

# 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:  $E_1 \# E_2 \# E_3 \# \dots \# E_j$

$E_i$  Index einer Kante des Spannbaumes mit  $i \in [1 \dots j]$ ,  $j \leq n$

**Vertifizierer:**

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

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

$O(2n)$

- Prüfe ob  $\{E_1, \dots, E_n\}$  ein Spannbaum von  $G$  ist. Prüfe ob alle  $v$  aus  $V$  verbunden sind.

$O(n)$

- Prüfe ob  $\sum_{i=1}^j E_i^G \geq c$

$O(n)$

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

□

(b). **Composite**

**Zertifikat:**

$k$  ist keine Primzahl, somit existiert eine Zerlegung  $T$  mit  $\prod_0^n T_i = k, n \in \mathbb{N}, T_i \in \text{Primzahlen}$

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

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

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

$O(2n)$

- Prüfe ob  $\prod_{i=1}^n T_i = k$

(polynomiell lösbar)

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

□

(c). **Graphisomorphie**

**Zertifikat:**

Sei  $\delta$  die Permutation der Indizes der Menge  $V_1$  die so der Abbildung  $f: V_1 \rightarrow V_2$  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.

$\delta = (p_1, p_2, \dots, p_n), Z = p_1 \# p_2 \# \dots \# p_n$

**Verifizierer:**

Der Verifizierer Zertifiziert das Zertifikat in polynomieller Zeit folgendermaßen:

- Prüfe ob Zertifikat in der Form " $p_1 \# p_2 \# p_3 \# \dots \# p_n$ " 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.  
 $\Rightarrow \text{Graphisomorphie} \in \text{NP}$ .

□

## 2 Aufgabe 9.3

DoubleSAT:

- I. DoubleSAT ist in NP da ein Verifizierer leicht ein Zertifikat verifizieren kann welches der Form zwei gültiger Belegungen sind. Somit  $DoubleSAT \in NP$
- II. Reduktion von SAT auf DoubleSAT:  
Es gibt eine polynomiell berechenbare Funktion  $f$ , die SAT auf DoubleSAT abbildet.  
Diese Funktion  $f$  bildet aus den Literalen von SAT neue Literale für DoubleSAT folgendermaßen:  
KNF von SAT:  $((l_1) \wedge (l_2) \wedge \dots (l_n))$   
 $\rightarrow$   
DoubleSAT:  $((l_1 \vee x) \wedge (l_2 \vee x) \wedge \dots (l_n \vee x) \wedge (l_1 \vee \bar{x}) \wedge (l_2 \vee \bar{x}) \wedge \dots (l_n \vee \bar{x}))$
- III. Korrektheit:  
AC entspricht der KNF der Form  $((l_1 \vee x) \wedge (l_2 \vee x) \wedge \dots (l_n \vee x))$   
 $A \neg C$  entspricht der KNF der Form  $((l_1 \vee \bar{x}) \wedge (l_2 \vee \bar{x}) \wedge \dots (l_n \vee \bar{x}))$   
A entspricht der KNF der Form  $((l_1) \wedge (l_2) \wedge \dots (l_n))$

Es gibt zwei Belegungen für  $\gamma \Rightarrow$  es gibt eine Belegung für  $\delta$

Es gibt zwei Belegungen für  $\gamma \Rightarrow AC \wedge A \neg C$  hat zwei Belegungen  
 $\Rightarrow A$  hat eine Belegung  
 $\Rightarrow$  es gibt eine Belegung für  $\delta$

Es gibt eine Belegung für  $\delta \Rightarrow$  es gibt zwei Belegungen für  $\gamma$

Es gibt eine Belegung für  $\delta \Rightarrow A$  hat eine Belegung  
 $\Rightarrow AC \wedge A \neg C$  hat zwei Belegungen  
 $\Rightarrow$  es gibt zwei Belegungen für  $\gamma$

□

Somit gilt  $SAT \leq_q DoubleSAT$  und DoubleSAT ist NP-vollständig.