Prof. Dr.Werner Bley
Eva Brenner

21.11.2023

# 6. Übungsblatt Quantencomputing

**Aufgabe 1** Seien $H^A$ und $H^B$ endlich dimensionale Hilberträume der Dimensionen $n_A$ und $n_B$. Seien $\mathcal{B}_A = \{e_a, a = 1, \ldots, n_A\}$ und $\mathcal{B}_B = \{f_b, b = 1, \ldots, n_B\}$ Orthonormalbasen von $H^A$ und $H^B$. Es sei $H = H^A \otimes H^B$ und

$$|\Psi\rangle = \sum_{a,b} \psi_{ab} |e_a\rangle \otimes |f_b\rangle$$

ein reiner Zustand auf dem Gesamtsystem $H$. Zeige, dass man den reduzierten Dichteoperator $\rho^A(\Psi)$ in der Form

$$\rho^A(\Psi) = \sum_a q_a |\tilde{e}_a\rangle\langle\tilde{e}_a|$$

mit einer ON-Basis $\widetilde{\mathcal{B}}_A = \{\tilde{e}_a, a = 1, \ldots, n_A\}$ und $q_a \in \mathbb{R}_{\geq 0}$ schreiben kann. Definiere $\tilde{\psi}_{ab} \in \mathbb{C}$ durch

$$|\Psi\rangle = \sum_{a,b} \widetilde{\psi}_{ab} |\tilde{e}_a\rangle \otimes |f_b\rangle$$

und zeige:

$$q_a = 0 \iff \widetilde{\psi}_{ab} = 0 \text{ für alle } b.$$

Für $q_a > 0$ definiere

$$|\tilde{f}_a\rangle := \frac{1}{\sqrt{q_a}} \sum_b \widetilde{\psi}_{ab} |f_b\rangle$$

und zeige, dass man diese $|\tilde{f}_a\rangle$ zu einer ON-Basis von $H^B$ ergänzen kann. Zeige schließlich:

$$|\Psi\rangle = \sum_a \sqrt{q_a} |\tilde{e}_a\rangle \otimes |\tilde{f}_a\rangle.$$

Man nennt dies die *Schmidt-Zerlegung* von $|\Psi\rangle$. Zeige abschließend:

$$\rho^A(\Psi) = \sum_a q_a |\tilde{e}_a\rangle\langle\tilde{e}_a|, \quad \rho^B(\Psi) = \sum_a q_a |\tilde{f}_a\rangle\langle\tilde{f}_a|.$$

**Aufgabe 2** In dieser Aufgabe wird der *Algorithmus von Deutsch* analysiert.
Sei $B = \{0, 1\}$ und $f \colon B \longrightarrow B$ eine Funktion. Offensichtlich ist $f$ entweder konstant (Typ (K)) oder bijektiv (Typ (B)). Wir wollen entscheiden, von welchem Typ eine gegebene Funktion $f$ ist. Ein klassischer Computer muss dazu die Funktion $f$ zweimal auswerten. Ein Quantencomputer schafft es mit nur einer Funktionsauswertung. Betrachte dazu die Abbildung

$$B^2 \xrightarrow{\pi_f} B^2, \quad (a, b) \mapsto (a, f(a) \text{ XOR } b).$$

Sei $H = {}^qH \otimes {}^qH$ und $U_f \colon H \longrightarrow H$ die durch die Permutation $|ab\rangle \mapsto |\pi_f(a, b)\rangle$ der Rechenbasis definierte lineare Abbildung. Zeige, dass $U_f$ unitär ist.
Analysiere nun den folgenden Algorithmus und beweise seine Korrektheit.

1. Präpariere den Anfangszustand $|01\rangle$.
2. Wende $H \otimes H$ an.
3. Wende $U_f$ an.

4. Wende $H \otimes H$ an.

5. Messe in der Rechenbasis. Falls $|01\rangle$ gemessen wird, so liegt Typ (K) vor, falls $|11\rangle$ gemessen wird, so liegt Typ (B) vor.

**Aufgabe 3** Programmieren Sie den Algorithmus von Deutsch.

**Aufgabe 4**
Studieren Sie im Protokoll zur Kryptographie aus dem SS 2023 die Abschnitte 4.6 und 4.7 zur Theorie der Kettenbrüche. Ausführlich ist dies teilweise im Buch von Otto Forster, Algorithmische Zahlentheorie, Kap.26, dargestellt.

Zu bearbeiten bis: Mi 30.11.2023