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

Präsenzübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 2 / 02. Mai 2016

AUFGABE 1:

Gegeben Sei ein 2-Qubit System im Zustand $|z\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$. Wenden Sie die lokal unitäre Matrix $\sqrt{M_\neg} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$ auf das 2. Qubit an. Was ist der resultierende Zustand?

AUFGABE 2:

Wir betrachten folgende Zustände eines 2-Qubit-Systems:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big)$$

(a) Zeigen Sie, dass obige 4 Zustände eine Orthonormalbasis bilden (die sogenannte Bell - Basis).

(b) Geben Sie 4 *lokal* unitäre Matrizen $U^{(00)}, U^{(01)}, U^{(10)}, U^{(11)}$ an, die auf dem 1. Qubit wirken, so dass gilt: $\big(U^{(ij)} \otimes \mathrm{id}\big)\beta_{00} = \beta_{ij}$, d.h. man kann mittels dieser lokal unitären Matrizen zwischen den Elementen der Bell-Basis wechseln.

(c) Zeigen Sie, dass alle β_{ij} verschränkt sind.

(d) Beschreiben Sie das Superdense-Coding Protokoll mittels der Bell-Basis, wobei der Empfänger Bob in der Bell-Basis messen darf.

Bitte wenden!

AUFGABE 3:

Entscheiden Sie ob folgende 2-Qubit Systeme verschränkt oder separabel sind.

1. $|z_1\rangle = \frac{1}{2}\big(|00\rangle - |01\rangle - |10\rangle + |11\rangle\big)$
2. $|z_1\rangle = \frac{1}{2}\big(|00\rangle + |01\rangle - |10\rangle + |11\rangle\big)$

Mit welcher Wahrscheinlichkeit messen Sie $|0\rangle$ bzw. $|1\rangle$ im 1. Qubit? In welchem Zustand befindet sich danach das 2. Qubit?

AUFGABE 4:

Alice und Bob führen ein Quantenprotokoll durch. Dabei teilen sich Alice und Bob ein $n+m$ -Qubit-System, wobei Alice Zugriff auf die ersten n Qubits hat und Bob auf die verbleibenden m. Während des Protokolls (oder eines Teils des Protokolls) führen Alice und Bob *Messungen* und *lokal unitäre Operationen* auf den ihnen zugeordneten Qubits aus, wobei die Aktionen evtl. von vorherigen Messungen / Eingaben abhängen können. Wenn sie nicht miteinander kommunizieren, wissen Alice und Bob nicht voneinander, wie weit der jeweils andere mit seinem Teil des Protokolls schon ist. Wir wollen zeigen, dass dies kein Problem darstellt.

(a) Überlegen Sie sich, was man hier alles zeigen muss.

(b) Nehmen Sie an, Alice und Bob führen beide je eine Messung an einem Teil ihrer Qubits durch. Die Ergebnisse der Messungen seien M_A bzw. M_B. Zeigen Sie, dass die gemeinsame Verteilung der Messergebnisse (M_A, M_B) nicht von der Reihenfolge der Messungen abhängt. Zeigen Sie weiterhin, dass für jedes Paar (M_A, M_B) von Messergebnissen der Zustand des $n + m$-Qubit-Gesamtsystems nach den Messungen nicht von der Reihenfolge der Messungen abhängt.

(Die Aufgabe wird in der Hausübung fortgesetzt)

AUFGABE 5:

Seien $A \in \mathbb{C}^{n\times n}$ und $B \in \mathbb{C}^{m\times m}$ unitäre Matrizen.
Zeigen Sie, dass dann auch $A\otimes B$ unitär ist.