{S}_G, k)$.

Angenommen, es gibt ein Set-Cover der Grösse k für $(E, \mathcal{S}_G, k)$. Dann gibt es ein $\mathcal{C} \subseteq \mathcal{S}_G$, so dass $|\mathcal{C}| = k$ und $\bigcup_{S \in \mathcal{C}} S = E$ gilt. Damit ist die Menge der k Knoten, die in unserer Reduktion auf die Mengen aus $\mathcal{C}$ abgebildet werden, inzident mit allen Kanten aus E. Dementsprechend bilden diese Knoten ein Vertex-Cover der Grösse k in G. Falls mehrere Knoten dieselbe Menge inzidenter Kanten haben und deshalb auf dieselbe Menge aus $\mathcal{C}$ abgebildet werden, reicht es offenbar aus, für jede solche Menge aus $\mathcal{C}$ einen solchen Knoten für den Vertex-Cover auszuwählen.

(b) Sei $(X, \mathcal{S}, k)$ eine Eingabe für SCP mit $X = \{x_1, x_2, \ldots, x_n\}$ und $\mathcal{S} = \{S_1, S_2, \ldots, S_m\}$ und einer natürlichen Zahl k. Jede solche Eingabe bilden wir wie folgt auf eine Eingabe (G, k) mit $G = (V, E)$ für DS ab. Für die Knoten von G gilt $V = V_X \mathbin{\dot\cup} V_{\mathcal{S}}$ mit $V_X = \{x_1, x_2, \ldots, x_n\}$ und $V_{\mathcal{S}} = \{s_1, s_2, \ldots, s_m\}$, wobei V_X also den Elementen aus

X entspricht und $V_{\mathcal{S}}$ den Mengen aus $\mathcal{S}$. Für die Kanten von G gilt zum einen, dass die Knoten aus $V_{\mathcal{S}}$ eine Clique bilden. Ferner ist

$$\{x_i, s_j\} \in E \iff x_i \in S_j \ ,$$

d. h., eine Kante zwischen einem Knoten von V_X und einem Knoten von $V_{\mathcal{S}}$ gibt es genau dann, wenn das Element $x_i \in X$ in der Menge $S_j \in \mathcal{S}$ enthalten ist, das S_j das Element x_i also überdeckt. Es gibt keine Kanten zwischen den Knoten aus V_X. Diese Konstruktion kann offensichtlich in polynomieller Zeit durchgeführt werden.

Sei nun $(X, \mathcal{S}, k)$ eine Eingabe für SCP, so dass X ein Set-Cover aus $\mathcal{S}$ der Grösse k besitzt; sei $\mathcal{C}$ ein solches Set-Cover. Die entsprechenden Knoten aus $V_{\mathcal{S}}$ sind ein Dominating-Set D derselben Grösse, was wie folgt begründet werden kann. Alle Knoten aus $V_{\mathcal{S}}$ sind trivialerweise dominiert, da $V_{\mathcal{S}}$ eine Clique ist. Ferner ist jeder Knoten aus V_X adjazent zu einem ausgewählten Knoten in $V_{\mathcal{S}}$, da jedes Element aus X in mindestens einer Menge aus $\mathcal{C}$ beinhaltet ist.

Sei andererseits D ein Dominating-Set der Grösse k von G. Falls $D \subseteq V_{\mathcal{S}}$, ist die entsprechende Auswahl an Mengen aus $\mathcal{S}$ ein Set-Cover der gleichen Grösse für X, was wie oben begründet werden kann. Falls ein Knoten $x \in D \setminus V_{\mathcal{S}}$ existiert, so können wir D modifizieren, indem wir x gegen einen adjazenten Knoten aus $V_{\mathcal{S}}$ austauschen. Die beiden Knoten bleiben dabei dominiert und kein anderer Knoten von V_X verliert mit x einen dominierenden Knoten, da sie untereinander nicht verbunden sind, während die Knoten aus $V_{\mathcal{S}}$ in jedem Fall dominiert sind (da $V_{\mathcal{S}}$ eine Clique ist).

Lösung zu Aufgabe 28

Es gilt TRIPEL-SAT $\in$ NP, denn eine NTM kann drei verschiedene Belegungen nichtdeterministisch raten und überprüfen, dass diese drei Belegungen die gegebene Formel erfüllen. Dies ist offenbar in polynomieller Zeit möglich.

Um zu zeigen, dass TRIPEL-SAT NP-schwer ist, zeigen wir SAT $\leq_p$ TRIPEL-SAT.

Sei ϕ eine Eingabe für SAT, also eine KNF-Formel $\phi = C_1 \wedge \ldots \wedge C_m$ mit den Klauseln $C_1, \ldots, C_m$ über den Variablen aus $X = \{x_1, \ldots, x_n\}$. Wir konstruieren aus ϕ eine Eingabe ψ für TRIPEL-SAT wie folgt. Seien $y_0, y_1 \notin X$ zwei neue Variablen, die in ϕ nicht vorkommen, sei $C_{m+1} = (y_0 \vee y_1)$. Dann definieren wir $\psi = C_1 \wedge \ldots \wedge C_m \wedge C_{m+1}$. Offenbar ist die Konstruktion von ψ aus ϕ in polynomieller Zeit möglich.

Wir zeigen nun, dass ϕ genau dann erfüllbar ist, wenn ψ mindestens drei erfüllende Belegungen besitzt.

Sei ϕ erfüllbar. Dann gibt es eine Belegung $\alpha \colon X \to \{0,1\}$, die die Klauseln $C_1, \ldots, C_m$ erfüllt. Wir können α zu drei Belegungen $\beta_i \colon X \cup \{y_0, y_1\} \to \{0,1\}$ für $i \in \{1,2,3\}$ erweitern, indem wir $\beta_1(x) = \beta_2(x) = \beta_3(x) = \alpha(x)$ setzen für alle $x \in X$, sowie $\beta_1(y_0) = \beta_2(y_0) = \beta_2(y_1) = \beta_3(y_1) = 1$ und $\beta_3(y_0) = \beta_1(y_1) = 0$. Offenbar sind die drei Belegungen β_i für $i \in \{1,2,3\}$ alle verschieden und sie erfüllen auch alle Klauseln $C_1, \ldots, C_m$, weil α diese Klauseln erfüllt. Die Klausel C_{m+1} wird auch von β_i erfüllt, weil $\beta_1(y_0) = \beta_2(y_0) = 1$ und $\beta_3(y_1) = 1$ gilt. Also sind β_i für $i \in \{1,2,3\}$ drei erfüllende Belegungen für ψ.

Sei ϕ nicht erfüllbar. Dann gibt es keine Belegung $\alpha \colon X \to \{0,1\}$, die alle Klauseln $C_1, \ldots, C_m$ gleichzeitig erfüllt, und damit auch keine erfüllende Belegung $\beta \colon X \cup \{y_0, y_1\} \to \{0,1\}$, weil die neuen Variablen y_0 und y_1 in $C_1, \ldots, C_m$ nicht vorkommen. Weil jede Klausel aus ϕ auch in ψ vorkommt, gibt es also auch keine Belegung, die ψ erfüllt.

Lösung zu Aufgabe 29

Sei ϕ eine Eingabe für SAT, also eine KNF-Formel, von der wir wissen wollen, ob sie erfüllbar ist. Wir bilden ϕ auf eine Eingabe für L_{H} ab. Zu diesem Zweck sei M eine TM, die eine Eingabe erwartet, die eine (aufgrund der Definition von L_{H} binär kodierte) KNF-Formel ist. Für jede solche Eingabe testet M jede mögliche Belegung. Wird eine erfüllende Belegung gefunden, hält M. Wird keine solche Belegung gefunden, läuft M in eine Endlosschleife. Die Eingabe für L_{H} ist

$$\mathrm{Kod}(M)\#\mathrm{Bin}(\phi) \; ,$$

wobei $\mathrm{Bin}(\phi)$ eine feste Binärkodierung von ϕ ist. Offensichtlich ist $|\mathrm{Bin}(\phi)|$ linear in der Länge von ϕ und $|\mathrm{Kod}(M)|$ ist konstant bezüglich der Länge von ϕ.

Sei nun $\phi \in \mathrm{SAT}$. Dann findet M eine erfüllende Belegung für die Eingabe $\mathrm{Bin}(\phi)$. Beachten Sie, dass es hierbei unerheblich ist, dass dies nicht effizient durchgeführt werden kann. Somit ist in diesem Fall $\mathrm{Kod}(M)\#\mathrm{Bin}(\phi) \in L_{\mathrm{H}}$.

Falls $\phi \notin \mathrm{SAT}$, so läuft M unendlich lange auf $\mathrm{Bin}(\phi)$ und es folgt $\mathrm{Kod}(M)\#\mathrm{Bin}(\phi) \notin L_{\mathrm{H}}$.