Übungen zur Vorlesung Quantencomputer – Blatt 2
Wintersemester 2010-2011*

(Dated: 17. Dezember 2010)

I. ANWESENHEITSÜBUNG: DAS "NO-CLONING" THEOREM

Beim klassischen Computer kann man die Information in einem Bit perfekt auf ein zweites kopieren. Wir wollen nun untersuchen, ob dies bei einem Quantencomputer auch möglich ist. Es sei Qubit 1 das zu kopierende Qubit und Qubit 2 das ursprünglich leere Qubit (im Zustand $|0\rangle_2$), das nach der Kopieroperation C den gleichen Zustand wie Qubit 1 haben soll. Die Notation wird im folgendem an einem Beispiel verdeutlicht, in dem wir als zu kopierende Zustände von Qubit 1 die Zustände $|0\rangle_1$ bzw. $|1\rangle_1$ wählen:

$$C|0\rangle_1|0\rangle_2 \rightarrow |0\rangle_1|0\rangle_2$$
$$C|1\rangle_1|0\rangle_2 \rightarrow |1\rangle_1|1\rangle_2$$

Beweisen Sie, daß nicht jedes beliebige Qubit mit C korrekt kopiert wird.

II. HAUSAUFGABE: UNIVERSALE GATTER

Um tatsächlich einen Quantencomputer bauen zu können, ist es wesentlich, dass man jede beliebig komplizierte Operation in kleinere Standardoperationen zerlegen kann. Denn in einem real existierenden Quantencomputer wird man natürlich nur eine endliche Zahl an Standardoperationen durchführen können, und will trotzdem jedes beliebige Problem berechnen können. Glücklicherweise kann man zeigen, daß es einen Satz an Gattern - sogenannte *universale Gatter* - gibt, mit denen man jede unitäre Operation $\mathbf{U}$ mit beliebig hoher Genauigkeit annähern kann. Man braucht dazu nur ein einziges 2 Bit Gatter, nämlich CNOT. Desweiteren muss man noch beliebige 1 Bit Operationen (Drehungen auf der Blochkugel) ausführen können. Diese kann man durch eine Kombination von den drei Gattern approximieren. Dies wollen wir im Folgenden mit Aufgaben beweisen bzw. veranschaulichen.

A. Zerlegung von U in 2-Niveau Matrizen $\mathbf{U}_i$

Jede unitäre Operation auf n Qubits lässt sich als $d \times d$ (mit $d = 2^n$) Matrix darstellen, wie hier am Bsp. n=2 gezeigt wird.

$$\mathbf{U} = a|00\rangle\langle 00| + b|00\rangle\langle 01| + ... = \begin{bmatrix} a_{|00\rangle\langle 00|} & b & c & d \\ e_{|01\rangle\langle 00|} & f & g & h \\ i_{|10\rangle\langle 00|} & j & k & l \\ m_{|11\rangle\langle 00|} & n & o & p \end{bmatrix}$$

Eine 2-Niveau Matrix ist definiert als eine Operation, die nur auf maximal 2 Vektoren nichttrivial wirkt, z.B. verändert U_{Bsp} nur die Zustände $|00\rangle$ und $|10\rangle$, während Controlled u im allgemeinen eine Drehung auf den Zuständen $|10\rangle$ und $|11\rangle$ bewirkt. CNOT ist ein Spezialfall von Controlled u mit u= σ_x:

$$U_{Bsp} = \begin{bmatrix} u & 0 & v & 0 \\ 0 & 1 & 0 & 0 \\ x & 0 & y & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad Controlled\, u = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}, \qquad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

1. Beweise, dass sich $\mathbf{U}$ in unitäre 2-Niveau Matrizen U_i zerlegen lässt nach dem Schema

$$U_k U_{k-1} ... U_2 U_1 \mathbf{U} = \mathbf{1}. \tag{1}$$

---

*bei Fragen: henning.moritz@physik.uni-hamburg.de, rodolphe.letargat@physik.uni-hamburg.de

Man kann also jede beliebige unitäre Operation **U** berechnen durch eine Abfolge von 2-Niveau Gattern U_i: $\mathbf{U} = U_1^\dagger U_2^\dagger ... U_{k-1}^\dagger U_k^\dagger$.

Tip: Finde 2-Niveau Matrizen U_i, mit denen man nacheinander die nichtdiagonalen Einträge von **U**, Spalte für Spalte, beginnend bei e eliminieren kann.

2. Nach diesem Schema braucht man maximal $k = \frac{d(d-1)}{2}$ Schritte U_i. Viele Operationen **U** kann man natürlich in sehr viel weniger Schritten zerlegen. Zu zeigen ist aber, dass es Operationen **U** gibt, die man nicht in Produkte mit weniger als (d-1) 2-Niveau Matrizen zerlegen kann.

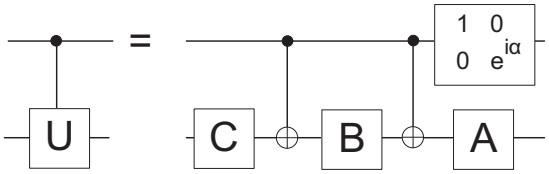
B. Erzeugung der $\mathbf{U}_i$ durch CNOT und 1 Bit Gatter (14Punkte)

Nachdem wir die **U** schon in 2-Niveau Matrizen zerlegen konnten, wollen wir uns mit der Darstellung der 2-Niveau Matrizen durch CNOT und beliebige 1 Bit Gatter beschäftigen. In Aufgaben B.1-4 werden wir uns dabei auf die Darstellung von Zweiniveau Matrizen beschränken, die von der folgenden Form sind:

$$U_i = \begin{bmatrix} 1 & 0 & . & 0 & 0 \\ 0 & 1 & . & 0 & 0 \\ . & . & . & . & . \\ 0 & 0 & . & u_{00} & u_{01} \\ 0 & 0 & . & u_{10} & u_{11} \end{bmatrix}, \tag{2}$$

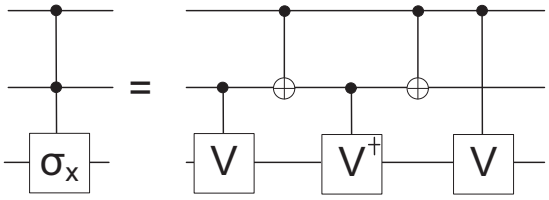
Den allgemeineren Fall können Sie in Nielsen + Chuang Kap. 4.5.2 nachlesen. Aufgabe B5 vertieft dieses Kapitel.

1. Als erstes wollen wir das allgemeine C(u) (Controlled u) durch CNOT und 1Bit Gatter darstellen. Dazu benutzen wir, dass man jede 2x2 Matrix u als $u = e^{i\alpha} A\sigma_x B\sigma_x C$ darstellen kann mit $ABC = \mathbf{1}$. Überprüfe den folgenden Schaltkreis:



Es ist praktisch, dies mit einer Wahrheitstabelle zu tun.

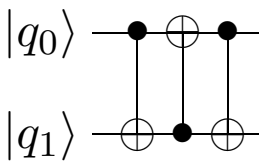
2. Das Toffoli-Gatter ($C^2(\sigma_x)$) ist ein Gatter auf drei Qubits und und vertauscht nur die Zustände $|110\rangle$ und $|111\rangle$. Es ist also eine Erweiterung des CNOT Gatters, da es nur dann auf Qubit C ein NOT anwendet, wenn A=1 und B=1. Zeige die folgende Identität, wobei V eine unitäre Matrix ist und $V^2 = \sigma_x$.



Allgemeiner lässt sich ein C^2(u) (Controlled u mit 2 Control-Qubits) ebenso darstellen, wenn man V so wählt, dass $V^2 = u$.

3. Leider ist hier noch eine "Controlled V" Operation, die Qubit A mit C verknüpft. Um dies zu beheben, ist die folgende Operation nützlich. Was macht Sie und wie können wir sie für Aufgabe 2 benutzten?

4. Konstruiere ein $C^3(\sigma_x)$, wobei man Toffoli-Gates benutzen darf, auch wenn sie nicht auf nächste Nachbarn wirken. Tip: Aufgabe 2 erweitern.



5. Das Fredkin-Gatter (Controlled Swap) ist folgendermaßen definiert:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Gib einen Schaltkreis an, der 3 Toffoli Gatter benutzt, um das Fredkin-Gatter zu erzeugen. (Tip: Lies Kapitel 4.5.2 im Nielsen + Chuang)