

Quantum Computing

Blatt 11

H. Klauck/D. Brendel
Universität Frankfurt
WS 2005/06
6.2.06

Aufgabe 1.

Betrachten Sie das Coin Flipping Protokoll aus der Vorlesung. Analysieren Sie, mit welcher Wahrscheinlichkeit Alice gewinnt, wenn sie zwar ein korrektes Commitment sendet, aber später ein falsches a behauptet.

Aufgabe 2.

Zeigen Sie, daß ein Oblivious Transfer Protokoll benutzt werden kann, um Coin Flipping zu implementieren.

Aufgabe 3.

Es seien zwei Wahrscheinlichkeitsverteilungen p_1, \dots, p_n sowie q_1, \dots, q_n gegeben. Die Distanz zwischen diesen Verteilungen ist als $d(p, q) = \sum_{i=1, \dots, n} |p_i - q_i|$ gegeben. Zeigen Sie, daß kein Algorithmus, der entscheiden soll, ob er Stichproben der einen oder der anderen Verteilung erhält, bessere Korrektheitswahrscheinlichkeit als $0.5 + d(p, q)/4$ haben kann.

Aufgabe 4.

Es sei ein Ensemble von Quantenzuständen wie folgt gegeben: Zustand $(|0\rangle + |1\rangle)/\sqrt{2}$ mit Wahrscheinlichkeit $1/2$ und $(|0\rangle - |1\rangle)/\sqrt{2}$ mit Wahrscheinlichkeit $1/2$. Bestimmen Sie eine Purifikation des entsprechenden Gesamtzustandes.

Aufgabe 5.

Zeigen Sie, daß in einem klassischen Coin Flipping Protokoll mindestens ein Spieler mit Wahrscheinlichkeit 1 mogeln kann.

Aufgabe 6.

Es seien Zustände ρ, σ als Dichtematrizen gegeben. Was ist die optimale Messung, um die beiden Zustände voneinander zu unterscheiden ?