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

Hausübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 2 / 27. April 2016

Abgabe: 9. Mai 2016, 10.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (4 Punkte)**:**

Wir betrachten ein 3-Qubit-System im Zustand

$$|z\rangle = \frac{1+i}{2}|0_1 0_2 0_3\rangle + \frac{1}{2}|1_1 1_2 0_3\rangle + \frac{i}{2}|1_1 0_2 1_3\rangle.$$

Wir führen nun eine Messung am 1. und 3. Qubit, jeweils in der Basis $|\alpha\rangle, |\beta\rangle$, durch, wobei

$$|\alpha\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{und}$$
$$|\beta\rangle = \frac{i}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle.$$

Was sind die möglichen Messergebnisse und mit welchen Wahrscheinlichkeiten treten diese jeweils auf? In welchem Zustand befindet sich das 3-Qubit-System jeweils (je nach Messergebnis) nach der Messung?

Bemerkung: Es darf vorausgesetzt werden, dass $|\alpha\rangle, |\beta\rangle$ eine Orthonormalbasis für ein einzelnes Qubit ist. Die Indizes in der Definition von $|z\rangle$ geben an, zu welchem Qubit die jeweilige Null / Eins gehört.

AUFGABE 2 (3 Punkte)**:**

Zeigen Sie, dass jede Permutationsmatrix unitär ist.

Erinnerung: Eine Permutationsmatrix ist eine quadratische Matrix, bei der in jeder Zeile und in jeder Spalte jeweils genau eine 1 und sonst nur 0en stehen.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Sei $H_n := \bigotimes_{i=1}^{n} W_2$ und $|y\rangle$ ein Basiszustand eines n-Qubit-Systems, für $y \in \{0,1\}^n$. Zeigen Sie, dass

$$H_n|y\rangle = 2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y}|x\rangle,$$

wobei $x \cdot y$ das Skalarprodukt $\sum_i x_i y_i$ der Bitvektoren x und y ist.

Erinnerung: $W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

AUFGABE 4 (3 Punkte)**:**

(a) Geben Sie eine unitäre Matrix U an, die den Zustand $|00\rangle$ eines 2-Qubit-Systems auf den Zustand $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ (d.h. auf ein EPR-Paar) abbildet.

(b) Gibt es auch eine lokal unitäre Abbildung U', die auf den beiden Qubits separat operiert, die $|00\rangle$ auf $|\mathrm{EPR}\rangle$ abbildet?

Hinweis zu (a): Präsenzübung 2, Aufgabe 2 kann einem die Arbeit erleichtern.

AUFGABE 5 (5 Punkte)**:**

(Fortsetzung Präsenzübung 2, Aufgabe 4)
Alice und Bob teilen sich ein $n+m$-Qubit-System, wobei Alice die ersten n Qubits besitzt und Bob die anderen m.

Das $n+m$-Qubit-System befinde sich im Gesamtzustand $|x\rangle$. Alice und Bob führen nun eine lokal unitäre Operation U_A bzw. U_B auf ihren jeweiligen Qubits aus.

(a) Zeigen Sie, dass der Zustand $|x'\rangle$ des Systems nach dieses beiden Operationen nicht davon abhängt, ob zuerst Alice oder ob zuerst Bob seine Operation durchführt.

Das $n+m$-Qubit-System befinde sich nun im Gesamtzustand $|y\rangle$. Alice führt eine Messung an einem Teil ihrer Qubits durch und Bob wendet eine lokal unitäre Operation U_B auf seinen Qubits an.

(b) Zeigen Sie, dass die Wahrscheinlichkeit, dass Alice ein mögliches Ergebnis $|v\rangle$ misst, nicht davon abhängt, ob sie vor oder nach Bobs Operation misst.

(c) Zeigen Sie, dass für jedes mögliche Messergebnis $|v\rangle$ der Gesamtzustand $|y'\rangle$ des Systems nach Messung von $|v\rangle$ und Anwenden von U_B nicht davon abhängt, ob Alice ihre Messung vor oder nach Bobs Operation durchführt.