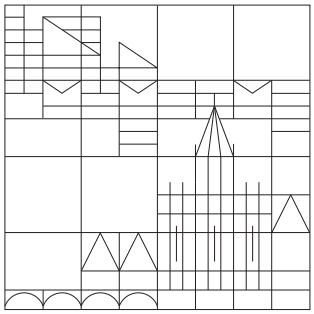
UNIVERSITÄT KONSTANZ
Fachbereich Physik
Prof. Dr. Guido Burkard
M. Kizmann
http://tinyurl.com/QCQS20



Quantencomputing und Quantensimulation
Sommersemster 2020 - Übungsblatt 1
Ausgabe: 05.06.2020, Abgabe: 12.06.2020, Übungen: 16./18.06.2020

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) Beweisen Sie

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

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

c) (1 Punkt) Zeigen Sie, dass

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

Aufgabe 18: Diffie-Hellman-Schlüsselaustausch (3 Punkte)

Der Diffie-Hellman-Schlüsselaustausch beschreibt ein Verfahren mittels dessen zwei Personen (Alice und Bob) einen gemeinsamen Schlüssel über einen unsicheren (abhörbaren) Kanal austauschen könenn, welcher dann zur Verschlüsselung weiterer Nachrichten verwendet werden kann. Zunächst einigen sich Alice und Bob auf eine große Primzahl p und eine weitere, kleine Zahl g, welche über den unsicheren Kanal ausgetauscht werden. Nun wählen sowohl Alice als auch Bob eine zufällige Geheimzahl a und b mit $0 \leq a, b \leq p-1$, welche Sie jeweils für sich behalten. Alice berechnet jetzt $A = g^a \bmod p$ und schickt das Resultat an Bob. Bob berechnet $B = g^b \bmod p$ und schickt das Resultat an Alice. Alice berechnet nun den Schlüssel K durch $K = B^a \bmod p$. Bob erhält den selben Schlüssel durch $K = A^b \bmod p$.
a) (1 Punkt) Berechnen Sie ein Beispiel für $g = 21$ und $p = 101$.

b) (1 Punkt) Zeigen Sie, dass $B^a \bmod p = A^b \bmod p$.

c) (1 Punkt) Der Diffie-Hellman-Schlüsselaustausch gilt als sicher für hinreichend große Primzahlen p. Beschreiben Sie, wie Eve durch abhören des Kanals dennoch den geheimen Schlüssel mithilfe eines Quantencomputers berechnen könnte.

Aufgabe 19: Versteckte Untergruppen (2 Punkte)

Gegeben sei eine Funktion $f : \{0,1\}^3 \mapsto \{0,1\}^2$ mit $f(x_2x_1x_0) = x_2x_0$ ($x_i \in \{0,1\}$). Der Funktionswert ergibt sich also aus dem ersten und letzten Bit der Eingabe.
a) (1 Punkt) Wie lautet die durch f versteckte Untergruppe K? Geben Sie alle Nebenklassen gK dieser Funktion an.

b) (1 Punkt) Durch welchen Quantenalgorithmus lässt sich die versteckte Untergruppe der Funktion f bestimmen?