Prof. Dr. A. Goerdt
A. Oertel

TU Chemnitz
Sommersemester 2020
3. Juni 2020

Einführung Quantencomputing

Lösungen zur 4. Übung

Aufgabe 1: Zeigen Sie die folgende Abschätzung, welche bei Simon's Algorithmus für die Wahrscheinlichkeit der Ziehung von $n-1$ linear unabhängigen Vektoren Verwendung findet.

$$P(n-1 \text{ linear unabhängige Vektoren}) = \left(1-\frac{1}{2^{n-1}}\right)\cdot\ldots\left(1-\frac{1}{4}\right)\cdot\left(1-\frac{1}{2}\right) \geq \frac{1}{4}$$

Hinweis: Überlegen Sie sich, wann $(1-a_1)(1-a_2) \geq 1-(a_1+a_2)$ und weiter $\prod_{i=1}^{n}(1-a_i) \geq 1-(\sum_{i=1}^{n} a_i)$ gilt. Diese Abschätzung kann nun auf alle bis auf den letzten Faktor anwenden werden. Dann kann die geometrische Reihe $\sum_{i=0}^{\infty} 1/2^i = 2$ angewendet und das Ergebnis berechnet werden.

Lösung 1:

$$(1-a_1)(1-a_2) = 1-a_1-a_2+a_1a_2 \geq 1-(a_1+a_2)$$

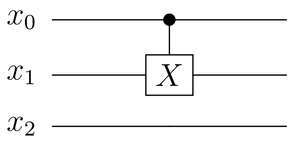
Das gibt das den Induktionsanfang für allgemeines n. Als Induktionsschritt gibt es

$$\begin{aligned}\prod_{i=1}^{n}(1-a_i)\cdot(1-a_{n+1}) \geq \left(1-\sum_{i=1}^{n} a_i\right)\cdot(1-a_{n+1}) &= 1-\sum_{i=1}^{n} a_i - a_{n+1} + \sum_{i=1}^{n} a_i a_{n+1} \\ &\geq 1-\sum_{i=1}^{n+1} a_i.\end{aligned}$$

Angewendet auf alle Faktoren bis auf den letzten Faktor ergibt sich

$$\begin{aligned}\left(1-\left(\frac{1}{2^{n-1}}+\ldots+\frac{1}{4}\right)\right)\cdot\left(1-\frac{1}{2}\right) &= \left(1-\frac{1}{4}\left(\frac{1}{2^{n-3}}+\ldots+1\right)\right)\cdot\left(1-\frac{1}{2}\right) \\ &\geq \left(1-\frac{2}{4}\right)\cdot\left(1-\frac{1}{2}\right) \\ &\geq \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}.\end{aligned}$$

Aufgabe 2: Stellen Sie die 8×8 Matrix auf, welche den folgenden Schaltkreis repräsentiert.



Lösung 2:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Daraus wird

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Aufgabe 3: Wir betrachten das No-Cloning-Theorem. Unter bestimmten Eigenschaften können Zustände trotzdem kopiert werden. Wir betrachten eine Kopieroperation, welche die folgenden beiden Abbildungen erfüllt.

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Wie kann diese Operation, unter Verwendung der Kopieroperation für die Standardbasis, realisiert werden?

Lösung 3: In der Standardbasis nutzen wir

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Der Trick ist die Bits vor der Anwendung von $CNOT$ in die Standardbasis zu transformieren und danach dann wieder zurück zu transformieren über die Inverse/Transponierte. Basistransformation muss von

$$\begin{pmatrix}1\\1\end{pmatrix} \mapsto \begin{pmatrix}1\\0\end{pmatrix}$$

$$\begin{pmatrix}1\\-1\end{pmatrix} \mapsto \begin{pmatrix}0\\1\end{pmatrix}$$

oder andersherum

$$\begin{pmatrix}1\\0\end{pmatrix} \mapsto \begin{pmatrix}1\\1\end{pmatrix}$$

$$\begin{pmatrix}0\\1\end{pmatrix} \mapsto \begin{pmatrix}1\\-1\end{pmatrix}.$$

Von der Standardbasis zu unserer Basis ergibt sich

$$\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

und damit gesamt die Rücktransformation

$$\begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{pmatrix},$$

was äquivalent zur Hintransformation ist. Damit ergibt sich die Kopieroperation

$$\begin{aligned}&\begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{pmatrix} \cdot \begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{pmatrix} \cdot \begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & 1 & -1 & -1\\1 & -1 & -1 & 1\end{pmatrix} \cdot \begin{pmatrix}1 & 1 & 1 & 1\\1 & -1 & 1 & -1\\1 & -1 & -1 & 1\\1 & 1 & -1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\end{pmatrix}\end{aligned}$$