

Übungen zur Vorlesung
Komplexitätstheorie und Effiziente Algorithmen
Wintersemester 2008/09
Blatt 14

Aufgabe 14.1 (5 Punkte)

Betrachte das Number-on-the-Forehead-Kommunikationsmodell aus Aufgabe 12.4. Wir definieren die Funktion MIP_n (*multiple inner product*) für drei Spieler und drei Bitstrings x , y und z der Länge n . Es sei $m_i = 1$ genau dann, wenn mindestens zwei der drei Bits x_i , y_i und z_i den Wert 1 haben. Sonst hat m_i den Wert 0. Schließlich ist $\text{MIP}_n(x, y, z)$ genau dann 1, wenn ungerade viele m_i den Wert 1 haben. Gib eine möglichst gute obere Schranke für die Kommunikationskomplexität von MIP_n im Number-on-the-Forehead-Modell an.

Hinweis: Versuche m_i „algebraisch“ auszudrücken.

Aufgabe 14.2 (5 Punkte)

Analysiere folgendes randomisiertes Kommunikationsprotokoll für den Gleichheitssets EQ_n . Sei p eine Primzahl größer als n^2 , aber kleiner als $2n^2$ (derartige Primzahlen existieren immer). Alice betrachtet für ihre Eingabe $a = (a_0, \dots, a_{n-1})$ das Polynom

$$f(x) = \left(\sum_{i=0}^{n-1} a_i \cdot x^i \right) \bmod p.$$

Bob betrachtet das analoge Polynom $g(x)$ bezüglich seiner Eingabe $b = (b_0, \dots, b_{n-1})$ statt a . Alice wählt zufällig t aus $\{1, \dots, p-1\}$, berechnet $f(t)$ und sendet t und $f(t)$ an Bob. Bob berechnet $g(t)$ und akzeptiert genau dann, wenn $f(t) = g(t)$ ist. Diese Entscheidung teilt er Alice mit.

1. Welche Länge hat dieses Protokoll?
2. Wie groß ist die Fehlerwahrscheinlichkeit im Fall $a = b$?
3. Wie groß ist die Fehlerwahrscheinlichkeit im Fall $a \neq b$?

Aufgabe 14.3 (5 Punkte)

Überlege dir eine Funktionenfolge $(f_n)_{n \in \mathbb{N}}$, die durch ein k -Rundenprotokoll effizient berechnet werden kann, jedoch nicht durch ein $k-1$ -Rundenprotokoll. Beweise die obere Schranke für das k -Rundenprotokoll und argumentiere, warum ein $k-1$ -Rundenprotokoll diese Funktion wohl nicht effizient lösen kann.

Aufgabe 14.4 (5 Punkte)

Zeige, dass der Anteil der Funktionen $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ mit $C_{\text{uniform}, 1/2-\varepsilon}(f) \geq n - \log(\log(n)) - O(\log(1/\varepsilon))$ mit wachsendem n gegen eins konvergiert.