Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Diskrete Mathematik II

SS 2011

Blatt 4 / 10. Mai 2011 / Abgabe **bis spätestens Dienstag 24. Mai, 09:00 Uhr**

AUFGABE 1:

Die Sprache 0-1-Programmierung besteht aus (Kodierungen von) allen linearen Ungleichssystemen mit ganzahlen Koeffizienten und $\{0,1\}$-wertigen Unbekannten, die mind. eine Lösung besitzen. Formal:

$$\text{0-1-Programmierung} = \{(A,b) \in \mathbb{Z}^{n\times m} \times \mathbb{Z}^n \mid \text{ Es gibt } x \in \{0,1\}^m, \text{ so dass } Ax \leq b\}$$

Hierbei bezeichnet Ax Matrix-Vektor-Multiplikation und für zwei Vektoren $u, v \in \mathbb{Z}^m$ bedeutet $u \leq v$, dass $u_i \leq v_i$ für *alle* Komponenten u_i, v_i, $1 \leq i \leq m$ gilt.

Zeigen Sie:

(a) 0-1-Programmierung $\in \mathcal{NP}$.[3P]

(b) Subset-Sum $\leq_p$ 0-1-Programmierung[4P]

AUFGABE 2:

Betrachten Sie die Sprache:

$$\text{LängsterPfad} = \Big\{ (G,s,t,k), G=(V,E) \text{ ungerichteter Graph }, s,t \in V, k \in \mathbb{N}, \text{ wobei gilt: } G \text{ hat einen einfachen Pfad von } s \text{ nach } t \text{ der Länge mindestens } k. \Big\}$$

Zeigen Sie:

LängsterPfad ist $\mathcal{NP}$-vollständig.[9P]

Tipp: Beachten Sie, dass Sie hier 2 Dinge zeigen müssen. Wählen Sie für den Reduktionsteil ein für diese Problemstellung möglichst gut geeignetes $\mathcal{NP}$-vollständiges Problem.

Bitte wenden!

Wir betrachten die Sprache DDH' [1]

DDH' $= \{(p-1, g, g_1, g_2, g_3) \mid p$ prim,
g Erzeuger von $\mathbb{Z}_p^*, g_1 = g^a, g_2 = g^b, g_3 = g^{ab}$ für geeignete $a, b \in \mathbb{Z}\}$

Erinnerung: g heisst Erzeuger von $\mathbb{Z}_p^*$ für p prim gdw. folgendes gilt:
p prim und jedes $x \not\equiv 0 \mod p$ lässt sich als $x = g^a \bmod p$ für ein geeignetes a schreiben.

Wenn g Erzeuger von $\mathbb{Z}_p^*$ für p prim ist, gilt zudem, dass a in obiger Aussage modulo $p-1$ eindeutig bestimmt ist.

AUFGABE 3:

Welche der folgenden Tupel sind in DDH':

(a) $(16, 3, 4, 4, 1)$ [1.5P]

(b) $(16, 3, 3, 15, 7)$ [1.5P]

(c) $(16, 3, 9, 4, 16)$ [1.5P]

(d) $(65536, 3, 81, 5, 625)$ [2.5P]

Sie dürfen ohne Beweis verwenden, dass 17 und 65537 Primzahlen sind sowie, dass 3 ein Erzeuger von $\mathbb{Z}_{17}^*$ und von $\mathbb{Z}_{65537}^*$ ist.
Die Richtigkeit der Aussage ist jeweils zu begründen. Ihre Lösung soll ohne Verwendung technischer Hilfsmittel nachvollziehbar sein.

[1] Wir betrachten hier im Gegensatz zur Vorlesung nur den Spezialfall, dass g die Gruppe $\mathbb{Z}_p^*$ (die $p-1$ Elemente hat) erzeugt. Die Ordnung von g ist hiermit $(q =)p-1$ und dabei im Allgemeinen (ausser $p = 3$) nicht prim.