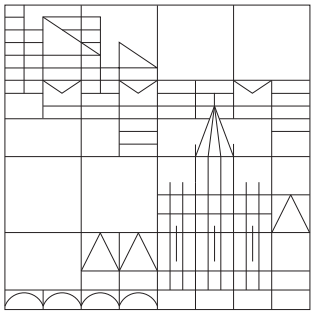
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Erik Welander
http://theorie.physik.uni-konstanz.de/burkard/teaching/13S-QI



Quanteninformationstheorie
Sommersemester 2013 - Übungsblatt 10
Ausgabe: 09.07.2013, Abgabe: 16.07.2013, Übungen: 18./19.07.2013

Aufgabe 1 : Universalität des CNOT-Gatters

a) Sei U eine beliebige 2×2 unitäre Matrix. Finden Sie unitäre Matrizen A, B, C mit den Eigenschaften

$$ABC = \mathbb{1}$$

und

$$e^{i\gamma} A\sigma_x B\sigma_x C = U,$$

Hinweis: Es gilt, dass $U = e^{i\gamma} R_z(\psi) R_y(\theta) R_z(\phi)$ (vgl. Eulerrotation), und $\sigma_x R_{y/z}(\phi)\sigma_x = R_{y/z}(-\phi)$.

b) Betrachten Sie ein Gatter mit Wirkung $U_\alpha = e^{i\alpha}\mathbb{1}$ auf dem zweiten Qubit falls das erste Qubit sich im Zustand $|1\rangle$ befindet und sonst $\mathbb{1}$. Zeigen Sie, dass U_α eigentlich ein Einzelqubitgatter ist.

c) Konstruieren Sie eine Schaltung, die aus CNOT-Gattern und Einzelqubitgattern besteht und ein *controlled-U*-Gatter implementiert, wo U eine beliebige unitäre 2×2 Abbildung ist.

Aufgabe 2 : Kettenbrüche

Ein Bruch p/q lässt sich als

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots + 1/a_M}} \equiv [a_0, \ldots, a_M]$$

($a_n \in \mathbb{N}$) darstellen. Die rationelle Zahl $p_n/q_n = [a_1, a_2, \ldots a_n], n < N$ wird *n-ter Näherungsbruch* gennant.

a) Berechnen Sie a_i für 19/17 und 77/65.

b) Die Näherungsbrüche können durch $p_0 = a_0, q_0 = 1, p_1 = 1 + a_0 a_1, q_1 = a_1$ und

$$p_n = a_n p_{n-1} + p_{n-2},$$
$$q_n = a_n q_{n-1} + q_{n-2},$$

für $2 \leq n \leq N$ rekursiv berechnet werden. Zeigen Sie, dass $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ für $n \geq 1$.

c) Sei $x \in \mathbb{Q}$ und

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}.$$

Zeigen Sie, dass p/q ein Näherungsbruch von x ist.

Aufgabe 3 : Shor-Algorithmus (schriftlich)

a) (1 Punkt) Zeigen Sie, dass $N = 15$ die kleinste Zahl ist, für die der Algorithmus zum Finden eine Periode erforderlich ist (d.h. die kleinste zusammengesetzte, ungerade Zahl die keine Potenz ist).

b) (2 Punkte) Wir wollen jetzt die Zahl 15 explizit mit dem Shor-Algorithmus in Primfaktoren zerlegen. Wir verwenden dazu ein zur Vorlesung leicht abgeändertes Verfahren (siehe Nielsen & Chuang). Dafür muss zuerst eine Zahl a gewält werden, damit a und N relativ prim sind. Wählen Sie $a = 7$ und definieren Sie den unitären Operator $U : |x\rangle \mapsto |ax \mod N\rangle$. Definieren Sie

$$|u_s\rangle \equiv r^{-1/2} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} \left|a^k \mod N\right\rangle .$$

Zeigen Sie, dass $|u_s\rangle$ ein Eigenvektor von U ist und berechnen Sie den Eigenwert.

c) (2 Punkte) Zeigen Sie, dass

$$r^{-1/2} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle .$$

d) (3 Punkte) Jetzt muss die Anzahl Qubits n des zweiten Registers festgestellt werden. Wählen Sie $n = 11$ und erzeugen Sie die Überlagerung

$$|\phi_n\rangle = 2^{-n/2} \sum_{k=0}^{2^n-1} |k\rangle |1\rangle .$$

Definieren Sie $U_{a,N} : |j\rangle |k\rangle \mapsto |j\rangle |a^j k \mod N\rangle$ und zeigen Sie jetzt, dass

$$U_{a,N} |\phi_n\rangle = 2^{-n/2} \sum_{k=0}^{2^n-1} |k\rangle \left|a^k \mod N\right\rangle \approx \frac{1}{\sqrt{r 2^n}} \sum_{s=0}^{r-1} \sum_{k=0}^{2^n-1} e^{2\pi i s k/r} |k\rangle |u_s\rangle .$$

Geben Sie die 5 ersten Terme der Zwischensumme explizit an. Welche Werte sind für das zweite Register möglich?

e) (2 Punkte) Nach Anwendung der Quanten-Fourier-Transformation auf das erste Register (und Messung des zweiten Registers) entsteht (näherungsweise) der Zustand $|0\rangle + |512\rangle + |1024\rangle + |1536\rangle$ (muss hier nicht berechnet werden). Nehmen Sie an, dass eine Messung den Wert 1536 liefert. Bestimmen Sie mit Hilfe von Kettenbruch die Ordnung r von $a \mod N$ aus der Gleichung $s/r = 1536/2048$. Überprüfen Sie ob $r = -1 \mod N$ und berechnen Sie schließlich $\mathrm{GGT}(x^{r/2} \pm 1, N)$.

Welche anderen Ergebnisse der letzten Messung würden es ermöglichen, die richtigen Primfaktoren zu finden?