BuK Abgabe 9 | Gruppe 17

Malte Meng (354529) , Charel Ernster (318949), Sebastian Witt (354738)

December 21, 2016

1 Aufgabe 9.1

(a). **MaxSpanTree**
Sei {V,E} der Graph G und E^G die Menge der Gewichte von G. n = |E|

Zertifikat:
Z ist das Zertifikat der Form: $E_1\#E_2\#E_3\#...E_j$
E_i Index einer Kante des Spannbaumes mit i ∈ [1...j], j ≤ n

Vertifizierer:
Der Vertifizierer verifiziert das Zertifikat in polynomieller Zeit folgendermaßen (l = länge Zertifikat $l \leq 2n$):

- Prüfe ob Zertifikat in der Form "$E_1\#E_2\#E_3\#...\#E_j$" ist.

  O($2n$)
- Prüfe ob $\{E_1, ..., E_n\}$ ein Spannbaum von G ist. Prüfe ob alle v aus V verbunden sind.

  O(n)
- Prüfe ob $\sum_{i=0}^{j} E_i^G \geq c$

  O(n)

Somit kann das Zertifikat in polynomieller Zeit O(4n) verifiziert werden. Es verifiziert, dass es einen Spannbaum mit Gewicht ≥ c in G gibt. Das Entscheidungsproblem ist somit in NP.

□

(b). **Composite**
Zertifikat:
k ist keine Primzahl, somit existiert eine Zerlegung T mit $\prod_0^n T_i = k, n \in \mathbb{N}, T_i \in Primzahlen$

Z ist das Zertifikat der Form: $T_1\#T_2\#...\#T_n$.

Verifizierer: Der Vertifizierer verifiziert das Zertifikat in polynomieller Zeit folgendermaßen (l = länge Zertifikat $l \leq 2n$):

- Prüfe ob Zertifikat in der Form "$T_1\#T_2\#T_3\#...\#T_n$" ist.

  O($2n$)

- Prüfe ob $\prod_{i=0}^{n} T_i = k$

  (polynomiell lösbar)

Somit kann Z in polynomieller Zeit verifiziert werden. Es verifiziert ob das Zertifikat eine Primzahlzerlegung von der binärkodierten Zahl k ist.

□

(c). **Graphisomorphie**
Zertifikat:
Sei δ die Permutation der Indizes der Menge V_1 die so der Abbildung f $V_1 \to V_2$ entspricht, so dass $(v_i, v_j) \in E_1 \implies (f(v_i), f(v_j)) \in E_2$
das Zertifikat Z ist nun diese Permutation in Tupelschreibweise.
$\delta = (p_1, p_2, ..., p_n), Z = p_1\#p_2\#...\#p_n$

Verifizierer:
Der Verifizierer Zertifiziert das Zertifikat in polynomieller Zeit folgendermaßen:

- Prüfe ob Zertifikat in der Form "$p_1\#p_2\#p_3\#...\#p_n$" ist.

  O($2n$)

- Prüfe ob

$$\forall(v_i, v_j) \in E_1 \; \exists i' = p_i, j' = p_j, (v_{i'}, v_{j'}) \in E_2$$

  O(n)

Somit kann in polynomieller Zeit verifiziert werden ob das Zertifikat stimmt, ob also eine Permutation existiert die die Knoten von G_1 auf G_2 abbildet und Kanten erhalten bleiben. Also prüft es ob die Graphen isomorph sind.
$\Rightarrow$ Graphisomorphie $\in$ NP.

□