Theoretische Physik für Quantentechnologien

Prof. Dr. Frank Wilhelm-Mauch
Prof. Dr. Giovanna Morigi

SS 2016 **31.05.2016**
Blatt 3 **Fälligkeitsdatum: 06.06.2016**

***Achtung**: Sie werden aus organisatorischen Gründen Ihre Lösungen immer zu Beginn der jeweiligen Übung abgeben, die zukünftig montags stattfinden werden.*

Aufgabe 1: Gruppentheorie, (*15 Punkte*)

Eine wichtige Grundlage für das Verständnis des RSA Verschlüsselsungsalgorithmus und damit auch des Shor Algorithmus ist die Gruppentheorie. Wir wollen in dieser Aufgabe verschiedene Gruppen und fundamentale Eigenschaften dieser untersuchen. Eine Menge G zusammen mit einer Verknüpfung $G\text{x}G \longmapsto G$, geschrieben als $(x, y) \longmapsto xy$ wird als Gruppe bezeichnet, falls folgende Eigenschaften erfüllt sind:

1. (Identität) $\exists e \in G$, so dass $\forall g \in G : eg = ge = g$.
2. (Assoziativität) $\forall x, y, z \in G : (xy)z = x(yz)$.
3. (Inverses Element) $\forall x \in G$, $\exists y \in G$, so dass $xy = yx = e$.
4. (Geschlossenheit) $\forall x, y \in G : xy \in G$

Wir haben die Gruppe multiplikativ geschrieben, $(x, y) \longmapsto xy$. Wenn wir die Verknüpfung als $(x, y) \longmapsto x + y$ schreiben, bezeichnen wir die Gruppe als additiv. Falls $\forall x, y \in G\ xy = yx$, bezeichnen wir die Gruppe als abelsch.

(a) Zeigen Sie, dass $\mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\}$ eine additive Gruppe ist. (*3 Punkte*)

(b) Betrachten Sie die Gruppe der $N\text{x}N$ Matrizen mit reellen Einträgen und Determinante ungleich null. Beweisen Sie, dass dies eine Gruppe ist und zeigen Sie, dass diese für $N > 1$ nicht kommutativ (abelsch) ist. Bildet diese Menge auch eine Gruppe unter Matrixaddition? (*2 Punkte*)

(c) Eine wichtige Gruppe für das Verständnis des Shor Algorithmus ist die Gruppe $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, ..., p-1\}$, wobei p eine Primzahl ist und $a \cdot b = ab \bmod p$. Zeigen Sie, dass es sich hierbei um eine multiplikative Gruppe handelt. (Für die Existenz des Inversen nutzen Sie den euklidischen Satz) (*2 Punkte*)

(d) Als erzeugendes Element der Gruppe $\mathbb{Z}/p\mathbb{Z}$ wird das Element g bezeichnet, für das gilt $< g >= \{g^i | i = 1, 2, ..., p-1\} = \mathbb{Z}/p\mathbb{Z}$. Die Gruppe $\mathbb{Z}/7\mathbb{Z}$ besitzt zwei Erzeuger. Bestimmen Sie diese und beweisen Sie, dass es sich tatsächlich um Erzeuger handelt. (*3 Punkte*)

(e) Die Ordnung bzw. Periodizität eines Elementes $x \in G$ ist durch die kleinste positive Zahl m gegeben, sodass $x^m = e$. Seine m_1 und m_2 koprim zueinander, das heißt der einzige gemeinsame Teiler der beiden Zahlen ist 1. Zeigen Sie, dass x^{m_1} die Ordnung m_2 besitzt. (x besitzt Ordnung m) (*2 Punkte*)

(f) Wir wollen eine Untergruppe H von G betrachten. Zeigen Sie, dass für alle $g_i, g_j \in G$ entweder $g_i H = g_j H$ oder $g_i H \cap g_j H = \{\}$ (*3 Punkte*)

Aufgabe 2: RSA Algorithmus (*20 Punkte*)

Die Sicherheit des RSA Algorithmus basiert darauf, dass Primfaktorzerlegung einer ausreichend großen Zahl mit klassischen Ressourchen nicht durchführbar ist. Möchte Bob sicherstellen, dass eine von Alice verschlüsselte Nachricht nur von ihm selbst gelesen werden kann, können beide auf die RSA Verschlüsselung zurückgreifen. In Kurzform wird dabei wie folgt vorgegangen:

1. Bob wählt zwei ausreichend große Primzahlen p und q. Diese sollten jeweils mindestens ungefähr 200stellig sein, um Sicherheit zu garantieren.
2. Bob berechnet das Produkt $N = pq$ und $\varphi(N) = (p-1)(q-1)$. Er wählt eine Zahl $c < \varphi(N)$, die groß und teilerfremd von $\varphi(N)$ ist.
3. Bob berechnet das modulare multiplikative Inverse d von c, $d \equiv c^{-1} \pmod{\varphi(N)}$
4. Bob übermittelt den öffentlichen Schlüssel (N, c) an Alice
5. Alice verschlüsselt ihre Nachricht a, indem Sie $b \equiv a^c \pmod{N}$ berechnet und sendet die verschlüsselte Nachricht b öffentlich an Bob
6. Bob, der als einziger Kenntnis über d hat, ist in der Lage die Nachricht von Alice zu entschlüsseln, indem er $b^d \pmod{N}$ berechnet

Wir wollen nun anhand eines einfachen Beispiels den RSA Algorithmus nachvollziehen. Sie dürfen sofern nicht anders angegeben auf Computerunterstützung (z.B. Wolfram Mathematica) zur Berechnung zurückgreifen. Geben Sie einen Ausdruck des verwendeten Codes mit ab.

(a) Bob hat öffentlich $N = 55$ und $c = 17$ als Schlüssel bekanntgegeben. Alice möchte nun die Nachricht $a = 9$ damit verschlüsseln. Wie lautet die verschlüsselte Nachricht b? (*2 Punkte*)

(b) Selbstverständlich können Sie für dieses einfache Beispiel die Primfaktoren p und q angeben. Berechnen Sie den unbekannten Teil d des privaten Schlüssels von Hand, indem Sie den euklidischen Algorithmus verwenden. Verifizieren Sie, dass $b^d = a \pmod{\varphi(N)}$. (*5 Punkte*)

(c) Nehmen Sie nun an, dass Eve einen Quantencomputer zur Verfügung hat, mit dem Sie in der Lage ist, die Periode r von $b \pmod{N}$ zu ermitteln. Wie lautet r? Schreiben Sie alle erforderlichen Teilschritte nieder. (*6 Punkte*)
Hinweis: Selbstverständlich besitzen Sie keinen Quantencomputer, wissen aber dass die Ordnung der zugrundeliegenden Gruppe $(p-1)(q-1)$ ist. Die Periode r muss ein Teiler der Ordnung sein.

(d) Bestimmen Sie $d' \equiv c \pmod{r}$. Bestätigen Sie, dass $b^{d'} \equiv a \pmod{N}$ gilt. (*2 Punkte*)

(e) In Teil d) haben Sie gezeigt, dass die RSA Verschlüsselung geknackt werden kann, sofern die Periode r der verschlüsselten Nachricht b bekannt ist. Um sich davon zu überzeugen, dass r sich nicht einfach ablesen lässt, plotten Sie die Funktion $f(x) = b^x \pmod{N}$ für

   (i) den zuvor betrachteten Fall,

   (ii) $b = 12448$ und $N = 86609$.

   Können Sie etwas über die Periode herausfinden? Variieren Sie dazu auch die minimalen/maximalen Werte von x. (*5 Punkte*)

Aufgabe 3: Experiment - Shor Algorithmus (*10 Punkte*)

Lesen Sie die folgenden Veröffentlichungen zur experimentellen Realisierung des Shor Algorithmus kritisch und beantworten Sie die jeweils zum Artikel gehörenden Fragen:

(a) doi:10.1038/414883a

   (i) Wie wird die Periode r experimentell bestimmt. Was ist hierbei das Hauptproblem? (*2 Punkte*)

(ii) Was ist die Hauptursache für Abweichungen von Experiment und Theorie? (*1 Punkt*)

(b) doi:10.1038/nphys2385

(i) Erklären Sie stichpunktartig, wie Qubits verschränkt werden. (*2 Punkte*)

(ii) Wie hoch ist die Wahrscheinlichkeit, die Zahl $N = 15$ korrekt in ihre Primfaktoren zu zerlegen? (*1 Punkt*)

(c) doi:10.1038/nature12290

(i) Fassen Sie kurz zusammen, was man unter einer kompilierten Version des Shor Algorithmus versteht. (*3 Punkte*)

(ii) Geben Sie die Kernaussage des Artikels in eigenen Worten wider. (*1 Punkt*)

Aufgabe 4: Quantenteleportation von Gattern, (*15 Punkte*)

In dieser Aufgabe wollen wir zeigen, dass nicht nur Zustände sondern auch die Wirkung von Gattern teleportiert werden kann. Wir betrachten dafür folgendes Set von Clifford-Gattern: CNOT, Pauli X,Y,Z, Hadamard, S-Phasen Gatter:

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

Dieses Set von Gattern ist nicht universell. Wenn wir aber zusätzlich noch das T- bzw. $\frac{\pi}{8}$-Gatter

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{i\frac{\pi}{4}} \end{pmatrix}$$

dazunehmen, wird das Set universell. Wir wollen zeigen, wie es möglich ist das T-Gatter zu implementieren, indem man sich die Quantenteleportation von Gattern zunutze macht.

a) Geben Sie die Wirkung der beiden Gattersequenzen die in Abb. 1 dargestellt sind auf die Eingangszustände an, indem Sie den zugehörigen Ausgangszustand hinschreiben. Die beiden Sequenzen werden als 1-Bit Z-Teleportation und 1-Bit X-Teleportation bezeichnet, warum? (*6 Punkte*)

b) Stellen sie sich vor sie wenden das oben angegebene T-Gatter auf das resultierende Qubit der X-Teleportionssequenz an. Zeigen Sie wie wir dieses T-Gatter an den Anfang der Sequenz verlagern können, sodass wir eine Sequenz haben, die ein einzelnes T-Ancilla, nämlich den Zustand $\mathrm{TH}\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \mathrm{e}^{i\frac{\pi}{4}}\right)$, ein $CNOT$-Gatter und ein klassisch kontrolliertes SX-Gatter (S bezeichnet das Phasengatter) benutzt.

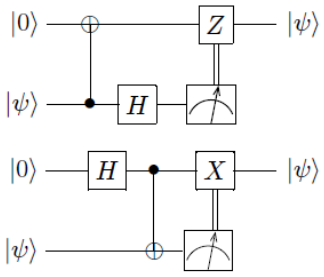

Abbildung 1: *Gattersequenz der 1-Bit Z-Teleportation (oben) und der 1-Bit X-Teleportation (unten). Die abgebildete Messung findet in der Z-Basis statt und bestimmt ob das jeweilige Pauli-Gatter angewandt wird oder nicht, wobei das Gatter angewendet wird wenn $Z = 1$.*

Die resultierende Sequenz sollte einen Eingangszustand $|\Psi\rangle$ in den Ausgangszustand $T|\Psi\rangle$ überführen und daher das T-Gatter implementieren. (*7 Punkte*)

c) Funktioniert dies analog auch für die Z-Teleportation und falls ja, wie sieht die zugehörige Gattersequenz und der Ancilla-Zutand aus? (*2 Punkte*)

Hinweis: Die Motivation für die Konstruktionen in dieser Aufgabe kommt von dem Problem der physikalischen Implementierung, die es einem oftmals nur erlaubt (einen Unterraum an) Cifford-Gatter anzuwenden (z.B. Topologischer Quantencomputer mit Ising Anionen, Surface Code, etc.). Diese Aufgabe zeigt wie es möglich ist universelle Quantenoperationen mit diesen Gattern und zusätzlichen speziellen Ancillas (wie bspw. hier das T-Ancilla) auszuführen. Zudem sind diese Konstruktion extrem wichtig, wenn man Rausch- bzw. Fehlertolerante Gattersequenzen konstruieren will.