

# Faktorisierung auf dem Quantencomputer

## Erklärung und Implementierung

*Einführung in die Funktionsweise von Quantencomputern und Implementation zweier Programmbibliotheken in Q# mit arithmetischen Operationen sowie einer vollständigen Implementierung des Shor-Algorithmus*

Maturaarbeit von   Joël Benjamin Huber  
Betreut von       Christian Steiger  
an der             Kantonsschule Freudenberg Zürich  
abgegeben am     15. Dezember 2020

**Zusammenfassung:** Die vorliegende Maturitätsarbeit beschäftigt sich mit Quantencomputern und ihrer Anwendung für das Faktorisierungsproblem. Zu diesem Zweck wurden arithmetische Operationen genauer betrachtet, um zu verstehen, wie sie auf Quantencomputern implementiert werden können. Danach wurde der Shor-Algorithmus genauer betrachtet, mit welchem sich Zahlen faktorisieren lassen. Dies alles wurde in der Form zweier Programmbibliotheken in der Quantenprogrammiersprache Q# und der klassischen Programmiersprache C# implementiert, sodass man diese Operationen auch in anderen Projekten verwenden kann.





# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>iii</b>
1.1	Vorwort . . . . .	iii
1.2	Die QInteger- und die QAlgorithm-Libraries und eine Implementierung des Faktorisierungsalgorithmus . . . . .	iv
<b>2</b>	<b>Grundlagen</b>	<b>1</b>
2.1	Lineare Algebra . . . . .	1
2.1.1	Schreibweise . . . . .	1
2.1.2	Vektorräume . . . . .	1
2.1.3	Skalarprodukt . . . . .	2
2.1.4	Lineare Operatoren . . . . .	2
2.1.5	Eigenwerte und Eigenvektoren . . . . .	3
2.1.6	Das Tensorprodukt . . . . .	3
2.2	Quantensysteme . . . . .	4
2.2.1	Qubits . . . . .	4
2.2.2	Die Blochkugel . . . . .	6
2.2.3	Operationen auf Qubits . . . . .	6
2.2.4	Wichtige Quantengatter . . . . .	7
2.2.5	Kontrollierte und adjungierte Operatoren . . . . .	8
<b>3</b>	<b>Arithmetische Operationen auf Qubits ausführen - Die QInteger Library</b>	<b>9</b>
3.1	Zahlen in Qubits speichern - Der QInt-Typ . . . . .	9
3.2	Die Quanten-Fouriertransformation und die Fourier-Basis . . . . .	10
3.2.1	Die Quantenfouriertransformation . . . . .	10
3.2.2	Unitarität . . . . .	12
3.2.3	Implementierung . . . . .	12
3.3	Addition . . . . .	13
3.4	Modulare Addition . . . . .	15
3.5	Modulare Multiplikation . . . . .	16
<b>4</b>	<b>Der Weg zum Shor-Algorithmus</b>	<b>17</b>
4.1	Überblick . . . . .	17
4.2	Phase Kickback . . . . .	17
4.3	Phasenabschätzung . . . . .	18
4.4	Periodenabschätzung . . . . .	19
4.5	Die Ordnung von Zahlen bestimmen . . . . .	21
4.6	Das Ziel - Der Shor-Algorithmus . . . . .	22
4.6.1	Der Algorithmus . . . . .	22

4.6.2	Analyse des Algorithmus . . . . .	23
<b>5</b>	<b>Ausblick</b>	<b>25</b>
5.1	Man kann Zahlen effizient faktorisieren - Was nun? . . . . .	25
5.2	Quantencomputer - Wie bald? . . . . .	25
<b>6</b>	<b>Nachwort</b>	<b>27</b>
<b>7</b>	<b>Anhang</b>	<b>28</b>
7.1	Mathematische Symbole . . . . .	28
7.2	Literatur . . . . .	28
7.3	Redlichkeitserklärung . . . . .	30

# Kapitel 1

## Einführung

### 1.1 Vorwort

Das Gebiet der Quantencomputer ist zweifellos eines der vielversprechendsten Forschungsgebiete. Quantencomputer würden uns theoretisch erlauben, Berechnungen auszuführen, die auf klassischen Computern nicht effizient ausgeführt werden können. Diese mathematischen Konstrukte werden in der Zukunft wahrscheinlich eine grössere Rolle spielen.

Immer wieder liest man in Zeitungs- und Journalartikeln über Relisierungen von Quantencomputern und immer wieder wurde von Durchbrüchen gesprochen. So wie zum Beispiel, als Google 2019 einen Artikel im Journal “Nature“ publizierte, in welchem sie behaupteten, die “Quantenüberlegenheit“ erreicht zu haben ([1]), was gleich darauf von der IBM in ihrem Blog angezweifelt wurde ([12]).

Aus diesem Grund ist es meiner Meinung nach ein guter Zeitpunkt, um sich vertieft mit dem Thema auseinanderzusetzen. Ich habe mich deshalb entschieden, mich auf diese Reise zu begeben und im Rahmen meiner Maturitätsarbeit zu versuchen zu verstehen, wie Quantencomputer funktionieren, um danach in einem nächsten Schritt arithmetische Operationen sowie den Shor-Algorithmus zu implementieren. Die grösste Schwierigkeit, mit der ich mich auf meinem Weg konfrontiert sah, war es, die Quantenalgorithmen zu debuggen.

Doch es dauerte immer eine Weile, bis etwas funktionierte. In der Tat denke ich, dass die grösste Schwierigkeit, die ich hatte, war, die Quantenalgorithmen zu debuggen. Mein Code war am Anfang noch sehr fehlerhaft und diese Fehler zu finden war schwierig. Dies liegt auch daran, dass Qubits schwierigere Konstrukte sind, so dass deren momentanen mit deren geplanten Zuständen zu vergleichen und zu finden, wieso etwas nicht stimmt, Stunden in Anspruch nehmen konnte.

In der Tat ist es meiner Meinung nach nicht sehr einfach, in dieses Gebiet einzusteigen. Auch deshalb soll meine Arbeit dazu dienen, zusammen mit der angegebenen Fachliteratur, den Einstieg zu vereinfachen. Dafür werden aber Kenntnisse der linearen Algebra vorausgesetzt, da diese sehr wichtig ist, um die mathematische Struktur zu verstehen. Zum Einstieg in die lineare Algebra habe ich selbst das Buch “Lineare Algebra“ von Gerd Fischer (siehe [6]) gelesen und empfehle dieses Buch, um sich die Grundlagen der linearen Algebra zu erarbeiten.

Ich habe mich sowohl damit auseinandergesetzt, wie arithmetische Operationen auf Quantencomputern programmiert werden können, als auch, wie man damit Zahlen faktorisieren kann. Was ich gelernt habe, habe ich in Code umgesetzt. Ich habe zwei Programmbibliotheken implementiert, die ich in Abschnitt 1.2 genauer beschreibe und in welchen man alle in dieser Arbeit betrachteten Operationen als Code finden kann. Zudem habe ich bei der Implementierung ge-

zielt darauf geachtet, dass diese Bibliotheken auch in späteren Projekten gut verwendet werden können und ich habe vor, diese Bibliotheken in Zukunft kontinuierlich zu erweitern und Implementierungen anderer Quantenalgorithmen hinzuzufügen, so dass sie aktuell bleiben.

## 1.2 Die QInteger- und die QAlgorithm-Libraries und eine Implementierung des Faktorisierungsalgorithmus

Das Produkt dieser Maturitätsarbeit sind zwei Programmbibliotheken, welche Algorithmen für Quantencomputer bereitstellen. Diese Programmbibliotheken sind in der Programmiersprache Q# geschrieben, einer Quantenprogrammiersprache entwickelt von Microsoft. Das Quantum Development Kit (QDK) von Microsoft beinhaltet dabei nicht nur die Sprache Q#, sondern auch einen Simulator, auf welchem man den Code ausführen kann. Gleichzeitig ist es das Ziel der Sprache, dass man sie auf echten Quantencomputern einsetzen kann, sobald diese genug weit entwickelt sein werden.

Die beiden Bibliotheken sollen mathematische Operationen auf Quantencomputern vereinfachen. Hier ein kurzer Überblick über ihre Funktionen:

- Die *QInteger-Library* definiert mit dem Typ “QInt“ die grundlegende Datenstruktur “Zahl“ auf einem Quantencomputer. Zudem stellt sie arithmetische Operationen und nützliche Funktionen für den Typ “QInt“ bereit.
- In der *QAlgorithms-Library* sind Algorithmen für Quantencomputer implementiert, darunter auch der quantenbasierte Teil von Shors Algorithmus zur Faktorisierung von Zahlen, welcher zweifelsohne einer der nennenswertesten Errungenschaften auf dem Gebiets der Quantencomputer ist.

Diese beiden Bibliotheken stellen generelle, nützliche Funktionen für Quantencomputer bereit, welche auch zur Vereinfachung in anderen Projekten gebraucht werden können. Den Code zu diesen Programmbibliotheken kann man auf GitHub finden, wo er in Zukunft einige Aktualisierungen erhalten wird. Auf GitHub ist er unter folgendem Link verfügbar:

<https://github.com/johutha/QInteger-QAlgorithms>

Ich habe Q# gewählt, da es aktuell eine der populärsten Quantenprogrammiersprachen ist, über eine gute Dokumentation verfügt, gut unterstützt und regelmässig aktualisiert wird. Zudem kann der Compiler automatisch zu einer Quantenoperation deren Inverses oder deren kontrollierte Version generieren <sup>1</sup>, was den Code kürzer und übersichtlicher macht.

Nebst diesen beiden Bibliotheken finden sich im GitHub-Repository weitere Projekte. In einem dieser Projekte ist der “Factorizer“ implementiert, welcher zusammen mit den Quanten-Programmbibliotheken eine komplette Implementierung von Shors Algorithmus bilden. Dazu sind im Projekt auch andere Faktorisierungsalgorithmen programmiert, so dass man diese miteinander vergleichen kann.

Im Weiteren befindet sich im Repository ein Projekt für eine einfache Konsolen-Applikation, welche den “Factorizer“ benützt, so dass man diesen als Proof of Concept ausprobieren kann. Zudem gibt es ein Projekt für einen Zeitmesser, welcher misst, wie lange der “Factorizer “ benötigt.

---

<sup>1</sup>Siehe auch Kapitel 2.2

Zudem befinden sich im Repository drei weitere Projekte, in welchen Unit-Tests implementiert sind. Unit-Tests testen die verschiedenen Komponenten einzeln, wodurch man einfacher Implementierungsfehler lokalisieren und Bugs finden kann.



# Kapitel 2

## Grundlagen

### 2.1 Lineare Algebra

Um mit Quantencomputern arbeiten zu können, braucht es Kenntnisse der linearen Algebra. Operationen, die man auf Quantencomputern implementiert, sind lineare Operationen auf Qubits. Ich werde an dieser Stelle eine kurze Zusammenfassung der nötigen Grundlagen geben, welche erforderlich sind, um die Quanten-Grundlagen und Shors Algorithmus zu verstehen. Dies wird jedoch nur eine kurze Zusammenfassung und keine Einführung in dieses Gebiet sein. Für eine Einführung verweise ich auf [6].

Vor der Zusammenfassung möchte ich kurz die in der Quantenmechanik gebräuchliche Notation für lineare Algebra einführen. Diese nennt sich Dirac- oder Bra-Ket-Notation.

#### 2.1.1 Schreibweise

Einen Vektor schreibt man in der Quantenmechanik als  $|\varphi\rangle$ . Diese besondere Art von Klammern wird als *ket* bezeichnet. Für einen Vektor  $|\varphi\rangle$  wird der dazugehörige duale Vektor als  $\langle\phi|$  bezeichnet. Diese zweite Klammer heisst *bra*, sodass die beiden Klammern zusammen ein Bra-Ket bildet, was vom englischen Wort bracket abstammt. Somit lässt sich das Skalarprodukt von  $|\psi\rangle$  und  $|\varphi\rangle$  als  $\langle\psi|\varphi\rangle$  darstellen.

#### 2.1.2 Vektorräume

Um Quantensysteme mathematisch beschreiben zu können, brauchen wir Vektorräume. Genauer benötigen wir endlichdimensionale Vektorräume über  $\mathbb{C}$ , zusammen mit einem Skalarprodukt. Diese Vektorräume werden auch unitäre Vektorräume<sup>1</sup> genannt. Diese sind isomorph zu  $\mathbb{C}^n$ .

Sei  $V$  ein solcher Vektorraum.

Wir nennen eine Menge von Vektoren in  $V$  ein *Erzeugendensystem*, falls jeder Vektor in  $V$  als eine Linearkombination der Vektoren in jener Menge geschrieben werden kann.

Eine Menge von Vektoren  $|v_0\rangle, |v_1\rangle, \dots, |v_{k-1}\rangle$  ist *linear unabhängig*, falls aus der Gleichung  $a_0 |v_0\rangle + a_1 |v_1\rangle + \dots + a_{k-1} |v_{k-1}\rangle = 0$  folgt, dass  $a_0 = a_1 = \dots = a_{k-1} = 0$  gilt. Dabei sind die Koeffizienten  $a_0, a_1, \dots, a_{n-1}$  komplexe Zahlen. Diese Aussage ist äquivalent zur Aussage,

---

<sup>1</sup>Im Allgemeinen braucht es sogenannte Hilberträume. Da man es im Zusammenhang mit Quantencomputern aber nur mit endlichdimensionalen Räumen zu tun hat, reichen unitäre Vektorräume

dass sich keiner der Vektoren  $|v_i\rangle$  als Linearkombination der anderen Vektoren in der Menge darstellen lässt.

Eine *Basis* ist ein linear unabhängiges Erzeugendensystem.

### 2.1.3 Skalarprodukt

Die für die Beschreibung der Qubits benötigten unitären Vektorräumen sind mit einem Skalarprodukt ausgerüstet: Das heisst, es gibt eine Funktion  $(\cdot, \cdot) : V \times V \rightarrow \mathbb{C}$  mit folgenden Eigenschaften:

1. Linear im zweiten Argument:

$$\sum_j \lambda_j (|\psi\rangle, |\varphi_j\rangle) = (|\psi\rangle, \sum_j \lambda_j |\varphi_j\rangle)$$

2. Hermitesch:

$$(|\psi\rangle, |\varphi\rangle) = \overline{(|\varphi\rangle, |\psi\rangle)}$$

3. Positiv definit:

$$\varphi \neq 0 \Rightarrow (|\varphi\rangle, |\varphi\rangle) > 0$$

Wie oben schon angetönt, schreibt man dieses Produkt in der quantenmechanischen Notation als  $\langle\psi|\varphi\rangle$ . Ich habe für diese drei Bedingungen jedoch die  $(\cdot, \cdot)$ -Schreibweise verwendet, da man mit ihr die Bedingungen übersichtlicher darstellen kann.

Wir benutzen hier das Standardskalarprodukt in  $\mathbb{C}^n$  definiert als:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} := \sum_{i=1}^n \overline{c_i} w_i$$

Es ist nicht schwierig zu sehen, dass das auf diese Weise definierte Skalarprodukt die oben genannten Bedingungen erfüllt.

Die *Norm* eines Vektors  $|\varphi\rangle$ , wird als  $\| |\varphi\rangle \|$  geschrieben und ist definiert als  $\| |\varphi\rangle \| = \sqrt{\langle\varphi|\varphi\rangle}$ . Ein Vektor  $|\varphi\rangle$  ist normiert, falls  $\| |\varphi\rangle \| = 1$  gilt.

### 2.1.4 Lineare Operatoren

Sei  $V$  ein endlichdimensionaler, unitärer Vektorraum<sup>2</sup>, seien  $|v\rangle$  und  $|w\rangle \in V$  und  $\lambda \in \mathbb{C}$ .

**Definition:** Ein *linearer Operator*<sup>3</sup>  $L$  ist eine Funktion

$$\begin{array}{ccc} L: & V & \longrightarrow V \\ & v & \longmapsto Lv \end{array}$$

welcher die Bedingung der Linearität  $L(\sum_i \lambda_i |v_i\rangle) = \sum_i \lambda_i L(|v_i\rangle)$  erfüllt. Für eine Matrix

<sup>2</sup>Die Definitionen dieses Abschnittes würden auch für allgemeinere Vektorräume funktionieren. Das ist aber für diese Arbeit nicht nötig.

<sup>3</sup>In dieser Arbeit wird der Begriff *linearer Operator* synonym zum Begriff *lineare Abbildung* benutzt

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \quad \text{mit Einträgen } a_{ij} \in \mathbb{C} \text{ schreiben wir kurz } A = (a_{ij}) \text{ und definieren } \dots$$

die *konjugierte* Matrix von  $A$ :  $\bar{A} := (\bar{a}_{ij})$

die *transponierte* Matrix von  $A$ :  $A^T := (a_{ji})$

die *adjungierte* Matrix von  $A$ :  $A^\dagger := \bar{A}^T$

**Definition:** Ein *unitärer Operator*  $U$  ist ein linearer Operator, welcher folgende Bedingung erfüllt:

$$U^\dagger U = I$$

. Aufgrund dieser Bedingungen erhalten unitäre Operationen das Skalarprodukt der Vektoren:

$$(U|u\rangle, U|v\rangle) = \langle u|U^\dagger U|v\rangle = \langle u|v\rangle$$

Insbesondere verändert sich auch das Skalarprodukt eines Vektors mit sich selbst nicht, weshalb auch die Norm eines Vektors unter unitären Operatoren erhalten bleibt.

Zustände eines Quantensystems können als Vektoren eines unitären Vektorraumes  $V$  beschrieben werden. Zustandsänderungen werden durch unitäre Operationen beschrieben.

### 2.1.5 Eigenwerte und Eigenvektoren

Ein Eigenvektor  $|\varphi\rangle$  zu einem linearen Operator  $U$  ist ein Vektor, sodass  $U|\varphi\rangle = \lambda|\varphi\rangle$  gilt, wobei  $\lambda$  als der dazugehörige Eigenwert bezeichnet wird und eine komplexe Zahl ist. Bei einem unitären Operator müssen alle Eigenwerte einen Betrag von 1 haben, denn sonst würde sich die Norm des Vektors verändern. Der grosse Vorteil von Eigenvektoren ist, dass sie sich bis auf einen skalaren Faktor nicht verändern, wenn der dazugehörige Operator auf sie angewendet wird.

### 2.1.6 Das Tensorprodukt

Das Tensorprodukt, geschrieben mit dem Zeichen  $\otimes$ , gibt uns die Möglichkeit alle mögliche Kombinationen der Einträge ihrer Operanden zu generieren. Sei  $A := (a_{ij})$  eine  $n_a \times m_a$  Matrix und  $B := (b_{ij})$  eine  $n_b \times m_b$  Matrix. Die daraus resultierende Matrix  $A \otimes B = C := (c_{ij})$  ist eine  $n_a n_b \times m_a m_b$  Matrix, die wie folgt generiert wird:

$$\begin{aligned}
C = A \otimes B &= \begin{bmatrix} a_{11} & \cdots & a_{1m_a} \\ \vdots & \ddots & \vdots \\ a_{n_a 1} & \cdots & a_{n_a m_a} \end{bmatrix} \otimes \begin{bmatrix} b_{11} & \cdots & b_{1m_b} \\ \vdots & \ddots & \vdots \\ b_{n_b 1} & \cdots & b_{n_b m_b} \end{bmatrix} \\
&= \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & \cdots & b_{1m_b} \\ \vdots & \ddots & \vdots \\ b_{n_b 1} & \cdots & b_{n_b m_b} \end{bmatrix} & \cdots & a_{1m_a} \begin{bmatrix} b_{11} & \cdots & b_{1m_b} \\ \vdots & \ddots & \vdots \\ b_{n_b 1} & \cdots & b_{n_b m_b} \end{bmatrix} \\ \vdots & \ddots & \vdots \\ a_{n_a 1} \begin{bmatrix} b_{11} & \cdots & b_{1m_b} \\ \vdots & \ddots & \vdots \\ b_{n_b 1} & \cdots & b_{n_b m_b} \end{bmatrix} & \cdots & a_{n_a m_a} \begin{bmatrix} b_{11} & \cdots & b_{1m_b} \\ \vdots & \ddots & \vdots \\ b_{n_b 1} & \cdots & b_{n_b m_b} \end{bmatrix} \end{bmatrix} \\
&= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1m_b} & a_{12}b_{11} & \cdots & a_{1m_a}b_{1m_b} \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{11}b_{2m_b} & a_{12}b_{21} & \cdots & a_{1m_a}b_{2m_b} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{11}b_{n_b 1} & a_{11}b_{n_b 2} & \cdots & a_{11}b_{n_b m_b} & a_{12}b_{n_b 1} & \cdots & a_{1m_a}b_{n_b m_b} \\ a_{21}b_{11} & a_{21}b_{12} & \cdots & a_{21}b_{1m_b} & a_{22}b_{11} & \cdots & a_{2m_a}b_{1m_b} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n_a 1}b_{n_b 1} & a_{n_a 1}b_{n_b 2} & \cdots & a_{n_a 1}b_{n_b m_b} & a_{n_a 2}b_{n_b 1} & \cdots & a_{n_a m_a}b_{n_b m_b} \end{bmatrix}
\end{aligned}$$

Zusätzlich ist die Schreibweise  $X^{\otimes n}$  eine verkürzte Schreibweise für die  $n$ -malige Anwendung des Tensorprodukts auf sich selbst. In anderen Worten,  $X^{\otimes n} = \bigotimes_{k=0}^{n-1} X$ .

## 2.2 Quantensysteme

Die Quantensysteme, die wir im Rahmen dieser Arbeit betrachten, sind rein mathematische Systeme, die nicht an eine fixe physikalische Realisierung gebunden sind. In der Tat gibt es verschiedene Möglichkeiten, solche Systeme physikalisch umzusetzen, wobei jede Variante eigene Vor- und Nachteile hat.

### 2.2.1 Qubits

Ein klassisches Bit hat genau zwei Zustände - 0 und 1 - und ist immer in genau einem dieser beiden Zustände. Kann man zwei solche Zustände in einem quantenmechanischen System gezielt herbeizuführen, treten auch die Gesetze der Quantenphysik in Kraft. Ein Beispiel einer physikalischen Realisierung, das bei der Vorstellung helfen kann, wäre ein Atom in einem Grundzustand und einem angeregten Zustand, wobei der Grundzustand einem klassischen 0 und der angeregte Zustand einem klassischen 1 entsprechen könnte. Gemäss den Gesetzen der Quantenphysik kann sich das Atom aber auch in einer Überlagerung der beiden Zustände befinden. Dies nennt man eine Superposition. Von diesem Beispiel aus können wir uns nun die genaue Definition eines Qubits betrachten:

**Definition:** Ein *Qubit* ist ein Quantensystem mit den beiden Basiszuständen  $|0\rangle$  und  $|1\rangle$ . Es kann alle Zustände  $\alpha|0\rangle + \beta|1\rangle$  annehmen, sodass  $|\alpha|^2 + |\beta|^2 = 1$  gilt.

Ein Zustand des Qubits, welcher durch die Parameter  $\alpha$  und  $\beta$  definiert ist, entspricht einem normierten Vektor im Vektorraum  $\mathbb{C}^2$ .<sup>4</sup>

Wenn wir zu unserem Beispiel von vorhin zurückgehen, dann würde der Zustand  $|0\rangle$  dem Grundzustand und der Zustand  $|1\rangle$  dem angeregten Zustand entsprechen.

Qubits können wir messen<sup>5</sup>. Betrachten wir ein Qubit im Zustand  $\alpha|0\rangle + \beta|1\rangle$ , so beträgt die Wahrscheinlichkeit, dass wir  $|0\rangle$  messen,  $|\alpha|^2$ , und die Wahrscheinlichkeit,  $|1\rangle$  zu messen, beträgt  $|\beta|^2$ . Die Bedingung, dass  $|\alpha|^2 + |\beta|^2 = 1$  gelten muss (dass der Vektor normiert sein muss), führt dazu, dass sich die Wahrscheinlichkeiten auf 1 summieren. Nach der Messung kollabiert das Quantensystem in den gemessenen Zustand. Messen wir also  $|1\rangle$ , befindet sich das Qubit nachher immer im Zustand  $|1\rangle$ , unabhängig davon, was  $\alpha$  und  $\beta$  vorher waren.

Ähnlich entspricht der Zustand eines Multiqubitsystems mit  $n$  Qubits einen normierten Vektor im Vektorraum  $\mathbb{C}^{2^n}$ . Die Basiszustände des Vektorraums entsprechen dabei den einzelnen Kombinationen der  $|0\rangle$ s und  $|1\rangle$ s der einzelnen Qubits. Zum Beispiel hat der Vektorraum zu einem Quantensystem mit 2 Qubits die vier Basiszustände  $|00\rangle, |01\rangle, |10\rangle$  und  $|11\rangle$ . Der Bitstring von Länge  $n$  innerhalb dem Ket, entspricht dabei der Konfiguration der Qubits. Der Zustand  $|101\rangle$  in einem System mit 3 Qubits entspricht dem Zustand, in welchem das erste Qubit im Zustand  $|1\rangle$ , das zweite im Zustand  $|0\rangle$  und das dritte im Zustand  $|1\rangle$  ist. Anstelle des Bitstrings wird innerhalb des Kets auch oft eine Zahl verwendet, welche in der Binärdarstellung diesen Bitstring ergibt. Zum Beispiel entspricht  $|5\rangle$  dem Zustand  $|101\rangle$ .

Ein Zustand ist nun ein normierter Vektor im Vektorraum  $\mathbb{C}^{2^n}$ . Der Koeffizient des Basiszustands  $|j\rangle$  eines Vektors in diesem Vektorraum entspricht dabei der Wahrscheinlichkeit, den Zustand  $j$  zu messen. Auch summieren sich die Wahrscheinlichkeiten wieder auf 1, da der Vektor normiert ist. Man schreibt man die Zustände oft als eine Linearkombination der Basiszustände:  $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle$ .

Um den Zustand des Multiqubitsystems beschreiben zu können, wenn wir im Besitz der Zustände der einzelnen Qubits sind, können wir die Vektoren der Zustände der einzelnen Qubits mit Hilfe des Tensorprodukts zusammenmultiplizieren. Zudem kann man mit dem Tensorprodukt auch Operationen zusammenmultiplizieren: Wenn wir  $n$  Qubits haben und auf jedes Qubit eine Operation anwenden (dies kann auch die Identität sein, falls wir das Qubit unverändert lassen wollen) und dann die Matrizen dieser Operationen multiplizieren, bekommen wir die Matrix, die der Operation entspricht, die alle unsere ausgewählten Operationen ausführt. Wichtig ist aber noch anzumerken, dass das Tensorprodukt nicht kommutativ ist, und die Reihenfolge der Faktoren somit wichtig ist.

Falls wir nur einzelne Qubits messen, kollabiert das System in die restlichen, noch möglichen Zustände. Nehmen wir als Beispiel ein 2-Qubit-System im Zustand  $\frac{1}{\sqrt{6}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{3}}|11\rangle$  und messen das erste Qubit. Die Wahrscheinlichkeit, dass wir dieses Qubit im Zustand  $|1\rangle$  messen,

<sup>4</sup>Dass sich der Zustand eines quantenmechanisches System als Vektor beschreiben lässt, garantiert uns das erste Postulat der Quantenmechanik. Da diese Postulate den Rahmen dieser Arbeit übersteigt, verweise ich für eine genauere Betrachtung dieser Postulate auf [11], Kapitel 2.2

<sup>5</sup>Auch die Messungen basieren auf einem Postulat der Quantenmechanik, nämlich auf dem dritten Postulat.

liegt bei  $|\alpha_{10}|^2 + |\alpha_{11}|^2 = \frac{1}{3}$ . Falls wir diesen Zustand messen, kollabiert unser Quantensystem sofort in den Zustand  $\frac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}} = |11\rangle$ , wobei der Nenner dafür sorgt, dass der neue Quantenzustand wieder normiert ist. Die Wahrscheinlichkeit eines  $|0\rangle$  in der Messung des ersten Qubit hingegen liegt bei  $|\alpha_{00}|^2 + |\alpha_{01}|^2 = \frac{2}{3}$ . Der Zustand des Systems nach der Messung ist dann  $\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} = \sqrt{\frac{1}{4}}|00\rangle + \sqrt{\frac{3}{4}}|01\rangle$ .

### 2.2.2 Die Blochkugel

Die Blochkugel dient der graphischen Darstellung des Zustands eines einzelnen Qubits. Zu diesem Zweck betrachten wir noch einmal ein einzelnes Qubit  $\alpha|0\rangle + \beta|1\rangle$  mit  $|\alpha|^2 + |\beta|^2 = 1$ . Diese Bedingung führt dazu, dass wir den Zustand als  $e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$  umschreiben können. Den Faktor  $e^{i\gamma}$  können wir nicht beobachten, da er auf beide Koeffizienten wirkt<sup>6</sup>. Deshalb ist der Zustand durch die beiden Winkel  $\theta$  und  $\varphi$  definiert. Diese beiden Winkel kann man graphisch als einen Punkt auf einer Einheitskugel darstellen. Diese Darstellung wird die Bloch-Kugel genannt.

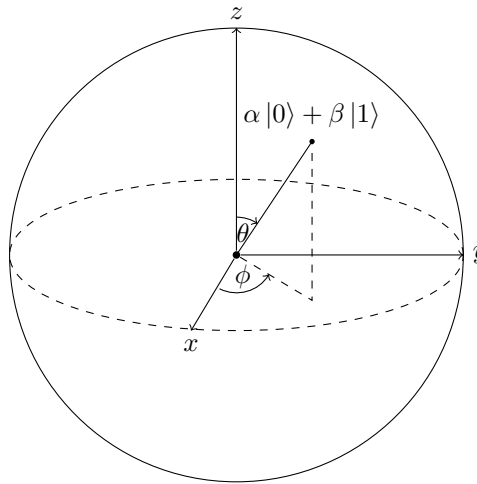


Abbildung 2.1: Beispiel einer Blochkugel

### 2.2.3 Operationen auf Qubits

Operationen, die man auf Qubits implementiert, sind lineare Operationen und lassen sich somit als Matrizen darstellen. Man kann den Vektor, welcher den Zustand beschreibt, mit der Matrix des Operators multiplizieren, um den Zustand nach der Operation zu erhalten. Dazu müssen die Operatoren die Norm des Quantenzustands bewahren, da die Zustände immer normiert sein müssen, und somit unitär sein. Dies hat die direkte Konsequenz (für eine unitäre Matrix  $U$  gilt  $UU^\dagger = I$ ), dass ein inverser Operator existieren muss und deshalb alle Berechnungen reversibel sein müssen. Beispielsweise kann der Modulo Operator nicht auf Quantencomputern implementiert werden, da man aus dem Ergebnis  $x \equiv 2 \pmod{3}$  die Eingabe  $x \in \{2, 5, 8, \dots\}$  nicht eindeutig wiederherstellen kann. Dies hat grosse Konsequenzen für die Berechnungen auf Quantencomputern.

<sup>6</sup>Dies nennt man eine globale Phase: Dieser Faktor hat Betrag 1 und verändert deshalb die Wahrscheinlichkeiten nicht. Da er sich zudem auf alle Zustände auswirkt, kann man ihn bei den Quantenoperatoren wegen der Linearität ausklammern. Somit bleibt er immer über alle Qubits bestehen.

Gleichzeitig stellt sich heraus, dass es verschiedene universelle Kombinationen von Operationen gibt, wobei universell in diesem Zusammenhang bedeutet, dass man jeden unitären Operator nur mit den ausgewählten Operatoren beliebig annähern kann. Die Konstruktion dazu kann man in [11], Seiten 188ff. nachlesen.

## 2.2.4 Wichtige Quantengatter

An dieser Stelle werden die wichtigsten Quantengatter eingeführt, die wir benötigen werden. Zuerst betrachten wir fünf grundlegende Gatter auf Qubits: die drei Pauli-Matrizen  $X, Y$  und  $Z$ , das  $H$ -Gatter und das  $CNOT$ -Gatter.

- Das  $X$ -Gatter ist das Qubit-Equivalent zum  $NOT$ -Gatter eines elektronischen Schaltkreises. In Matrixform sieht der Operator so aus:  $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ . Dieses Gatter dreht den Zustand des Qubits um  $\pi$  um die  $x$ -Achse in der Blochkugel.
- Das  $Y$ -Gatter wird durch die Matrix  $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$  dargestellt. Dieses Gatter entspricht einer Rotation von  $\pi$  um die  $y$ -Achse in der Blochkugel.
- Das  $Z$ -Gatter, als Matrix  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ , dreht den Zustand um  $\pi$  um die  $z$ -Achse.
- Das Hadamard-Gatter, meistens einfach durch den Buchstaben  $H$  abgekürzt, ist der einfachste Weg, eine Superposition zu erzeugen. Mit der Matrix  $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  kann man die beiden Zustände  $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  und  $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  erzeugen. Diese beiden Zustände kommen so häufig vor, dass man ihnen die Namen  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  und  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  gegeben hat.
- $CNOT$  steht als Abkürzung für "Controlled NOT". Dieses Gatter wirkt auf zwei Qubits und wendet ein  $NOT$  auf das zweite Qubit an, wenn das erste Qubit auf 1 ist. Als Matrix sieht die Operation so aus:

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

Diese Gatter gehören zu den wichtigsten Gattern im Bereich der Quantencomputer. Wir werden auf unserem Weg jedoch weitere Gatter antreffen. Eines, von welchem wir noch mehr Gebrauch machen werden, möchte ich hier kurz definieren. Ich nenne es  $\text{Rot}(k)$  und in Matrix-Form sieht es so aus:  $\text{Rot}(k) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{bmatrix}$ . Dieses Gatter multipliziert den Koeffizienten von  $|1\rangle$  mit  $e^{\frac{2i\pi}{2^k}}$

und wir werden es bei der Quanten-Fouriertransformation<sup>7</sup> und dessen Anwendungen antreffen.

Abschliessend möchte ich noch ein Gatter auf zwei Qubits erwähnen, bekannt als das SWAP-Gatter. Dieses Gatter vertauscht die Zustände der beiden Qubits, indem es die Amplituden in

---

<sup>7</sup>Siehe Kapitel 3

derjenigen Zustände vertauscht, in welchen die beiden Qubits nicht gleich sind. Es wird durch die folgende Matrix beschrieben:

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

Wenn wir das erste Qubit als  $a$  und das zweite als  $b$  bezeichnen, sehen wir auf der rechten Seite, dass wir das  $SWAP(a, b)$  als Abfolge dreier  $CNOT$ -Gates ( $CNOT(a, b)$ , dann  $CNOT(b, a)$  und dann  $CNOT(a, b)$ ) programmieren können.

### 2.2.5 Kontrollierte und adjungierte Operatoren

Wie wir bereits erfahren haben, müssen die Operatoren, welche man auf Quantencomputern umsetzen kann, unitär und somit reversibel sein. Dies setzt sofort die Existenz eines adjungierten Operatoren (auch inversen Operator genannt) zu einem Operator  $U$  voraus, welcher aus einem Zustand  $|\varphi\rangle$  den Zustand  $|\psi\rangle$  mit  $U|\varphi\rangle = |\psi\rangle$  macht. Ein Schaltkreis zu diesem adjungiertem Operator lässt generieren, indem man die Gatter des Schaltkreises für  $U$  rückwärts durchgeht, und immer den adjungierten Operator des jeweiligen Gatters nimmt. Viele Quantenprogrammiersprachen können deshalb auch die adjungierte Version eines Quantenoperators aus dem Programmcode des ursprünglichen Operators generieren.

Auch lassen sich kontrollierte Versionen eines Operators bilden. Die kontrollierte Version eines Operators nimmt zusätzlich zu den Qubits, auf welche die Operation ausgeführt werden soll, noch eine Menge an sogenannten Kontrollqubits. Diese Version der Operation wird nur auf denjenigen Zuständen ausgeführt, in welchen alle Kontrollqubits im Zustand  $|1\rangle$  sind. Als Beispiel nehmen wir eine Operation, welche die Bitrepräsentation zyklisch um ein Bit nach rechts verschiebt (also aus dem Zustand  $|01101\rangle$  den Zustand  $|10110\rangle$  macht). Haben wir nun den Zustand  $|0\rangle|11101\rangle + |1\rangle|10110\rangle + |0\rangle|01000\rangle$  haben (das erste Bit habe ich hier getrennt dargestellt, da es für diese Operation als Kontrollqubit verwenden will). Wenn wir nun die Operation mit dem ersten Bit als Kontrollqubit anwenden, so bekommen wir den Zustand  $|0\rangle|11101\rangle + |1\rangle|01011\rangle + |0\rangle|01000\rangle$ . Sei  $U$  ein Operator, welcher auf Quantencomputern programmierbar ist. Dann schreiben wir die durch das Qubit  $c$  kontrollierte Version von  $U$  als  $U^c$ . In den Fällen, in denen wir mit  $U^k$  die  $k$  mal wiederholte Anwendung des Operators  $U$  meinen, werde ich darauf hinweisen.

Ein Qubit darf aber nie gleichzeitig ein Kontrollqubit und eines jener Qubits, auf dem der Operator angewendet wird, sein. Um dies zu sehen betrachten wir das  $CNOT$ , welches die kontrollierte Variante des  $X$ -Operators ist. Wenn wir den Operator auf ein Qubit mit demselben Qubit als Kontrollqubit anwenden, so wird dieses Qubit nach der Anwendung immer im Zustand  $|0\rangle$  sein. Somit ist dieser Operator nicht mehr reversibel. Wenn diese Bedingung aber eingehalten wird, so ist dieser Operator reversibel, da man aus den Kontrollqubits, welche während der Operation nicht verändert werden, ablesen kann, ob die Operation durchgeführt wurde.

Auch diese Version wird von den meisten Quantenprogrammiersprachen automatisch generiert, da man den Schaltkreis der kontrollierten Version einfach herstellen kann, indem man vom Schaltkreis des ursprünglichen Operators bei jedem Gatter die kontrollierte Version nimmt.

Zudem lassen sich die beiden oben genannten Varianten auch kombinieren, um eine kontrollierte, adjungierte Version eines Operators zu generieren.



## Kapitel 3

# Arithmetische Operationen auf Qubits ausführen - Die QInteger Library

### 3.1 Zahlen in Qubits speichern - Der QInt-Typ

Da ich davon ausgehe, dass in absehbarer Zeit die Anzahl Qubits zwar wachsen, allerdings jedoch nicht so schnell ansteigen wird, dass man schon bald mehrere grössere Qubit-Einheiten speichern kann, habe ich mich entschieden, in meiner Implementation auf eine einheitliche Grösse zu verzichten und für den Moment eine variable Anzahl von Qubits für eine Zahl zu benutzen. Deshalb besteht der QInt-Typ aus einer klassischen Zahl, der Anzahl Qubits, und einem Array von Qubits, welcher die eigentliche Zahl, welche in den Qubits gespeichert werden soll, speichert.

```
// Definition of the QInt type with variable size. QInts
// are represented in little-endian.
newtype QInt = (Size : Int , Number : Qubit []);
```

Dies ist die Definition des Typs QInt in meinem Code: Wir definieren den neuen Typ “QInt” als eine Kombination einer Zahl, genannt *Size*, und einem Array von Qubits, genannt *Number*.

Im weiteren Verlauf dieser Arbeit werde ich Zahlen, die auf eine klassische Art und Weise gespeichert sind und somit keine Superpositionen erlauben, als eine “klassische Zahl” bezeichnen und Zahlen, welche in Qubitregistern gespeichert werden, als “Quantenzahlen” oder “QInts” bezeichnen.

## 3.2 Die Quanten-Fouriertransformation und die Fourier-Basis

### 3.2.1 Die Quantenfouriertransformation

Sei  $|x\rangle$  ein Element einer Orthonormalbasis. Damit können wir die QFT wie folgt definieren:

$$QFT |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{xj}{2^n}} |j\rangle$$

Für diesen Zustand gibt es eine Faktorisierung. Diese werde ich kurz zeigen und darauf auch beweisen.

$$\left(|0\rangle + e^{2i\pi \frac{x}{2^1}} |1\rangle\right) \otimes \left(|0\rangle + e^{2i\pi \frac{x}{2^2}} |1\rangle\right) \otimes \dots \otimes \left(|0\rangle + e^{2i\pi \frac{x}{2^n}} |1\rangle\right) = \bigotimes_{j=0}^{n-1} \left(|0\rangle + e^{2i\pi \frac{x}{2^{1+j}}} |1\rangle\right)$$

Diese Faktorisierung werde ich nun kurz beweisen. Sei die Darstellung von  $j \in \{0, 1, \dots, 2^n - 1\}$  im Binärsystem:

$$j = 2^{n-1} \cdot j_{n-1} + \dots + 2^1 \cdot j_1 + 2^0 \cdot j_0 = \sum_{s=0}^{n-1} 2^s j_s$$

Dann können wir folgende Umformung durchführen:

$$\begin{aligned} \bigotimes_{s=0}^{n-1} \left(|0\rangle + e^{2i\pi \frac{x}{2^{1+s}}} |1\rangle\right) &= \bigotimes_{s=0}^{n-1} \left(e^{2i\pi \frac{0 \cdot x}{2^{1+s}}} |0\rangle + e^{2i\pi \frac{1 \cdot x}{2^{1+s}}} |1\rangle\right) \\ &= \sum_{(j_{n-1}, \dots, j_0) \in \{0,1\}^n} \bigotimes_{s=0}^{n-1} e^{2i\pi \frac{x \cdot j_{n-1-s}}{2^{1+s}}} = \sum_{(j_{n-1}, \dots, j_0) \in \{0,1\}^n} \left(\prod_{s=0}^{n-1} e^{2i\pi \frac{x \cdot j_{n-1-s}}{2^{1+s}}}\right) |j_{n-1} j_{n-2} \dots j_0\rangle \\ &= \sum_{j=0}^{2^n-1} \left(\prod_{s=0}^{n-1} e^{2i\pi \frac{x \cdot j_{n-1-s}}{2^{1+s}}}\right) |j\rangle = \sum_{j=0}^{2^n-1} \left(e^{2i\pi \frac{x \sum_{s=0}^{n-1} j_{n-1-s} \cdot 2^{n-1-s}}{2^n}}\right) |j\rangle = \sum_{j=0}^{2^n-1} e^{2i\pi \frac{xj}{2^n}} |j\rangle \end{aligned}$$

Schauen wir uns nun die Produktionsdarstellung der Fouriertransformation von  $|x\rangle$  genauer an. Dazu benutzen wir die folgende Notation, um  $x$  im Binärsystem darzustellen:

$$x = 2^{n-1} \cdot x_{n-1} + \dots + 2^1 \cdot x_1 + 2^0 \cdot x_0 =: (x_{n-1} \dots x_1 x_0) \quad \text{für } x_s \in 0, 1$$

und für  $k \in \mathbb{N}, k < n$  schreiben wir:

$$\frac{x}{2^k} =: (x_{n-1} \dots x_k \cdot x_{k-1} \dots x_1 x_0) \quad \text{und} \quad \frac{x}{2^n} =: (0.x_{n-1} \dots x_1 x_0)$$

Diese Schreibweise ist das Äquivalent zu den Dezimalzahlen mit Nachkommastellen im binären Zahlensystem.

Mit dieser Notation erhält man:

$$\begin{aligned}
& \left(|0\rangle + e^{2i\pi \frac{x}{2^1}}\right) \otimes \left(|0\rangle + e^{2i\pi \frac{x}{2^2}}\right) \otimes \dots \otimes \left(|0\rangle + e^{2i\pi \frac{x}{2^{n-1}}}\right) \otimes \left(|0\rangle + e^{2i\pi \frac{x}{2^n}}\right) \\
&= \left(|0\rangle + e^{2i\pi \frac{(x_{n-1} \dots x_0)}{2^1}}\right) \otimes \left(|0\rangle + e^{2i\pi \frac{(x_{n-1} \dots x_0)}{2^2}}\right) \otimes \dots \otimes \left(|0\rangle + e^{2i\pi \frac{(x_{n-1} \dots x_0)}{2^n}}\right) \\
&= \left(|0\rangle + e^{2i\pi \cdot (x_{n-1} \dots x_1 + 0 \cdot x_0)}\right) \otimes \left(|0\rangle + e^{2i\pi \cdot (x_{n-1} \dots x_2 + 0 \cdot x_1 x_0)}\right) \otimes \dots \\
&\quad \dots \otimes \left(|0\rangle + e^{2i\pi \cdot (x_{n-1} + 0 \cdot x_{n-2} \dots x_0)}\right) \otimes \left(|0\rangle + e^{2i\pi \cdot (0 \cdot x_{n-1} \dots x_0)}\right) \\
&= \left(|0\rangle + e^{2i\pi \cdot (0 \cdot x_0)}\right) \otimes \left(|0\rangle + e^{2i\pi \cdot (0 \cdot x_1 x_0)}\right) \otimes \dots \\
&\quad \dots \otimes \left(|0\rangle + e^{2i\pi \cdot (0 \cdot x_{n-2} \dots x_0)}\right) \otimes \left(|0\rangle + e^{2i\pi \cdot (0 \cdot x_{n-1} \dots x_0)}\right)
\end{aligned}$$

Wobei wir im letzten Abschnitt benutzt haben, dass für  $z \in \mathbb{Z}$  und  $\alpha \in \mathbb{R}$  gilt:

$$e^{2i\pi \cdot (z+\alpha)} = \underbrace{e^{2i\pi z}}_1 \cdot e^{2i\pi \alpha} = e^{2i\pi \alpha}$$

Unter der Darstellung der Zahl  $x \in \mathbb{N}_0$  in der *binären Basis* verstehen wir die Darstellung von  $x$  im Binärsystem, also  $x = 2^{n-1} \cdot x_{n-1} + \dots + 2^1 \cdot x_1 + 2^0 \cdot x_0$ , beziehungsweise die Darstellung durch den Zustand  $|x_{n-1} \dots x_0\rangle$ .

Unter der Darstellung  $x$  in der *Fourierbasis* verstehen wir die Produktionsdarstellung der Fouriertransformierten von  $|x\rangle$ , also

$$\frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2i\pi(0 \cdot x_0)}\right) \otimes \left(|0\rangle + e^{2i\pi(0 \cdot x_1 x_0)}\right) \otimes \dots \otimes \left(|0\rangle + e^{2i\pi(0 \cdot x_{n-1} \dots x_0)}\right)$$

Die im obigen Produkt vorkommenden Zustände nennen wir in diesem Zusammenhang die *Fourierbasis*<sup>1</sup>. Hier soll noch darauf hingewiesen werden, dass die Qubits aber von rechts nach links im Array gespeichert sind (da in der binären Basis das rechteste Qubit das mit dem Wert  $2^0 \cdot x_0$  ist).

Dass wir die Darstellung einer Zahl in der Fourierbasis als Tensorprodukt der einzelnen Qubits schreiben können, bedeutet, dass diese Qubits unabhängig voneinander, also nicht verschränkt sind. Dies bedeutet für uns, dass wenn wir mit einer Zahl in der Fourierbasis rechnen wollen, so können wir die Qubits einzeln bearbeiten. Zudem sehen wir, wenn wir den Zustand eines einzelnen Qubits betrachten,  $\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2i\pi \frac{x}{2(1+s)}}\right)$  betrachten, dass dieser Zustand einem Zeiger in der Blochkugel entspricht, welcher in der XY-Ebene liegt und dort um  $2\pi \frac{x}{2s+1}$  um den Mittelpunkt gedreht ist.

---

<sup>1</sup>Man beachte, dass die Fourierbasis keine Vektorraumbasis im Sinne von Kapitel 2.1.2 ist.

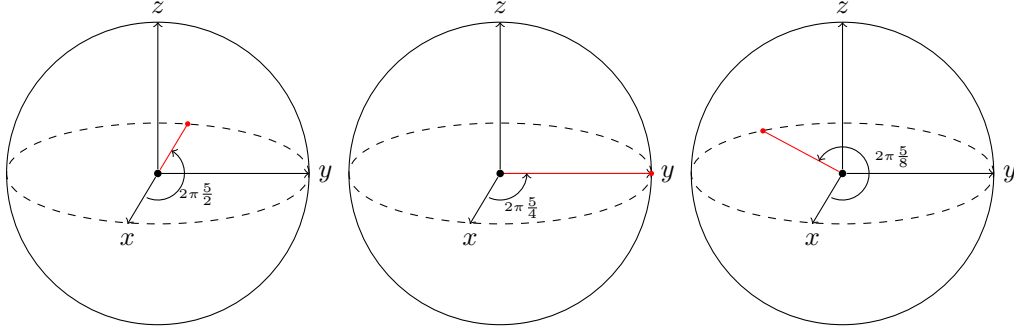


Abbildung 3.1: Die Darstellung der Zahl 5 in der Fourierbasis

Hier können wir feststellen, dass wenn wir die Zahl in der Fourierbasis verändern wollen, müssen wir nur die Qubits im richtigen Winkel drehen, was der Multiplikation des Koeffizienten von  $|1\rangle$  mit  $e^{i\pi\theta}$  entspricht. Zudem können wir feststellen, dass wenn wir den Koeffizienten von  $|1\rangle$  eines Qubits der Fourierbasis mit  $e^{2i\pi\theta}$  multiplizieren, dann können wir den Winkel  $\theta$  mit Hilfe der inversen  $QFT$  auslesen. Dies werden wir im Kapitel 4.3 benötigen.

### 3.2.2 Unitarität

Wir haben allerdings noch nicht gezeigt, dass die oben beschriebene Operation unitär ist. Dafür schauen wir uns die Matrix an, die die Operation der  $QFT$  darstellt. Dafür sei  $\omega_N^j = e^{2i\pi \frac{j}{N}}$ . Dann können wir die  $QFT$  wie folgt darstellen  $QFT := (\omega_{2^n}^{ij})$ . Nun können wir die Bedingung  $QFT^\dagger QFT = I$  überprüfen. Dazu berechnen wir den Eintrag  $ij$  von  $QFT^\dagger QFT$ :

$$\sum_{k=0}^{2^n-1} \frac{\overline{\omega_{2^n}^{ik}}}{\sqrt{2^n}} \cdot \frac{\omega_{2^n}^{kj}}{\sqrt{2^n}} = \frac{1}{2^n} \sum_{k=0}^{2^n-1} \omega_{2^n}^{-ik} \cdot \omega_{2^n}^{kj} = \frac{1}{2^n} \sum_{k=0}^{2^n-1} \omega_{2^n}^{k(j-i)}$$

Nun stellen wir fest, dass falls  $i = j$  gilt, dass dann  $\omega_{2^n}^{k \cdot 0} = 1$  gilt und somit  $\frac{1}{2^n} \sum_{k=0}^{2^n-1} \omega_{2^n}^{k \cdot 0} = 1$  gilt. Gleichzeitig, falls  $i \neq j$  gilt, dann gilt  $\frac{1}{2^n} \sum_{k=0}^{2^n-1} \omega_{2^n}^{k(j-i)} = \frac{1}{2^n} \cdot \frac{w_{2^n}^{(j-i)2^n} - 1}{w_{2^n}^{(j-i)} - 1}$  (da  $\omega_{2^n}^{0(j-i)}, \dots, \omega_{2^n}^{(2^n-1)(j-i)}$  eine geometrische Reihe ist). Gleichzeitig gilt  $w_{2^n}^{(j-i)2^n} = 1$ , und somit  $\frac{1}{2^n} \cdot \frac{w_{2^n}^{(j-i)2^n} - 1}{w_{2^n}^{(j-i)} - 1} = 0$ , da  $\omega_{2^n}^{(j-i)} \neq 1$  gilt.

Nun sehen wir, dass in der resultierenden Matrix der Eintrag  $ij$  dann 1 ist, wenn  $i = j$  gilt, und sonst 0. Dies ist aber genau die Definition von  $I$ . Daraus folgt, dass die  $QFT$  eine unitäre Operation ist, und somit auf Quantencomputern implementierbar ist.

### 3.2.3 Implementierung

Gehen wir zurück zur Produktdarstellung der Fouriertransformierten von  $|x\rangle$ . Diese lässt sich folgendermassen mit Quantengattern realisieren:

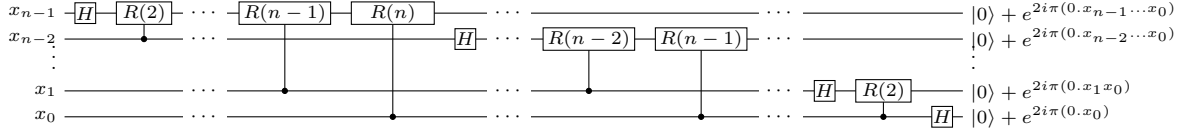


Abbildung 3.2: Schaltkreis der QFT

In dieser Grafik habe ich aus Platzgründen den Namen  $R(k)$  für das  $Rot(k)$ -Gatter verwendet. Um die Funktionsweise dieses Schaltkreises zu sehen, bemerken wir, dass  $H|x_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_j)}|1\rangle)$  gilt, da  $e^{2i\pi \cdot 0} = 1$  und  $e^{2i\pi \cdot \frac{1}{2}} = -1$  gilt. Nun wenden wir  $Rot(2)^{x_{j-1}}$  an. Wir bekommen:

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_j)}|1\rangle) \xrightarrow{Rot(2)^{x_{j-1}}} \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(\frac{x_j}{2} + 2i\pi\frac{x_{j-1}}{4})}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_jx_{j-1})}|1\rangle)$$

Dies können wir fortsetzen:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_jx_{j-1})}|1\rangle) &\xrightarrow{Rot(3)^{x_{j-2}}} \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(\frac{x_j}{2} + \frac{x_{j-1}}{4} + \frac{x_{j-2}}{8})}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_jx_{j-1}x_{j-2})}|1\rangle) \\ \dots & \\ \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_jx_{j-1}\dots x_{j-k+1})}|1\rangle) &\xrightarrow{Rot(1+k)^{x_{j-k}}} \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi(0.x_jx_{j-1}x_{j-2}\dots x_{j-k+1}x_{j-k})}|1\rangle) \end{aligned}$$

So können wir mit Hilfe der  $Rot(k)$ -Gatter die Nachkommastellen der Binärzahl eine Stelle nach der anderen aufbauen. Zum Schluss müssen wir noch die Reihenfolge der Qubits umkehren, was mit  $SWAP$ -Gattern erreicht werden kann.

Wenn wir uns den Schaltkreis anschauen, stellen wir fest, dass wir  $O(n^2)$  Gatter benötigen, um diese Operation zu implementieren, wobei  $n$  die Anzahl Qubits des Registers ist. Dabei werden auch keine zusätzlichen temporäre Qubits benötigt.

### 3.3 Addition

Die wohl grundlegendste arithmetische Operation ist die Addition. Die Subtraktion kann als Addition ausgedrückt werden und auch die Multiplikation (und somit die Division) ist abhängig von der Addition. Deshalb ist sie die erste arithmetische Operation, die wir betrachten.

Wir wollen die Operation implementieren, welche zwei QInts mit Quantenregistern der Größe  $n$  in den Zuständen  $|x\rangle$  und  $|y\rangle$  nimmt und den Zustand des zweiten QInt zu  $|x+y\rangle$  umwandelt. Die Implementation anderer Additionsmethoden (Addition einer klassischen Zahl zu einem QInt, Addition zweier QInts in ein drittes QInt) funktioniert analog. Zusätzlich kann man feststellen, dass die Subtraktion nichts anderes als die inverse Operation zur Addition ist, somit hat man zur Addition die Subtraktion mit-implementiert.

Für die Addition gibt es zwei verschiedene Techniken, die oft benutzt werden. Die eine erreicht eine Gatterzahl von  $O(n)$ , benötigt aber  $O(n)$  zusätzliche Qubits, während die andere ohne zusätzliche Qubits auskommt, dafür aber  $O(n^2)$  Gatteroperationen benötigt. Ich habe mich entschieden, die zweite Version in meiner QInteger-Library zu implementieren. Gründe dafür sind, dass in heutigen Systemen die Anzahl verfügbarer Qubits stark begrenzt ist und in Simulationen

einzelne Qubits sehr viel zusätzliche Leistung benötigen, während eine Laufzeit von  $\mathcal{O}(n^2)$  in diesem Fall weniger ausmacht. Sobald mehr Qubits zur Verfügung stehen, wird es lohnenswerter, auf die andere Version zu wechseln, denn da die Addition eine Operation auf einem sehr tiefen Level ist, kann die Zeit, welche sie benötigt, beträchtliche Auswirkungen auf die gesamte Laufzeit eines komplexeren Algorithmus haben.

Schauen wir uns nun den in der QInteger-Library verwendeten Additionsalgorithmus an. Der Algorithmus basiert auf der Fourierbasis (und somit auf der Faktorisierung der Fouriertransformation). Bei der Addition in der binären Basis sind die einzelnen Bits voneinander abhängig. Deshalb werden sogenannte Carry-Bits verwendet, welche für jedes Bit abspeichern, ob wir beim nächsten Bit noch eine zusätzliche 1 addieren müssen. Dies ist bei der Fourierbasis nicht der Fall: Die Bits sind voneinander unabhängig. Das heisst, wir können die einzelnen Bits voneinander unabhängig modifizieren, ohne dabei auf die anderen Bits achten zu müssen. Dies ist der grosse Vorteil der Fourier-Basis, welcher uns erlaubt, auf zusätzliche Qubits zu verzichten. Betrachten wir nun noch einmal die Faktorisierung: Das  $j$ -te Qubit der Zahl  $y$  in der Fourierbasis ist im Zustand  $\frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{y}{2^{1+j}}} |1\rangle)$ . Wir wollen es aber in den Zustand  $\frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{x+y}{2^{1+j}}} |1\rangle)$  bringen, denn wenn wir alle Qubits in den entsprechenden Zustand bringen könnten, könnten wir mit der inversen  $QFT$  den Zustand  $|x+y\rangle$  wiederherstellen. Nehmen wir wieder das aus der Fouriertransformation bereits bekannte Gatter  $Rot(k) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{bmatrix}$ . Mit dem Gatter können wir den Wert  $2i\pi \frac{1}{2^k}$  zum Exponenten des Koeffizienten von  $|1\rangle$  addieren. Das heisst, wenn wir das Gatter auf ein Qubit im Zustand  $\frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{y}{2^{1+j}}} |1\rangle)$  anwenden, wird es in den Zustand  $\frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{y+2^{n-j-k}}{2^{n-j}}} |1\rangle)$  versetzt. Wir können also mit Hilfe dieses Gatters Zweierpotenzen zum Qubit in der Fourierbasis addieren. Wenn wir das Qubit im Zustand  $|x\rangle$  in der binären Basis belassen, können wir die Addition wie folgt mit  $\mathcal{O}(n^2)$  Gatteroperationen implementieren:

1. Wende  $QFT$  auf den zweiten Summanden im Zustand  $|y\rangle$  an. Das Register befindet sich nun im Zustand  $\frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \left( |0\rangle + e^{2i\pi \frac{y}{2^{1+j}}} |1\rangle \right)$ .
2. Für jedes  $j = 0, \dots, n-1$ , wende für jedes Bit  $x_k$  mit  $k \leq j$  ein kontrolliertes  $Rot(j+1-k)$  auf das Qubit im  $y$ -Register im Zustand  $\frac{1}{\sqrt{2}} \left( |0\rangle + e^{2i\pi \frac{y}{2^{1+j}}} |1\rangle \right)$  an. Dieses befindet sich danach im Zustand:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{y}{2^{1+j}}} |1\rangle) \cdot e^{2i\pi \sum_{s=0}^j \frac{x_{j-s} \cdot 2^{j-s}}{2^{1+s} \cdot 2^{j-s}}} |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{y + \sum_{s=0}^j x_{j-s} \cdot 2^{j-s}}{2^{1+j}}} |1\rangle) \\ & = \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{y+x}{2^{1+j}}} |1\rangle) \end{aligned}$$

Wobei uns alle Bits mit Indizes grösser als  $j$  nicht interessieren, wie man analog zu den Überlegungen aus dem Kapitel 3.2.1 feststellen kann.

3. Die Qubits im zweiten Register befinden sich nun in folgendem Zustand:  $\frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \left( |0\rangle + e^{2i\pi \frac{x+y}{2^{1+j}}} |1\rangle \right)$ . Mit der inversen  $QFT$  kann man aus diesem Zustand den Zustand  $|x+y\rangle$  wiederherstellen.

### 3.4 Modulare Addition

Den uns bekannten Modulo-Operator kann man auf Qubits nicht implementieren, da er nicht invertierbar ist ( $a$  und  $a + m$  haben dasselbe Resultat Modulo  $m$ ). Die modulare Addition ist jedoch invertierbar, wenn beide Summanden kleiner als  $m$  sind. Wir haben wieder zwei QInts in den Zuständen  $|x\rangle$  und  $|y\rangle$  und eine klassische Zahl  $m$  und möchten den Zustand des zweiten QInts auf  $|x + y \pmod{m}\rangle$  setzen. Hier lässt sich das Modulo  $m$  durch einen QInt ersetzen (oder den ersten Summanden durch eine klassische Zahl). Für den Shor-Algorithmus benötigen wir die Operation nur mit einem klassischen Modulo  $m$ , die Implementationen für QInt-Modulos folgen analog und sind auch in der QInt-Library enthalten.

Zuerst addieren wir  $|x\rangle$  zum Register  $|y\rangle$ , um das Register in den Zustand  $|x + y\rangle$  zu versetzen. Nun überprüfen wir, ob diese Summe grösser oder gleich dem Modulo  $m$  ist.

Wie überprüfen wir, ob ein QInt  $x$  grösser oder gleich einer anderen Zahl  $y$  ist? Hier unterscheiden sich die Implementationen für den Fall, wenn die andere Zahl auch ein QInt oder eine klassische Zahl ist, die zugrunde liegende Idee ist jedoch bei beiden Implementationen die gleiche. In der QInteger-Bibliothek ist die Funktion *GreaterOrEqual* als  $\neg$ *LessThan* implementiert. Das heisst, wir probieren herauszufinden, ob  $x < y$  gilt, und negieren dann das Resultat. Wir können dies wie folgt umformen:  $x < y \Leftrightarrow x - y < 0$ . Subtrahieren wir also nun  $y$  von  $x$  müssen wir nun herausfinden, ob das Resultat negativ ist. Ist  $x - y$  nun tatsächlich negativ, passiert ein sogenannter *Underflow*. Dies bedeutet, dass  $x - y$  zu  $2^n + (x - y)$  wird, weil das nächstgrössere Bit fehlt. Um zu sehen, dass dieses von klassischen Bits bekannten Phänomen auf auch Qubits auftritt, beobachten wir, was passiert, wenn wir  $a$  und  $b$  auf Qubits addieren, mit  $a + b \geq 2^n$ . Der Zustand in der Addition vor der inversen *QFT* ist:

$$\bigotimes_{s=0}^{n-1} \left( |0\rangle + e^{2i\pi \frac{a+b}{2^{(1+s)}}} |1\rangle \right) = \bigotimes_{s=0}^{n-1} \left( |0\rangle + e^{2i\pi \left( \frac{a+b}{2^{(1+s)}} - 1 \right)} |1\rangle \right) = \bigotimes_{s=0}^{n-1} \left( |0\rangle + e^{2i\pi \frac{a+b-2^n}{2^{(1+s)}}} |1\rangle \right)$$

Die Resultate  $a + b$  und  $a + b - 2^n$  sind somit nicht unterscheidbar. Da aber nach der inversen *QFT* kein Bit vorhanden ist, um das Bit mit dem Wert  $2^n$  zu speichern, wird das Resultat dieser Addition zu  $a + b - 2^n$ . Gleichzeitig ist die Subtraktion dazu die inverse Operation. Dies bedeutet, wenn wir  $b$  von  $a + b - 2^n$  subtrahieren, gilt  $a - 2^n < 0$ , das Resultat wird aber zu  $a$ . Dies bedeutet, dass wenn das Resultat einer Subtraktion  $x - y$  kleiner als 0 ist, wird es zu  $2^n + (x - y)$ . Dies bedeutet, wir können messen, ob  $x - y < 0$  gilt, indem wir uns einfach das vorderste Qubit anschauen. Ist dieses 1, dann gab es möglicherweise einen Underflow. Um sicherzugehen, dass das vorderste Bit nur dann 1 ist, und nicht wenn  $x - y \geq 2^{n-1}$  gilt, verlängere ich in meiner Implementation noch die Länge der beiden Register um 1.

Nun können wir schauen, ob  $x + y \geq m$  gilt, und diese Information in einem zusätzlichen Qubit speichern. Falls  $x + y \geq m$  gilt, subtrahieren wir  $m$  von der Zahl und haben somit die Zahl  $x + y - m$  im zweiten QInt. Nun ist die Information, ob  $x + y \geq m$  gilt, noch in einem Qubit gespeichert, welches wir zurücksetzen müssen. Dazu behaupte ich, dass  $x + y \geq m$  genau dann gilt, wenn das Resultat grösser oder gleich dem Summanden  $x$  ist.

Die Richtung  $res < x \rightarrow x + y \geq m$  ist nicht schwierig. Für die andere Richtung sehen wir, dass  $x + y - m \geq x$  genau dann gelten kann, falls  $y \geq m$  gilt, was aber nach der Annahme  $x, y < m$  nicht stimmen kann. Somit können wir mit diesem Vergleich die Information in unserem Aushilfsqubit wieder löschen.

### 3.5 Modulare Multiplikation

Mit Hilfe der modularen Addition können wir nun die modulare Multiplikation implementieren. Zuerst stellen wir fest, dass wir die modulare Multiplikation  $|x\rangle \rightarrow |(ax) \pmod{m}\rangle$  nur dann implementieren können, wenn  $\text{ggT}(a, m) = 1$  gilt, ansonsten wäre sie nicht invertierbar (zum Beispiel ist  $2 \cdot 3 \equiv 2 \equiv 2 \cdot 1 \pmod{4}$ ). Gilt aber  $\text{ggT}(a, m) = 1$ , so lässt sich ein inverses  $a^{-1}$  zu  $a$  modulo  $m$  finden, so dass  $a \cdot a^{-1} \equiv 1 \pmod{m}$  gilt. Somit lässt sich die Operation durch die Multiplikation mit  $a^{-1}$  invertieren.

Wir schauen uns die modulare Multiplikation auf QInts in zwei Schritten an. Zuerst implementieren wir die Quantenoperation auf zwei Registern, welche für gegebenes  $a$  und  $m$  folgende Operation bewirkt:

$$U'_{a,m} |x\rangle |y\rangle = |x\rangle |(y + ax) \pmod{m}\rangle$$

Wir sehen, dass wenn wir  $x = 2^0 x_0 + 2^1 x_1 \dots$  in seine Zweierpotenzen aufteilen, dann können wir  $ax \pmod{m} = x_0(2^0 a \pmod{m}) + x_1(2^1 a \pmod{m}) + \dots$  schreiben. Dieses  $+ x_0(\dots)$  ist nichts anders als Addition, kontrolliert durch das  $x_0$  Qubit. Dies heisst, wir können diese Operation relativ einfach durchführen:

Für jedes  $j$ , führe eine modulare Addition, kontrolliert durch das Qubit  $x_j$ , auf das Ausgaberegister mit dem Summanden  $2^j a \pmod{m}$  durch, den wir klassisch berechnen können.

Diese Unteroperation ruft den modularen Addierer  $\mathcal{O}(n)$  mal auf und jede dieser Additionen braucht  $\mathcal{O}(n^2)$  Gatteroperationen. Damit kommen wir auf  $\mathcal{O}(n^3)$  Gatteroperationen.

Mit Hilfe dieser Unteroperation können wir nun die Operation, welche

$$U_{a,m} |x\rangle = |(ax) \pmod{m}\rangle$$

bewirkt, implementieren:

1. Führe ein temporäres Register im Zustand  $|0\rangle$  ein und bringe es mit Hilfe der oberen Unteroperation in den Zustand  $|ax \pmod{m}\rangle$ .
2. Berechne klassisch das Inverse von  $a$  Modulo  $m$ . Dieses lässt sich effizient mit Hilfe des erweiterten euklidischen Algorithmus berechnen. Das Inverse existiert, da  $a$  und  $m$  teilerfremd sind.
3. Die inverse Operation zur oben definierten Unteroperation  $U'_{a,m}$  ist

$$[U'_{a,m}]^{-1} |u\rangle |v\rangle = |u\rangle |v - av \pmod{m}\rangle$$

. Wende diese Operation mit  $a^{-1}$  mit dem temporären Register als erstem Register und dem Register im Zustand  $|x\rangle$  als zweitem Register an. Dies ergibt den Zustand:

$$[U'_{a^{-1},m}]^{-1} |ax \pmod{m}\rangle |x\rangle = |ax \pmod{m}\rangle |x - a^{-1}(ax) \pmod{m}\rangle = |ax \pmod{m}\rangle |0\rangle$$

4. Wechsle den Zustand der beiden Register mit Hilfe der Swap-Operation, sodass  $|ax \pmod{m}\rangle$  in unserem Register und das temporäre Register wieder im Zustand  $|0\rangle$  ist. Das temporäre Register im Zustand kann wieder freigegeben werden und das erste Register befindet sich nun im Zustand  $|ax \pmod{m}\rangle$ .

Diese Multiplikation benötigt  $n$  extra Qubits für das temporäre Register. Sie ruft die Unteroperation 2  $\in \mathcal{O}(1)$  mal auf und benötigt somit  $\mathcal{O}(n^3)$  Gatteroperationen. Wir erinnern uns, dass man die Addition mit  $\mathcal{O}(n)$  Gatteroperationen und dafür  $n$  zusätzlichen Qubits implementieren könnte, was dazu führt, dass wir nur noch  $\mathcal{O}(n^2)$  Gatteroperationen, dafür aber  $2n$  extra Qubits benötigen würden.



## Kapitel 4

# Der Weg zum Shor-Algorithmus

### 4.1 Überblick

In diesem Kapitel werden wir uns die notwendigen Konzepte und Ideen hinter dem quantenbasierten Teil des Shor-Algorithmus anschauen. Dabei beginnen wir beim simplen Konzept des “Phase Kickback“, schauen uns dann die darauf basierende Phasenabschätzung an, bevor wir mit deren Hilfe die Ordnung einer Zahl finden. Zum Schluss werden wir uns den kompletten quantenbasierten Teil des Algorithmus zusammenfassend anschauen.

### 4.2 Phase Kickback

Beginnen wir den Abschnitt mit einer Frage: Wenn wir eine kontrollierte Operation ausführen, sollte sich das Control-Qubit eigentlich nicht ändern, oder? In diesem Abschnitt werden wir sehen, dass dies überraschenderweise doch so sein kann. Dafür schauen wir uns das CNOT-Gatter an. Was geschieht, wenn wir CNOT auf zwei Qubits im Zustand  $|+-\rangle$  anwenden<sup>1</sup>, mit dem ersten Qubit als Control-Qubit? Zuerst haben wir  $|+-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$ . Nachdem wir das CNOT anwenden, bekommen wir den Zustand  $\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = |--\rangle$ . Überraschenderweise stellen wir fest, dass sich das Control-Qubit verändert hat, während das Ziel-Qubit gleich blieb. Was ist passiert? Betrachten wir das CNOT-Gatter genauer: Das CNOT-Gatter ist nichts anderes als eine kontrollierte Version des  $X$ -Gatters. Was geschieht, wenn wir das  $X$ -Gatter auf den  $|-\rangle$ -Zustand anwenden?  $X|-\rangle = -|0\rangle + |1\rangle = -|-\rangle = (-1) * |-\rangle$ . Hier können wir sehen, dass  $|-\rangle$  ein Eigenvektor des  $X$ -Gatters mit Eigenwert  $-1$  ist. Der Zustand ändert sich somit bis auf einen globalen Faktor nicht, den wir - wie in 2.2.2 erklärt wurde - nicht durch eine Messung unterscheiden können.

Wenn wir hingegen die Operation kontrolliert durchführen, wird diese Phase nur in den Zuständen sichtbar, in welchen die Operation durchgeführt wurde, sprich in den Zuständen, in denen das Control-Qubit im Zustand  $|1\rangle$  ist. Dies konnten wir zuvor beim CNOT-Gatter beobachten. Betrachten wir nun eine allgemeinere Operation  $U$  mit einem Eigenvektor  $|\psi\rangle$  und dem Eigenwert  $\lambda$ . Nehmen wir jetzt ein Kontrollqubit im Zustand  $\alpha|0\rangle + \beta|1\rangle$ , ein Qubit-Register im Zustand  $|\psi\rangle$  und wenden  $U$  auf das Register  $|\psi\rangle$  an, kontrolliert durch jenes Kontrollqubit:

$$(\alpha|0\rangle + \beta|1\rangle)|\psi\rangle \xrightarrow{U^c} \alpha|0\rangle + \beta|1\rangle * U|\psi\rangle = (\alpha|0\rangle + \lambda\beta|1\rangle)|\psi\rangle$$

---

<sup>1</sup> $|+\rangle$  und  $|-\rangle$  sind im Kapitel 2.2.4 definiert.

Das Ziel-Qubit verändert sich nicht, es ist ja ein Eigenvektor, stattdessen sehen wir, dass der Eigenwert zurück in die Phase des Kontrollqubit “gekickt“ wird, daher der Name “Phase Kickback“. Im nächsten Abschnitt werden wir diesen Effekt anwenden, um den Eigenwert eines Operators abzuschätzen.

### 4.3 Phasenabschätzung

Verschiedene Quanten-Algorithmen basieren darauf, den Eigenwert eines Operators zu einem Eigenvektor abzuschätzen. Dazu benutzen wir Phase-Kickbacks, um den Eigenwert in ein Zählerregister in der Fourier-Basis zu schreiben, welches wir dann mit der inversen Quantenfouriertransformation in die binäre Basis zurückrechnen. Dazu können wir die Anzahl Qubits variieren, um die Präzision der Approximation festlegen. Genauer gibt der Algorithmus zum Eigenwert  $\lambda = e^{2i\pi\theta}$  die Zahl  $2^n\theta$  zurück, wobei  $n$  die Anzahl Qubits des Zählerregisters ist, die für bessere Präzision erhöht werden kann.

Um zu verstehen, wie dieser Algorithmus funktioniert, erinnern wir uns zuerst daran, wie eine Zahl in der Fourierbasis aussieht. Dafür benutzen wir die Bloch-Kugel. Wir erinnern uns, dass für die Zahl  $x$  in der Fourierbasis mit  $n$  Qubits das  $k$ -te Qubit (hier muss man wieder aufpassen, denn wenn man die Faktorisierung anschaut, ist das  $k$ -te Qubit das  $k$ -te Qubit von rechts) um  $\frac{2^k x}{2^n}$  um die Z-Achse gedreht wird. Das heisst, es befindet sich im Zustand  $\frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{2^k x}{2^n}} |1\rangle)$ . Wir machen jetzt die Beobachtung, dass wir mit Hilfe von Phase-Kickback das gesuchte  $\theta$  in der Fourierbasis in die Kontrollqubits schreiben können, da der Phase-Kickback nichts anderes macht, als das Kontrollqubit auf die selbe Art und Weise zu rotieren. Schauen wir uns einmal an, was passiert, wenn wir  $2^k$  mal kontrolliert den Operator  $U$  anwenden (wobei hier  $(U^c)^{2^k}$  für die kontrollierte Version von  $U$   $2^k$  mal angewendet bedeutet):

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) |\psi\rangle &\xrightarrow{(U^c)^{2^k}} \frac{1}{\sqrt{2}}(|0\rangle |\psi\rangle + |1\rangle \otimes U^{2^k} |\psi\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + (e^{2i\pi\theta})^{2^k} |1\rangle) |\psi\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi 2^k \theta} |1\rangle) |\psi\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{2i\pi \frac{2^k (2^n \theta)}{2^n}} |1\rangle) |\psi\rangle \end{aligned}$$

Dies entspricht genau dem  $k$ -ten Qubit der Repräsentation von  $2^n\theta$  in der Fourierbasis. Das heisst, wenn wir also ein Zählerregister im Zustand  $|0\rangle$  nehmen und dann für  $k = 0, \dots, n-1$  zuerst das  $H$ -Gatter auf das  $k$ -te Qubit und dann  $2^k$  mal ein kontrolliertes  $U$  mit dem  $k$ -ten Qubit als Kontrollqubit auf den Eigenwert anwenden, erhalten wir das  $k$ -te Qubit der Darstellung von  $2^n\theta$  in der Fourierbasis. Wenden wir anschliessend die inverse Fouriertransformation an, können wir die Zahl  $2^n\theta$  im Zählerregister ablesen. Falls  $2^n\theta$  keine ganze Zahl ist, erhalten wir im Zählerregister eine Superposition, wobei eine Zahl wahrscheinlicher ist, je näher sie beim echten Eigenwert liegt.

Um die Phase abzuschätzen, müssen wir also den Operator  $U$  mehrmals hintereinander anwenden, zuerst nur einmal, dann zweimal, im  $i$ -ten Mal  $2^i$  mal. Dies führt dazu, dass wir die Operation  $2^n$  mal anwenden müssen. Allerdings ist es oft möglich, dass wir die Operation  $U^{2^m}$

für einen beliebigen Parameter  $m$  implementieren können. Wenn dies möglich ist, brauchen wir nur  $n$  Anwendungen jener Operation.

### Algorithmus

1. Initialisiere zwei Quantenregister, das Zählerregister und das Eigenvektor-Register, und setze das Eigenvektor-Register auf den gewünschten Eigenvektor  $|\psi\rangle$ .
2. Wende  $H^{\otimes n}$  auf das Zähler-Register an, um es auf  $|+\rangle^{\otimes n}$  zu setzen.
3. Für  $k = 0, \dots, n-1$ : Wende auf den Eigenvektor  $|\varphi\rangle$  die Operation  $(U^{c_k})^{2^k}$ , also die zur  $2^k$ -fachen Anwendung von  $U$  äquivalente Operation kontrolliert durch das Qubit  $c_k$ , an.
4. Wende die inverse Quantenfouriertransformation auf das Zählerregister an, um die Approximation in die binäre Basis umzurechnen.
5. Miss das Zählerregister, um die Abschätzung abzulesen.

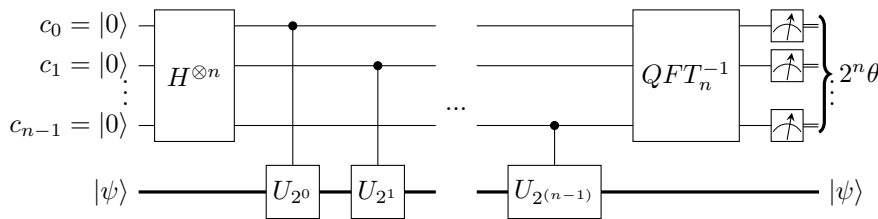


Abbildung 4.1: Schaltkreis der Phasenabschätzung

## 4.4 Periodenabschätzung

Gegeben sei eine Funktion  $f : S \rightarrow S$  über eine endlichen Menge  $S \subset \mathbb{Z}$ , welche sich auf einem Quantencomputer implementieren lässt, und ein Wert  $x \in S$ . Wir versuchen nun, die kleinste Zahl  $r \in \mathbb{N}$  zu berechnen, sodass  $f^r(x) = x$  gilt.

Da die auf Quantencomputern berechneten Operationen unitär sind, müssen die Funktionswerte von  $f$  mit invertierbaren Operation berechnet werden. Deshalb muss  $f$  injektiv sein. Aus diesem Grund müssen  $|S|$  verschiedene Funktionswerte von  $f$  existieren, woraus die Surjektivität folgt. Somit ist  $f$  bijektiv und man kann  $f$  als Permutation der Elemente von  $S$  interpretieren. Diese Permutation kann man als Komposition disjunkter Zykeln darstellen<sup>2</sup>. Seien nun  $\sigma_0, \dots, \sigma_{k-1}$  diese verschiedenen Zykeln. Dazu sei  $S_i$  die Menge der Zahlen  $j \in S$ , so dass  $\sigma_i(j) \neq j$  gilt.

Sei nun  $x \in S_i$ . Da  $\sigma_i$  einen Zykel bildet, gilt  $f^{|S_i|}(x) = x$ . Gleichzeitig kann kein  $r \in \mathbb{N}$  mit  $r < |S_i|$  existieren, sodass  $f^r(x) = x$  gilt, denn sonst hätte unser Zykel nur  $r < |S_i|$  Elemente. Wir wollen nun also für ein  $x \in S_i$  die Grösse  $|S_i|$  finden.

<sup>2</sup>Für eine genauere Beschreibung und einen Beweis verweise ich auf Seiten 23 ff. von [10]

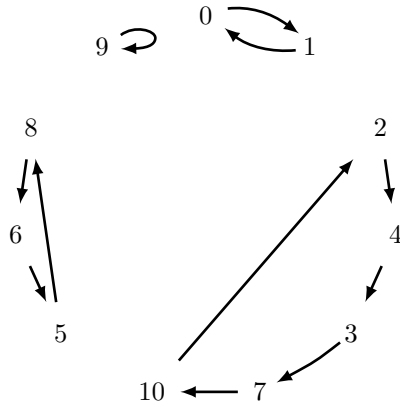


Abbildung 4.2: Der Funktionsgraph der Funktion  $g(x) = -x^3 + 1 \pmod{11}$

Als Beispiel nehmen wir  $g : S \rightarrow S$  mit  $S = \mathbb{Z}/11\mathbb{Z}$ ,  $g(x) = -x^3 + 1$ . Betrachten wir uns die Funktionswerte von  $g$  an, sehen wir, dass diese Funktion bijektiv ist. Wenn wir den Graphen anschauen, sehen wir die einzelnen Zykeln und deren dazugehörige Mengen  $S_i$ :  $S_0 = \{0, 1\}$ ,  $S_1 = \{2, 3, 4, 7, 10\}$ ,  $S_2 = \{5, 6, 8\}$  und  $S_3 = \{9\}$ . Wir sehen nun, dass  $g^1(9) = 9$ ,  $g^3(8) = 8$ ,  $g^5(2) = 2$  etc.

Die Frage ist nun, wie wir effizient die Grösse der Teilmenge finden können, in der  $x$  sich befindet. Sei dafür  $U_f$  der Operator, welcher  $f$  auf Quantencomputern implementiert (welcher nach Voraussetzung existiert). Was passiert, wenn wir diesem Operator eine Superposition der Zahlen in  $S_i$  übergeben?

Seien  $r = |S_i|$ ,  $x_0, x_1, \dots, x_{r-1}$  die Zahlen in  $S_i$ , sodass  $f(x_j) = x_{(j+1) \pmod r}$  und  $U_f$  die Quantenoperation, die  $f$  implementiert. Schauen wir mal, was passiert, wenn wir  $U_f$  auf den Zustand  $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |x_j\rangle$  anwenden. Wir bekommen:

$$U_f\left(\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |x_j\rangle\right) = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |f(x_j)\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |x_{(j+1) \pmod r}\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |x_j\rangle$$

Daraus schliessen wir, dass  $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |x_j\rangle$  ein Eigenvektor von  $U_f$  mit Eigenwert 1 ist. Dieser Eigenwert ist nicht wirklich interessant. Wir können ihn aber interessanter machen, indem wir den einzelnen Summanden eine Phase mitgeben. Dazu konstruieren wir die Superposition  $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)$  für ein  $k < r$ . Was passiert, wenn wir  $U_f$  darauf anwenden?

$$\begin{aligned} U_f\left(\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)\right) &= \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_{(j+1) \pmod r}\rangle) = \\ &= \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{k(j-1)}{r}} |x_j\rangle) = e^{2i\pi \frac{k}{r}} \left(\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)\right) \end{aligned}$$

Hier haben wir es mit einem Eigenvektor zum Eigenwert  $e^{2i\pi \frac{k}{r}}$  zu tun. Dieser ist für uns interessant, weil  $r$  darin vorkommt. Wir machen auch die Beobachtung, dass unser Eigenvektor von vorher ( $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |x_j\rangle$ ) auch von der Form ist, die wir gerade analysiert haben, einfach mit  $k = 0$ . Falls wir jetzt irgendwie einen Zustand von der Form  $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)$  erzeugen können, könnten wir mit Hilfe der Phasenabschätzung den Quotienten  $\frac{k}{r}$  abschätzen. Die Frage ist, wie können wir solch einen Zustand generieren? Zuerst sagen wir,  $|\psi_k\rangle$  sei  $\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)$ . Was passiert nun, wenn wir die Vektoren  $|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_{r-1}\rangle$  aufsummieren?

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \frac{1}{\sqrt{r}} \left(\sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)\right) = \frac{1}{r} \sum_{j=0}^{r-1} \sum_{k=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle) = |x_0\rangle$$

Dieses überraschende Resultat lässt sich durch Expandieren beweisen. Aber eine einfachere Art zu sehen, dass dieses überraschende Resultat stimmt, ist, dass man die Summe  $\sum_{k=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)$  für  $j = 0$  betrachtet. Da  $j = 0$  gilt, gilt  $e^{-2i\pi \frac{kj}{r}} = e^0 = 1$  und somit  $\sum_{k=0}^{r-1} (e^{-2i\pi \frac{k \cdot 0}{r}} |x_0\rangle) = r |x_0\rangle$ . Da  $\frac{1}{r}(r |x_0\rangle)$  bereits einen Betrag von 1 hat, kann kein anderer Zustand mit positivem Betrag existieren, da die Beträge sich sonst zu etwas Grösserem als 1 aufsummieren würden.

Sei nun  $|\psi_k\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} (e^{-2i\pi \frac{kj}{r}} |x_j\rangle)$  eine kürzere Schreibweise für die oben genannten Eigenvektoren. Somit ist  $|x_0\rangle$  einfach eine Superposition der Eigenvektoren  $|\psi_0\rangle, \dots, |\psi_{r-1}\rangle$ . Das heisst, wenn wir der Periodenabschätzungsfunktion einen Wert mitgeben, den wir als  $|x_0\rangle$  gebrauchen können, haben wir eine Superposition dieser Eigenvektoren. Probieren wir nun, den Eigenwert dieser Superposition abzuschätzen.

Betrachten wir den Phasenabschätzungs-Algorithmus nochmals bis zum Punkt bevor wir das Register messen. Dies alles können wir als eine Operation  $P$  mit  $P |0\rangle |\psi\rangle \rightarrow |2^m \theta\rangle |\psi\rangle$  zu einem Eigenvektor  $|\psi\rangle$  schreiben, wobei  $m$  die gewählte Genauigkeit der Phasenabschätzung ist. Da die auf Quantencomputern implementierten Operationen linear sind, gilt:

$$P |0\rangle |x_0\rangle = P \left( |0\rangle \left( \sum_{k=0}^{r-1} |\psi_k\rangle \right) \right) = \sum_{k=0}^{r-1} (P |0\rangle |\psi_k\rangle) = \sum_{k=0}^{r-1} (|2^m \theta_k\rangle |\psi_k\rangle) = \sum_{k=0}^{r-1} \left( \left| 2^m \frac{k}{r} \right\rangle |\psi_k\rangle \right)$$

Messen wir somit dann das Resultat, so kollabiert diese Superposition und wir bekommen den Wert  $2^m \frac{k}{r}$  für ein  $k \in \{0, \dots, r-1\}$ , wobei alle die gleiche Wahrscheinlichkeit haben. Mit Hilfe der von Kettenbrüchen<sup>3</sup> können wir nun den Bruch  $\frac{k}{r}$  vom Bruch  $\frac{2^m r}{2^m}$  abschätzen. Nun stellt sich heraus, wenn  $m \geq 2n$  gilt, dann ist der Bruch  $\frac{2^m k}{2^m}$  genug genau, dass der nächste Bruch mit Nenner kleiner oder gleich  $n$  an  $\frac{2^m k}{2^m}$  der Bruch  $\frac{k}{r}$  selbst ist<sup>4</sup>. Wenn wir also mit Hilfe von Kettenbrüchen den Näherungsbruch mit dem grössten Nenner kleiner oder gleich  $n$  nehmen, dass dieser Näherungsbruch  $\frac{k}{r}$  sein muss.

Nun kann es sein, dass  $\text{ggT}(k, r) = g \neq 1$  gilt, somit der Bruch mit  $g$  gekürzt wird, und wir so an Stelle von  $r$  die Zahl  $\frac{r}{g}$  zurückbekommen. Wir können aber durch Anwendung von  $f^r$  überprüfen, ob  $r$  tatsächlich die Periode ist, da für  $r' < r$  die Gleichung  $f^{r'}(x) = x$  nicht gelten kann. Und um den richtigen Wert  $r$  zu bekommen, können wir die Prozedur wiederholen. Wiederholen wir sie  $2 \log(N)$  mal, bekommen wir mit sehr hoher Wahrscheinlichkeit mindestens einmal die korrekte Periode. Den Beweis dazu kann man in [11], Seiten 229ff., nachlesen.

## 4.5 Die Ordnung von Zahlen bestimmen

Der Algorithmus von Shor ist deshalb so schnell, da mit Hilfe des quantenbasierten Teils des Algorithmus die Ordnung einer Zahl effizient bestimmt werden kann. Die Ordnung einer Zahl  $a$  modulo einer Zahl  $n$ , geschrieben als  $\text{ord}_n(a)$ , ist die kleinste positive Zahl  $r$ , sodass  $a^r \equiv 1 \pmod{n}$  gilt. Dabei muss  $\text{ggT}(a, n) = 1$  gelten, denn sonst kann dieses  $r$  nicht existieren (zum Beispiel gibt es kein  $r$  mit  $2^r \equiv 1 \pmod{8}$ ). Wenn diese Bedingung aber erfüllt ist, so sagt der Satz von Euler-Fermat, dass  $a^{\phi(n)} \equiv 1 \pmod{n}$  gilt, wobei  $\phi(n)$  die eulersche Phi-Funktion ist.

<sup>3</sup>Auf eine genauere Betrachtung von Kettenbrüchen verzichte ich hier, sollte der Leser damit nicht vertraut sein, verweise ich auf [14]

<sup>4</sup>Für dieses Resultat verweise ich auf [11]. Die Beschreibung befindet sich auf Seite 229 und der Beweis des dazu gebrauchten Theorems im Appendix 4

Da  $\text{ggT}(a, n) = 1$  gilt, ist die Restklasse kongruent zu  $a$  modulo  $n$  ein Element der primen Restklassengruppe  $(\mathbb{Z}/n\mathbb{Z})^\times$ . Dies setzt sofort die Existenz eines inversen Elements  $a^{-1}$  modulo  $n$  voraus. Wir rechnen nun in  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

Sei  $f$  definiert als  $f(x) := ax$ . Da diese Funktion invertierbar ist (die inverse Funktion ist  $f^{-1}(x) = a^{-1}x$ ), ist sie bijektiv. Wir stellen nun fest, dass die Zahl  $r = \text{ord}_n(n)$  die kleinste Zahl ist, sodass  $f^r(1) = a^r \cdot 1 = 1$  gilt. Da  $f$  bijektiv ist, ist es wahrscheinlich, dass man sie auf Quantencomputern implementieren kann. Und tatsächlich haben wir diese Funktion implementiert: Sie ist nichts anderes als die in 3.5 beschriebene Modulare Multiplikation.

Sei  $U_f$  die Quantenoperation, die  $f$  auf Quantencomputern implementiert. Nun können wir der Periodenabschätzungsfunktion diesen Quantenoperator und als Startwert die Zahl 1 übergeben, und sie berechnet für uns die kleinste Zahl  $r$ , so dass  $f^r(1) = 1$  gilt, was tatsächlich die gesuchte Ordnung ist. Um klassisch effizient überprüfen zu können, ob das gefundene  $r$  die wirkliche Ordnung ist, können wir den den Binären Exponentiation verwenden.

Nun stellt sich die Frage, ob sich  $U_f^{2^k}$  effizient implementieren lässt. Dazu stellen wir fest, dass  $U_f^{2^k}$  nichts anderes als die Quantenoperation ist, welche  $f^{2^k}$  implementiert. Gleichzeitig gilt  $f^{2^k}(x) = a^{2^k}x$ . Dies wiederum ist nichts anderes als eine Modulare Multiplikation mit der Zahl  $a^{2^k}$ , wobei sich die Zahl  $a^{2^k} \pmod n$  klassisch effizient berechnen lässt (auch dazu können wir wieder den Algorithmus der Binären Exponentiation verwenden). Somit können wir für jedes  $k$  die Quantenoperation  $U_f^{2^k}$  mit nur einer modularen Multiplikation implementieren.

Fassen wir all dies zusammen, können wir die im vorherigen Kapitel erklärte Periodenabschätzungsfunktion verwenden, um die Ordnung einer Zahl  $a$  modulo einer Zahl  $n$  effizient abzuschätzen, falls  $\text{ggT}(a, n) = 1$  gilt.

## 4.6 Das Ziel - Der Shor-Algorithmus

### 4.6.1 Der Algorithmus

Im Grunde genommen erlaubt uns der Algorithmus von Shor nur, einen nicht-trivialen Teiler  $d$  von  $n$  zu finden. Dies lässt sich jedoch leicht zu einem Algorithmus, welcher Zahlen faktorisiert, umschreiben: Solange  $n$  keine Primpotenz ist, finde einen nicht-trivialen Teiler  $d$  von  $n$  und faktorisiere rekursiv die beiden Zahlen  $d$  und  $\frac{n}{d}$ . Probieren wir nun, einen nicht-trivialen Teiler von  $n$  zu finden.

In einem ersten Schritt überprüfen wir, ob  $n$  durch 2 teilbar oder eine Primpotenz ist. Letzteres lässt sich überprüfen, indem man für jede möglich Potenz  $s \leq \log(n)$  überprüft, ob eine Zahl  $p$  mit  $p^s = n$  existiert. Diese Zahl  $p$ , falls sie existiert, kann man mit einer binären Suche finden.

Als nächstes wählen wir eine zufällige Zahl  $a$  mit  $1 < a < n$ . Falls  $\text{ggT}(a, n) \neq 1$  gilt, hat man bereits einen nicht-trivialen Teiler gefunden, den man zurückgeben kann. Sonst bestimmen wir mit Hilfe der Periodenabschätzung wie im Kapitel 4.5 beschrieben die Ordnung der Zahl  $a$  modulo  $n$ . Dies ist der einzige Schritt des Algorithmus, an dem wir Quantencomputer benötigen. Sei diese Ordnung  $r$ . Falls  $r$  ungerade ist oder  $a^{\frac{r}{2}} \equiv -1 \pmod n$  gilt, beginnen wir wieder von vorne. Die Wahrscheinlichkeit, dass wir wieder von vorne beginnen müssen, ist dabei aber kleiner

oder gleich  $\frac{1}{2^m}$ , wobei  $m$  die Anzahl verschiedener Primteiler von  $n$  ist. Den Beweis dazu kann man in [11] Seiten 233ff. nachlesen.

Wir sind nun im Besitz einer Zahl  $a$  mit Ordnung  $r$ , wobei  $2 \mid r$  und  $a^{\frac{r}{2}} \not\equiv -1 \pmod{n}$  gilt. Da  $r$  die Ordnung ist, gilt auch  $a^{\frac{r}{2}} \not\equiv 1 \pmod{n}$ . Dies bedeutet, wir haben eine nicht-triviale Wurzel von 1 modulo  $n$  gefunden. Nun gilt  $n \mid (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$ , aber  $n \nmid a^{\frac{r}{2}} + 1$  und  $n \nmid a^{\frac{r}{2}} - 1$ . Somit haben wir zwei Zahlen  $b = a^{\frac{r}{2}} + 1$  und  $c = a^{\frac{r}{2}} - 1$  mit:

$$n \mid bc \tag{1}$$

$$n \nmid b \tag{2}$$

$$n \nmid c \tag{3}$$

Sei nun  $p_0^{\alpha_0} p_1^{\alpha_1} \dots = n$  die Primzahlzerlegung von  $n$ ,  $p_0^{\beta_0} p_1^{\beta_1} \dots = b$  diejenige von  $b$  und  $p_0^{\gamma_0} p_1^{\gamma_1} \dots = c$  diejenige von  $c$ . Aus (1) wissen wir nun, dass für jedes  $k$  die Ungleichung  $\beta_k + \gamma_k \geq \alpha_k$  gelten muss. Gleichzeitig folgt aus (2) und (3), dass ein  $i$  und ein  $j$  existieren müssen, so dass  $\beta_i < \alpha_i$  und  $\gamma_j < \alpha_j$  gelten. Daraus folgt, dass  $\text{ggT}(b, n)$  und  $\text{ggT}(c, n)$  nicht  $n$  sein können. Gleichzeitig müssen wegen  $\beta_k + \gamma_k \geq \alpha_k$  auch  $\gamma_i > 0$  und  $\beta_j > 0$  gelten, woraus  $\text{ggT}(b, n) > 1$  und  $\text{ggT}(c, n) > 1$  folgt.

Daraus schliessen wir, dass beide Zahlen  $b$  und  $c$  Faktoren von  $n$  enthalten. Diese können durch die Berechnung von  $\text{ggT}(b, n)$  und  $\text{ggT}(c, n)$  mit Hilfe des euklidischen Algorithmus extrahiert werden. Fassen wir all dies zusammen, sind wir nun im Besitz eines Algorithmus, der einen nicht-trivialen Teiler von  $n$  findet:

1. Falls  $n$  durch zwei teilbar ist, gib 2 zurück und terminiere.
2. Falls  $n = p^a$  eine Primpotenz ist, gib die Primzahl  $p$  zurück und terminiere.
3. Bestimme eine zufällige Zahl  $1 < a < n - 1$ .
4. Finde  $g = \text{ggT}(a, n)$ . Falls  $g \neq 1$  ist, gib  $g$  zurück und terminiere.
5. Bestimme die Ordnung von  $a$  modulo  $n$  mit Hilfe des Quantenteils des Algorithmus:
  - (a) Schätze die Phase des Operators  $U_f$  ab, der  $f(x) = ax$  implementiert mit einer Präzision von  $m = 2 \log_2(n)$  ab. Benutze dazu den in Kapitel 4.3 vorgestellten Algorithmus. Sei das Resultat  $2^m \lambda$ .
  - (b) Schätze den Quotienten  $\frac{k}{r}$  von  $\frac{2^m \lambda}{2^m}$  ab. Falls  $r$  nicht die gesuchte Periode ist, gehe zurück zu (a), sonst gib die Periode  $r$  zurück.
6. Falls  $r$  ungerade ist, gehe zurück zu 2. Sonst berechne  $a^{\frac{r}{2}} \pmod{n}$ . Falls dies kongruent zu  $-1 \pmod{n}$  ist, gehe zurück zu 2.
7. Berechne  $b = (a^{\frac{r}{2}} + 1)$ . Gib  $\text{ggT}(b, n)$  zurück und terminiere.

#### 4.6.2 Analyse des Algorithmus

Wie in der Einführung bereits angetönt, liegt der grosse Vorteil dieses Algorithmus daran, dass er effizienter als alle auf klassischen Computern bekannten Algorithmen ist, wobei wir diesen Algorithmus als effizient bezeichnen, weil seine Laufzeit nicht direkt von der zu faktorisierenden Zahl abhängig ist, sondern nur von deren Logarithmus.

Sei  $L$  die Anzahl Bits, die benötigt wird, um die zu faktorisierende Zahl  $n$  abzuspeichern. In anderen Worten  $L = \lceil \log 2(n) \rceil$ . Die Laufzeit der meisten auf klassischen Computern bekannten Algorithmen sind exponentiell in  $L$ , während Shor's Algorithmus eine Laufzeit hat, die nur polynomiell in  $L$  ist.

Die Periodenabschätzungsfunktion ruft die mitgegebene Funktion  $2L \in \mathcal{O}(L)$  mal auf. Diese mitgegebene Funktion ist die modulare Multiplikation, welche die Addition  $\mathcal{O}(L)$  mal aufruft. Diese jedoch ruft die Fouriertransformation auf, welche eine  $\mathcal{O}(L^2)$  Gatteroperationen benötigt. Multiplizieren wir dies zusammen, so braucht die Periodenabschätzungsfunktion  $\mathcal{O}(L^4)$  Gatteroperationen. Würde man an Stelle der auf der *QFT*-basierenden Addition die aus klassischen Schaltkreisen bekannte Addition verwenden, kann man diese Gatterzahl auf  $\mathcal{O}(L^3)$  herunterbringen. Diese Periodenabschätzungsfunktion wird im Erwartungswert  $\mathcal{O}(1)$  mal aufgerufen, was zu einer gesamten Laufzeit von  $\mathcal{O}(L^4)$  führt.



# Kapitel 5

## Ausblick

### 5.1 Man kann Zahlen effizient faktorisieren - Was nun?

Wir haben nun gesehen, dass man Zahlen mit Hilfe von Quantencomputern effizient faktorisieren kann. Einerseits ist dies eine grosse Errungenschaft: Shors Algorithmus demonstriert uns, wie man mit Quantencomputern exponentielle Verschnellerungen erreichen kann. Auf der anderen Seite birgt diese Errungenschaft auch Gefahren. Zum Beispiel können Verschlüsselungsverfahren geknackt werden, wenn man Zahlen faktorisieren kann. Ich möchte hier kurz vorzeigen, wie man das RSA-Verschlüsselungsverfahren knacken kann, wenn man Zahlen effizient faktorisieren kann. Zu einer kurzen Beschreibung verweise ich auf [3] oder für die originale Arbeit auf [13].

Sei  $n = pq$  der Modulus der Verschlüsselung und  $e$  der öffentliche Schlüssel. Da wir nun  $n = pq$  faktorisieren können, können wir  $\phi(n) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$  berechnen. Damit können wir den privaten Schlüssel  $d \equiv e^{-1} \pmod{\phi(n)}$  berechnen, denn wir wissen, dass  $m^{e \cdot d} \equiv m^{e \cdot e^{-1} \pmod{\phi(n)}} \equiv m^1 \equiv m \pmod{n}$  gilt, wobei die letzte Äquivalenz wegen des Satzes von Euler-Fermat gilt.

Da nun Verschlüsselungen, die auf der Schwierigkeit der Faktorisierung beruhen, geknackt werden können, steht das Forschungsgebiet der Kryptographie vor neuen Herausforderungen. Das neue Gebiet, welches sich mit der Kryptographie im Zeitalter der Quantencomputer befasst, nennt sich Post-Quantum-Kryptographie.

### 5.2 Quantencomputer - Wie bald?

Wie bereits angesprochen, gibt es verschiedene Möglichkeiten, Quantencomputer physikalisch zu realisieren. Technik-Firmen und Forschungsinstitute versuchen schon länger, Quantencomputer zu bauen. Bereits im Jahr 1998 gelang es zwei Forschern aus Oxford, einen Quantenalgorithmus für Deutschs Problem [8], und drei amerikanischen Forschern, Grovers Algorithmus experimentell zu realisieren [4]. Bereits im Jahr 2001 folgte darauf die erste experimentelle Realisation des Shor-Algorithmus [15], mit welcher die Zahl 15 faktorisiert werden konnte.

Über die Jahre entwickelten sich Quantencomputer immer weiter. Zum Zeitpunkt dieser Arbeit haben Tech-Firmen wie Google, IBM, Intel etc. Quantenprozessoren mit bis zu 72 Qubits (Googles Bristlecone [9]). Im Jahr 2019 legte Google einen Artikel [1] vor, laut welchem sie die Quantenüberlegenheit erreicht hätten. Dies bedeutet, dass sie auf einem Quantencomputer etwas effizient berechnet hätten, was auf einem klassischen Computer nicht effizient berechenbar wäre. Dies löste prompt einen Disput aus und die IBM zweifelte in einem Blog die Quantenüberlegenheit

an [12]. Während im Bericht von Google behauptet wurde, ein klassischer Computer würde 10000 Jahre benötigen, wurde in IBMs Blog behauptet, dass ein klassischer Computer dies in 2.5 Tage tun könne. Der Artikel von Google blieb unpubliziert. Trotzdem ist es meiner Meinung nach beeindruckend, dass Googles Quantencomputer für diese Aufgabe nur etwa 200 Sekunden benötigt, während ein Supercomputer 2.5 Tage benötigt.

Die IBM selbst jedoch hat auch grosse Pläne. Im September 2020 hat sie in ihrer Quantum Roadmap [7] angekündigt, dass sie bis im Jahr 2023 einen Quantencomputer mit 1121 Qubits bauen und somit die Qubit-Zahlen sprengen möchte.

Wenn die IBM diesen Plan durchziehen kann und Google sowie die anderen Tech-Firmen auch in naher Zukunft so grosse Quantencomputer bauen, denke ich, dass die Zeit, in der quantenbasierte Supercomputer schwierige Berechnungen übernehmen werden, nicht mehr weit entfernt ist.

## Kapitel 6

# Nachwort

Ich höre immer wieder die Frage, ob Quantencomputer die Computer der Zukunft sind. Ich denke, dass Quantencomputer in Zukunft sehr wichtig werden. Da sie auf anderen physikalischen Vorgängen beruhen als normale Computer, kann man mit ihnen weitaus schwierigere Dinge berechnen als mit klassischen Computern. Zudem ist das Gebiet der Quantencomputer noch sehr neu, deshalb denke ich, dass wir noch nicht das ganze Potenzial von Quantencomputern kennen.

Quantencomputer sind ein aktuelles Thema. Ich lese immer wieder Zeitungs- und Journalartikel über Fortschritte in diesem Gebiet.

Dieses Gebiet weckte so mein Interesse, jedoch verstand ich anfangs nichts davon und ich brauchte eine gewisse Zeit, bis ich die Grundlagen auch nur ansatzweise verstand. Aber das Gebiet faszinierte mich sehr und ich war motiviert, weiterzufahren. Zu sehen, wenn etwas funktionierte, erfreute mich jedes Mal von Neuem.

Ich habe durch diese Arbeit sehr viel gelernt und es war die Mühe wert, in dieses komplexe Thema einzutauchen.

# Kapitel 7

## Anhang

### 7.1 Mathematische Symbole

$|v\rangle$  Schreibweise des Vektors  $v$  in der Bra-Ket-Notation.

$(|u\rangle, |v\rangle)$  **oder**  $\langle u|v\rangle$  Skalarprodukt der beiden Vektoren  $|u\rangle$  und  $|v\rangle$ .

$\| |v\rangle \|$  Norm des Vektors  $|v\rangle$

$\mathbb{R}, \mathbb{C}$  Raum der reellen beziehungsweise der komplexen Zahlen.

$\mathbb{R}^n, \mathbb{C}^n$   $n$ -dimensionaler Vektorraum über die reellen beziehungsweise die komplexen Zahlen

$\overline{A}, A^T, A^\dagger$  Die komplex konjugierte, die transponierte und die adjungierte Matrix zu der Matrix  $A$ . Siehe 2.1.4

$I$  Die Identitätsmatrix mit der Eigenschaft  $I |v\rangle = |v\rangle$  für alle  $|v\rangle$ .

$H, X, Y, Z$  Das Hadamard- und die drei Pauli-Gatter. Siehe 2.2.4

$QFT$  Die Quantenfouriertransformation. Siehe 3.2

$f^k$   $k$ -fache Anwendung der Funktion  $f$ .

$U^c$  Kontrollierte Anwendung der Operation  $U$ . Siehe 2.2.5.

$\mathbb{Z}/n\mathbb{Z}$  Restklassenring der Restklassen bei der Division durch  $n$ .

$(\mathbb{Z}/n\mathbb{Z})^\times$  Prime Restklassengruppe der Restklassen bei der Division durch  $n$ , welche mit  $n$  teilerfremd sind.

### 7.2 Literatur

# Literatur

- [1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven und J. M. Martinis, “Quantum supremacy using a programmable superconducting processor,” *Nature*, Jg. 574, Nr. 7779, S. 505–510, Okt. 2019, ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5. Adresse: <https://doi.org/10.1038/s41586-019-1666-5>.
- [2] A. Asfaw, L. Bello, Y. Ben-Haim, S. Bravyi, N. Bronn, L. Capelluto, A. C. Vazquez, J. Ceroni, R. Chen, A. Frisch, J. Gambetta, S. Garion, L. Gil, S. D. L. P. Gonzalez, F. Harkins, T. Imamichi, D. McKay, A. Mezzacapo, Z. Mineev, R. Movassagh, G. Nannicini, P. Nation, A. Phan, M. Pistoia, A. Rattew, J. Schaefer, J. Shabani, J. Smolin, K. Temme, M. Tod, S. Wood und J. Wootton. (2020). “Learn Quantum Computation Using Qiskit,” Adresse: <http://community.qiskit.org/textbook>.
- [3] S. Asjad, “The RSA Algorithm,” Dez. 2019.
- [4] I. L. Chuang, N. Gershenfeld und M. Kubinec, “Experimental Implementation of Fast Quantum Searching,” *Phys. Rev. Lett.*, Jg. 80, S. 3408–3411, 15 Apr. 1998. DOI: 10.1103/PhysRevLett.80.3408. Adresse: <https://link.aps.org/doi/10.1103/PhysRevLett.80.3408>.
- [5] T. G. Draper, “Addition on a Quantum Computer,” Sep. 1998. Adresse: <https://cds.cern.ch/record/450434/files/0008033.pdf>.
- [6] G. Fischer, *Lineare Algebra*, 18 A. Springer Spektrum, 2013, ISBN: 978-3-658-03944-8.
- [7] J. Gambetta, *IBM’s Roadmap For Scaling Quantum Technology*, Sep. 2020. Adresse: <https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/> (besucht am 28.10.2020).
- [8] J. A. Jones und M. Mosca, “Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer,” *The Journal of Chemical Physics*, Jg. 109, Nr. 5, S. 1648–1653, Aug. 1998, ISSN: 1089-7690. DOI: 10.1063/1.476739. Adresse: <http://dx.doi.org/10.1063/1.476739>.

- [9] J. Kelly, *A Preview of Bristlecone, Google's New Quantum Processor*, März 2018. Adresse: <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html> (besucht am 28.10.2020).
- [10] G. Mislin, *Algebra I*. vdf Hochschulverlag, 1998, ISBN: 978-3-7281-2408-1.
- [11] M. A. Nielsen und I. L. Chuang, *Quantum Computation and Quantum Information*, 10. Aufl. Cambridge University Press, 2010, ISBN: 978-1-107-00217-3.
- [12] E. Pednault, J. Gunnels, D. Maslov und J. Gambetta. (Okt. 2019). "On "Quantum Supremacy"," Adresse: <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/> (besucht am 25.10.2020).
- [13] R. L. Rivest, A. Shamir und L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, Jg. 21, Nr. 2, S. 120–126, Feb. 1978, ISSN: 0001-0782. DOI: 10.1145/359340.359342. Adresse: <https://doi.org/10.1145/359340.359342>.
- [14] P. Stopp, *Zur Arithmetik von Kettenbrüchen*, Sep. 2009. Adresse: <https://www.math.uni-sb.de/ag/gekeler/PERSONEN/Bachelorarbeiten/Stopp.pdf>.
- [15] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood und I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, Jg. 414, Nr. 6866, S. 883–887, Dez. 2001, ISSN: 1476-4687. DOI: 10.1038/414883a. Adresse: <https://doi.org/10.1038/414883a>.
- [16] V. Vedral, A. Barenco und A. Ekert, "Quantum networks for elementary arithmetic operations," *Physical Review A*, Jg. 54, Nr. 1, S. 147–153, Juli 1996, ISSN: 1094-1622. DOI: 10.1103/physreva.54.147. Adresse: <http://dx.doi.org/10.1103/PhysRevA.54.147>.

## 7.3 Redlichkeitserklärung