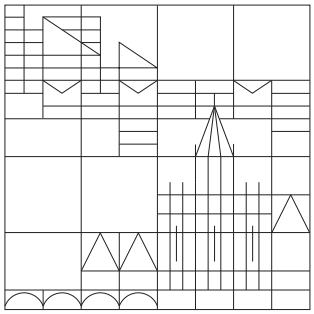
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
Dr. Regina Finsterhoelzl
https://tinyurl.com/QC-S22



**Quantencomputing und Quantensimulation**
**Sommersemster 2022 - Übungsblatt 6**
Ausgabe: 25.05.2022, Abgabe: 06.06.2022, Übungen: 09.06.2022

## Aufgabe 14: Inverse Quanten-Fouriertransformation (3 Punkte)

a) (2 Punkte) Zeigen Sie, dass die inverse Fouriertransformation durch

$$f(x) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i x y/2^n} \hat{f}(y)$$

gegeben ist.

b) (1 Punkt) Die Quanten-Fouriertransformation wird durch die unitäre Abbildung

$$\hat{U}_{\mathrm{QFT}} = \frac{1}{\sqrt{2^n}} \sum_{x,y=0}^{2^n-1} e^{2\pi i x y/2^n} |x\rangle \langle y|$$

beschrieben. Zeigen Sie, dass diese Abbildung unitär ist. Was beschreibt $\hat{U}_{\mathrm{QFT}}^{\dagger}$ demnach?

## Aufgabe 15: Shor-Algorithmus (5 Punkte)

Anhand eines Beispiels zur Faktorisierung der Zahl $N = 21$ soll der Shor-Algorithmus verdeutlicht werden. Nehmen Sie an, dass Sie $t$ Qubits zur Verfügung haben, womit ihr Anfangszustand durch

$$|\psi_1\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |0\rangle$$

gegeben ist.
a) (1 Punkt) Als nächstes wird ein $a$ mit $\mathrm{GGT}(a, N) = 1$ gewählt und der Zustand

$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle \left|a^k \mathrm{mod}\ N\right\rangle$$

erzeugt. Wie viele orthogonale Zustände $\left|a^k \mathrm{mod}\ N\right\rangle$ erhält man im zweiten Register für $a = 5$?

b) (1 Punkt) Nun wird das zweite Register gemessen. Welchen Zustand $|\psi_3\rangle$ erhält man, falls im zweiten Register der Zustand $\left|a^k \mathrm{mod}\ N = 4\right\rangle$ gemessen wird?

c) (2 Punkte) Nach der Messung des zweiten Registers wird eine Fouriertransformation $|\psi_4\rangle = \hat{U}_{\mathrm{QFT}} |\psi_3\rangle$ durchgeführt. Anschließend wird das erste Register gemessen. Berechnen Sie die Wahrscheinlichkeit $p(k) = |\langle k|\psi_4\rangle|^2$ den Zustand $|k\rangle$ zu messen und skizzieren Sie diese für $t = 6$ und für $t = 15$ Qubits.

d) (1 Punkt) Berechnen Sie $\frac{k_1}{2^t}$ für $t = 6$ und $t = 15$ Qubits, wobei $k_1$ die Stelle des ersten Maximums in $p(k)$ mit $k \neq 0$ beschreibt. Vergleichen Sie diesen mit dem Wert $1/r$, wobei $r$ die Periode von $|\psi_3\rangle$ beschreibt.

**Aufgabe 16: Euklidischer Algorithmus und Kettenbrüche (2 Punkte)**

a) (1 Punkt) Bestimmen Sie den größten gemeinsamen Teiler der beiden Zahlen 3486 und 2856 mit Hilfe des Euklidischen Algorithmus.

b) (1 Punkt) Bestimmen Sie den Kettenbruch zu der Zahl $\frac{225}{157}$.

**Aufgabe 17: Periodenfinden als Phasenschätzen (4 Punkte)**

a) (2 Punkte) Zeigen Sie, dass $U_{N,a} : \ |y\rangle \mapsto |ay \bmod N\rangle$ mit GGT$(a, N)$=1 unitär ist.

b) (1 Punkt) Zeigen Sie, dass $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} \left|a^k \bmod N\right\rangle$ ein Eigenvektor von $U_{N,a}$ ist, also $U_{N,a} |u_s\rangle = u_s |u_s\rangle$ mit $u_s = e^{2\pi is/r}$.

c) (1 Punkt) Beweisen Sie

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = \left|a^k \bmod N\right\rangle ,$$

und somit

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