Institut für Informatik
der Universität München

Prof. Martin Hofmann

WS 2012/13

9. Januar 2013

Übungen zur Vorlesung Komplexitätstheorie

Blatt 10

Aufgabe P-33: Das Problem „Quadratischer Rest“ ist wie folgt definiert:

Gegeben: $n, m \in \mathbb{N}, n < m$
Frage: Gibt es $k \in \mathbb{N}$ mit $k^2 \equiv n \bmod m$

Begründen Sie, warum folgender Algorithmus zeigt, dass das Komplement von „Quadratischer Rest“ in der Klasse IP liegt.

```
1   Eingabe: n, m mit n < m
2   wähle zufällig z_1, z_2 mit z_i < m und z_i, m teilerfremd
3   wähle zufällig b_1, b_2 mit b_i ∈ {1, 2}
4   for i = 1,2 do
5       if b_i = 1 then w_i := z_i^2 mod m
6       else w_i := n z_i^2 mod m
7       done
8   übertrage w_1, w_2 an P
9   empfange c_1, c_2 von P
10  for i = 1,2 do
11      if b_i ≠ c_i then REJECT
12      done
13  ACCEPT
```

Hinweis: Beachten Sie, dass $n z_i^2 \bmod m$ genau dann ein quadratischer Rest ist, wenn n ein quadratischer Rest ist.

Aufgabe P-34: Im IP-Protokoll für UNSAT aus der Vorlesung soll der Verfier davon überzeugt werden, dass folgende Formel unerfüllbar ist:

$$(\neg a \vee b) \wedge (\neg b \vee \neg c) \wedge (c \vee \neg d) \wedge (a \vee d) \wedge (\neg a \vee c)$$

Geben Sie für die Zufallszahlen $r_1 = 3, r_2 = 5, r_3 = 7, r_4 = 9$ die Polynome $g_i(x)$ an. Nehmen Sie dafür an, dass die Primzahl p so groß ist, dass sie alle Zahlen in der Rechnung übersteigt, also rechnen Sie ohne Modulo.

Aufgabe P-35: Zeigen Sie, dass das Problem für drei gegebene Matrizen A, B, C zu zeigen, ob gilt $AB = C$ im BPP-Sinne in $O(n^2)$ lösbar ist.

Hausaufgaben:

Aufgabe H-25: Zeigen Sie, dass die Klassen DIP und IP unter FP-Reduktionen abgeschlossen sind.

Bemerkung: Der Beweis soll ab Definition erfolgen und nicht die Gleichheiten zu anderen Komplexitätsklassen verwenden.

Aufgabe H-26: Im IP-Protokoll für UNSAT aus der Vorlesung soll der Verfier davon überzeugt werden, dass folgende Formel unerfüllbar ist:

$$(a \vee b \vee \neg c) \wedge (\neg a \vee \neg b \vee c) \wedge (a \vee \neg b) \wedge (b \vee c) \wedge (\neg a \vee \neg c)$$

Geben Sie für die Zufallszahlen $r_1 = 2, r_2 = 3, r_3 = 4$ die Polynome $g_i(x)$ an. Nehmen Sie dafür an, dass die Primzahl p so groß ist, dass sie alle Zahlen in der Rechnung übersteigt, also rechnen Sie ohne Modulo.

Abgabe: Mittwoch, der 16. Januar 2013 in der Vorlesung oder bis 12:00 im Sekretariat bei Fr. Roden (Oettingenstraße L1.03).