



Mathematisch-Naturwissenschaftliche Fakultät II Institut für Informatik  
Lehrstuhl für Komplexität und Kryptografie

## Diplomarbeit

# Quantenalgorithmen zum Auffinden versteckter Untergruppen

eingereicht von: Philipp-Immanuel Schneider

Berlin, den 19.03.2008

Betreuer: Prof. J. Köbler

Viele auf Quantencomputern effizient lösbare Probleme, für die kein effizienter klassischer Algorithmus bekannt ist, lassen sich auf eine Instanz des Hidden Subgroup Problems (HSP) zurückführen. Diese Diplomarbeit soll die wissenschaftlichen Fortschritte in diesem Bereich in einer einheitlichen Notation zusammenfassen. Besonderer Wert wird auf die möglichst lückenlose Einführung in die zugrunde liegenden Theorien Quantenmechanik, Gruppentheorie und Darstellungstheorie gelegt, so dass beim Leser lediglich Vorwissen in der linearen Algebra vorausgesetzt wird. Darauf aufbauend werden ein allgemeines Lösungsverfahren des HSP im abelschen Fall vorgestellt und weiterführende Ergebnisse der Komplexitätstheorie und des nichtabelschen Falles des HSP beleuchtet.

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Physikalischer Hintergrund und quantenmechanische Notation</b>	<b>5</b>
2.1	Mathematische Struktur der Quantenmechanik . . . . .	5
2.2	Quantenregister . . . . .	8
2.3	No-Cloning Theorem . . . . .	10
<b>3</b>	<b>Quanten-Komplexitätstheorie</b>	<b>12</b>
3.1	Turingmaschine und Quanten-Turingmaschine . . . . .	12
3.2	Die Komplexitätsklassen EQP und BQP . . . . .	15
3.3	Orakeltechniken in der Quanten-Komplexitätstheorie . . . . .	17
<b>4</b>	<b>Darstellungstheorie</b>	<b>19</b>
4.1	Grundlegende Definitionen der Gruppentheorie . . . . .	19
4.2	Darstellung von Gruppen . . . . .	21
4.3	Charaktere einer Darstellung . . . . .	23
4.4	Schur'sches Lemma . . . . .	24
4.5	Darstellung abelscher Gruppen . . . . .	28
<b>5</b>	<b>Fouriertransformation für Gruppen</b>	<b>31</b>
<b>6</b>	<b>Das Hidden Subgroup Problem</b>	<b>34</b>
6.1	Die schwache Form des Algorithmus . . . . .	35
6.2	Die starke Form des Algorithmus . . . . .	37
6.3	HSP für abelsche Gruppen . . . . .	38
6.3.1	Beispiel: Simon's Problem . . . . .	41
6.3.2	Beispiel: Primzahlfaktorisierung mit dem Algorithmus von Shor . . . . .	42
6.4	HSP für nichtabelsche Gruppen . . . . .	44
6.4.1	Normale Untergruppen . . . . .	44
6.4.2	Einige effizient lösbare Fälle des nichtabelschen HSP . . . . .	46
6.5	Das Graphisomorphieproblem als negatives Resultat . . . . .	47
6.5.1	Darstellungstheorie der symmetrischen Gruppe . . . . .	49
6.5.2	GI ist nicht mithilfe des Quantenalgorithmus lösbar . . . . .	51
<b>7</b>	<b>Schlussbemerkung</b>	<b>55</b>

# 1 Einführung

Die Anfänge der Quantenmechanik reichen zum Beginn des 20. Jahrhunderts zurück. Es wird ihr zu Beginn ein eigenes Kapitel gewidmet, um ihre grundlegende mathematische Struktur einzuführen, wie sie bis in die 1930er Jahre entwickelt wurde. Die Quantenmechanik sagt Phänomene voraus, wonach Teilchen mehrere Zustände gleichzeitig annehmen können und physikalische Observablen wie die Energie meist nur in diskreten, d.h. „gequantelten“ Größen auftreten können.

Charles H. Bennett, David Deutsch und Richard P. Feynman waren in den 1970er Jahren unter den ersten, die das Potenzial erkannten, welches diese Phänomene für eine neue Art von Berechnung bereitstellte. Computer, die die Phänomene der Quantenphysik nutzen, sollten nach ihrer Meinung Probleme effizient lösen können, die auf klassischen Computern exponentiellen Rechenaufwand benötigen.

Das erste abstrakte Modell eines Quantencomputers wurde 1982 von Feynman entwickelt. Er schlug vor, mit ihm physikalische Prozesse zu simulieren, was klassisch einen hohen Aufwand bedeutet [RF].

1985 erweiterte Deutsch das Prinzip der universellen Turingmaschine auf einen universellen Quantencomputer, der alle auf quantenmechanischen Systemen lösbare Probleme berechnen konnte [DD]. Die Definition der universellen Turingmaschine wurde von Bernstein und Vazirani weiter verbessert. Damit gelang ihnen eine grobe Einordnung der Komplexitätsklasse BQP, der auf Quantencomputern effizient und mit kleiner Fehlerwahrscheinlichkeit berechenbaren Probleme in bereits bekannte klassische Komplexitätsklassen [BV]. Obgleich sich nicht beweisen lässt, dass Quantencomputer mehr als einen polynomiellen Geschwindigkeitszuwachs gegenüber klassischen Computern liefern, lassen sich doch interessante Aussagen über die Komplexitätsklasse BQP treffen, die im zweiten Kapitel vorgestellt werden.

Da die Quantenphysik viele klassisch undenkbare Phänomene bietet, wurde auch die Suche nach interessanten Algorithmen und Anwendungen, die diese Phänomene ausnutzen, entfacht. Nachdem viele Jahre lang nur sehr künstliche mathematische Probleme als Kandidaten ausgemacht werden konnten, entwickelte Peter Shor 1994 eine Methode der schnellen Faktorisierung auf Quantencomputern [PS]. Dies stellte eine ernsthafte Gefährdung der gängigen kryptographischen Methoden dar. Quantencomputer waren plötzlich von hohem Interesse und die Forschung in diesem Bereich intensivierte sich.

Die Frage, die sich natürlicher Weise stellt, ist, was die bisher gefundenen Quanten-Algorithmen vereint. Welche Klasse von Problemen lassen sich mit welchen Techniken auf Quantencomputern effizient lösen? Gibt es eine verborgene mathematische Struktur die diesen Problemen zugrunde liegt? In den letzten Jahren ist man der Beantwortung dieser Fragen näher gerückt: Viele der bisher gefundenen Quantenalgorithmen lassen sich auf das so genannte *Hidden Subgroup Problem* zurückführen:

## **Problem 1.1 (HSP)**

**gegeben:** Eine Funktion  $f : G \rightarrow A$ , wobei  $G$  eine endliche Gruppe und  $A$  eine beliebige Menge ist.

**promise:** Es existiert eine Untergruppe  $H \leq G$ , sodass  $f$  auf unterschiedlichen Linksnebenklassen  $gH$  verschiedene Werte annimmt und auf allen Linksnebenklassen konstant ist.

**gesucht:** Ein vollständiger Satz von Generatoren  $S \subset G$  mit  $\langle S \rangle = H$

Der entscheidende Schlüssel in allen Algorithmen ist eine Fouriertransformation, welche man für Gruppen im Allgemeinen definieren kann. Sie nimmt für die Spezialfälle die unterschiedlichsten Formen an. So ist die Walsh-Hadamard Transformation die Fouriertransformation der Gruppe  $\mathbb{Z}_2^n$ . Die Fouriertransformation auf Gruppen stellt eine Verbindung zwischen dem Raum der Gruppenelemente und dem Raum der *Darstellungen* der Gruppe dar. Die Darstellungstheorie wird also von besonderem Interesse sein und wird ebenfalls in einem Kapitel zusammen mit einem kurzen Überblick über die Grundlagen der Gruppentheorie eingeführt.

Danach ist man in der Lage, die Fouriertransformation auf Gruppen zu definieren und den allgemeinen Lösungsweg für das Hidden Subgroup Problem auf Quantencomputern zu entwickeln. Für den Spezialfall abelscher Gruppen lässt sich ein konkreter Algorithmus angeben, der ebenfalls vorgestellt wird. Der nichtabelsche Fall des HSP wird sich als ungleich schwieriger herausstellen. Neben einigen positiven Ergebnissen, die kurz vorgestellt werden, scheint das Graphisomorphieproblem nicht mit den zu behandelnden algorithmischen Methoden effizient lösbar. Dazu werden Beweistechniken vorgestellt und aktuelle Ergebnisse genannt.

## 2 Physikalischer Hintergrund und quantenmechanische Notation

### 2.1 Mathematische Struktur der Quantenmechanik

Die Quantenmechanik (QM) ist eine der am besten bestätigten physikalischen Theorien. Leider ist unsere Intuition von unserer makroskopischen Umwelt geprägt, in der sich die quantenmechanischen Gesetze nicht direkt beobachten lassen, wohl aber ihre Effekte, wie zum Beispiel die Farbigkeit von Objekten. In der QM können Teilchen im Allgemeinen nicht mehr exakte Werte für physikalische Größen wie die Geschwindigkeit oder den Aufenthaltsort zugeordnet werden, sondern nur noch eine Wahrscheinlichkeitsverteilung dieser Größen. Sie werden daher nicht mehr durch eine Funktion, die jedem Zeitpunkt  $t$  den Ortsvektor des Teilchens  $\vec{x}(t)$  zuordnet, dargestellt. Ein Teilchen ist vielmehr eindeutig durch einen Zustandsvektor  $|\psi\rangle$  in einem Hilbertraum  $\mathcal{H}$  definiert.

Ein Hilbertraum  $\mathcal{H}$  ist dabei ein Vektorraum, der vollständig ist, auf dem also jede Cauchyfolge konvergiert. Außerdem muss auf ihm ein Skalarprodukt  $\langle\phi|\psi\rangle$  für alle  $\phi, \psi \in \mathcal{H}$  definiert sein, welches für die Wahrscheinlichkeitsaussagen der QM wichtig ist.

Meist benutzt man in der Physik als Körper von  $\mathcal{H}$  die komplexen Zahlen  $\mathbb{C}$ . In diesem Fall muss für beliebige  $x, y, z \in \mathcal{H}$  und beliebige  $c \in \mathbb{C}$  das Skalarprodukt  $\langle\cdot|\cdot\rangle : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$  folgende Eigenschaften haben:

**positiv definit** :  $\langle x|x\rangle \geq 0$  und  $\langle x|x\rangle = 0$  gdw.  $x = 0$

**linear im zweiten Glied** :

- $\langle x|y+z\rangle = \langle x|y\rangle + \langle x|z\rangle$
- $\langle x|c \cdot y\rangle = c \cdot \langle x|y\rangle$

**hermitisch** :  $\langle x|y\rangle = \overline{\langle y|x\rangle}$

Mit ihm wird die Norm  $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$  eines Vektors  $\psi \in \mathcal{H}$  definiert. Den Vektor  $\psi$  bezeichnet man als normiert, wenn  $\|\psi\| = 1$  ist.

Durch ein Skalarprodukt auf  $\mathcal{H}$  wird auch der Dualraum  $\mathcal{H}^*$  der linearen Abbildungen  $F : \mathcal{H} \rightarrow \mathbb{C}$  leicht zugänglich. Nach dem Darstellungssatz von Riesz existiert für jede dieser Abbildungen  $F$  genau ein Vektor  $\phi_F \in \mathcal{H}$ , sodass für beliebige  $\psi \in \mathcal{H}$  gilt

$$F(\psi) = \langle\phi_F|\psi\rangle$$

Das Funktional  $F$  bezeichnet man allgemein mit  $\langle\phi_F|$  und jeden Zustandsvektor  $\psi \in \mathcal{H}$  mit  $|\psi\rangle$ , sodass sich das Skalarprodukt als Multiplikation eines Funktionals mit einem Zustandsvektor darstellen lässt. Man nennt  $\langle\phi_F|$  den zu  $|\phi_F\rangle$  dualen Zustandsvektor. Das Skalarprodukt  $\langle\cdot|\cdot\rangle$  findet in der QM eine so häufige Anwendung, dass sich die Notation der so genannten Bra- und Ket-Vektoren ( $\langle\psi|$  und  $|\psi\rangle$ ) für Zustandsvektoren und duale Zustandsvektoren durchgesetzt hat. Leider wirkt sie zu Beginn oft abschreckend, macht die Rechnungen aber sehr bequem.

Eine wichtige Rolle kommt in der Quantentheorie den *linearen Operatoren*  $\hat{A} : \mathcal{H} \rightarrow \mathcal{H}$  zu. Auch hier erweist sich die Bra-Ket-Schreibweise als nützlich. Sei  $|\psi\rangle$  ein normierter

Zustandsvektor, so ist durch  $\hat{A}_\psi = |\psi\rangle \langle\psi|$  ein linearer Operator durch die Vorschrift

$$\hat{A}_\psi |\phi\rangle = |\psi\rangle \langle\psi|\phi\rangle$$

definiert. Wegen  $\hat{A}_\psi^2 = |\psi\rangle \langle\psi|\psi\rangle \langle\psi| = |\psi\rangle \langle\psi| = \hat{A}_\psi$  ist  $\hat{A}_\psi$  außerdem ein Projektionsoperator.

Man definiert den zu einem Operator  $\hat{A}$  eindeutig bestimmten *adjungierten* Operator  $\hat{A}^\dagger$  als den Operator, für den gilt

$$\langle \hat{A}\phi | \psi \rangle = \langle \phi | \hat{A}^\dagger \psi \rangle$$

Er existiert immer, falls  $\hat{A}$  ein linearer Operator ist.

Um von einem Zustandsvektor den dualen Vektor zu bilden, betrachte man, dass für ein komplexes Skalarprodukt und ein  $c \in \mathbb{C}$  gilt  $\langle c \cdot \psi | \phi \rangle = \langle \psi | \bar{c} \cdot \phi \rangle$ . Also gilt  $|\alpha\rangle = c|\psi\rangle \Leftrightarrow \langle \alpha| = \langle \psi| \bar{c}$ , was sich auf beliebige Linearkombinationen forsetzen lässt. Analoges gilt für einen adjungierten Operator, also  $\hat{A} = c\hat{B} \Leftrightarrow \hat{A}^\dagger = \bar{c}\hat{B}^\dagger$ .

Ein linearer Operator  $\hat{A}$ , für den gilt  $\hat{A}^\dagger = \hat{A}$  wird *hermitischer* Operator genannt. Hermitesche Operatoren können demnach von einer Seite des Skalarprodukts auf die andere Seite gezogen werden. Die gleichberechtigtere Schreibweise  $\langle \phi | \hat{A} | \psi \rangle$  verdeutlicht, dass die Operatoren prinzipiell nach beiden Seiten auf  $\langle \phi |$  oder  $|\psi\rangle$  wirken können. Dabei muss bei Anwendung auf den linken Term  $\langle \phi |$  ein nichthermitischer Operator adjungiert werden.

Ein häufige Aufgabe in der Quantenphysik ist das Auffinden der Eigenwerte und Eigenvektoren eines linearen Operators  $\hat{A} : \mathcal{H} \rightarrow \mathcal{H}$ , also die Menge der Zustandsvektoren  $|i\rangle \in \mathcal{H} \setminus \{0\}$ , für die das Anwenden des Operators gerade der Multiplikation mit einer (komplexen) Zahl  $a_i \in \mathbb{C}$  entspricht:

$$\hat{A} |i\rangle = a_i |i\rangle.$$

Im Falle von hermiteschen Operatoren sind die Eigenwerte  $a_i$  immer reell und Eigenvektoren zu verschiedenen Eigenwerten orthogonal. Ist ein Eigenwert  $a$  entartet, existieren also  $g_a > 1$  linear unabhängige Eigenvektoren  $|i_1\rangle, \dots, |i_{g_a}\rangle$  mit demselben Eigenwert  $a$ , so wählt man diese im Allgemeinen so, dass sie ebenfalls orthogonal zueinander sind. Normiert man zudem alle Eigenvektoren, so gilt für beliebige  $|i\rangle, |j\rangle$ :

$$\langle i | j \rangle = \delta_{ij} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{sonst} \end{cases}$$

Da Eigenvektoren der im Folgenden auftretenden linearen Operatoren den entsprechenden Hilbertraum vollständig aufspannen, spricht man von *vollständigen Orthonormalsystemen* (VONS). Jeden Hilbertraumvektor  $|\psi\rangle$  lässt sich also in der Basis  $\{|i\rangle \mid i = 1, 2, \dots\}$  mit den Fourierkoeffizienten  $c_i = \langle \psi | i \rangle$  darstellen. Es folgt

$$|\psi\rangle = \sum_i \langle \psi | i \rangle \cdot |i\rangle = \left( \sum_i |i\rangle \langle i| \right) |\psi\rangle \Rightarrow \sum_i |i\rangle \langle i| = 1$$

**Quantenmechanische Postulate** Die folgenden Postulate sind die Grundlage der Quantenmechanik. Als solche sind sie nicht beweisbar, spiegeln jedoch viele experimentelle Beobachtungen von physikalischen Systemen wider. Sie wurden im Wesentlichen 1932 von John von Neumann formuliert.

1. Der Zustand eines physikalischen Systems zu einem Zeitpunkt  $t_0$  wird durch die Angabe eines zu einem Hilbertraum  $\mathcal{H}$  gehörenden normierten Zustandsvektors  $|\psi(t_0)\rangle$  eindeutig beschrieben.
2. Jede messbare physikalische Größe „A“ ist durch einen im Zustandsraum wirkenden hermiteschen Operator  $\hat{A}$  beschrieben. Dieser Operator ist eine Observable.
3. Resultat der Messung einer physikalischen Größe „A“ kann nur einer der Eigenwerte der entsprechenden Observablen  $\hat{A}$  sein.\*
4. Wenn die physikalische Größe „A“ an einem System im normierten Zustand  $|\psi\rangle$  gemessen wird, ist die Wahrscheinlichkeit  $P(a_n)$ , den nichtentarteten Eigenwert  $a_n$  der entsprechenden Observable  $\hat{A}$  zu erhalten durch  $P(a_n) = |\langle u_n | \psi \rangle|^2$  gegeben, wobei  $|u_n\rangle$  der zum Eigenwert  $a_n$  gehörende normierte Eigenvektor ist.†
5. Wenn die Messung der physikalischen Größe „A“ an einem System im Zustand  $|\psi\rangle$  das Ergebnis  $a_n$  ergibt, ist im nichtentarteten Fall das System unmittelbar nach der Messung im normierten Zustand  $|u_n\rangle$ .‡
6. Die Zeitentwicklung des Zustandsvektors  $|\psi(t)\rangle$  ist gegeben durch die Schrödingergleichung  $\hat{H}(t) |\psi(t)\rangle = i\hbar \frac{d}{dt} |\psi(t)\rangle$  wobei  $\hat{H}(t)$  die der totalen Energie des Systems zugeordnete Observable ist.§

Eine der Grundaufgaben der Physik ist es, den korrekten so genannten Hamiltonoperator  $\hat{H}(t)$  der Schrödingergleichung für ein gegebenes System zu finden.

Der so genannte *Zeitentwicklungsoperator*  $\hat{U}(t, t_0)$  ist der Operator, der angewendet auf einen Zustandsvektor zum Zeitpunkt  $t_0$  den Zustandsvektor zur Zeit  $t$  liefert:  $|\psi(t)\rangle = \hat{U}(t, t_0) |\psi(t_0)\rangle$ . Für ihn gilt der wichtige Satz:

**Satz 2.1.** *Der Zeitentwicklungsoperator  $\hat{U}(t, t_0)$  eines Quantenmechanischen Systems mit Hilbertraum  $\mathcal{H}$ , das isoliert ist, also keiner Messung unterzogen wird, ist unitär. D.h.  $\hat{U}^\dagger = \hat{U}(t, t_0)$  lässt das Skalarprodukt zwischen beliebigen  $|\psi\rangle, |\phi\rangle \in \mathcal{H}$  für beliebige Zeiten  $t, t_0$  invariant:*

$$\langle U\psi | U\phi \rangle = \langle \psi | U^\dagger U \phi \rangle = \langle \psi | \phi \rangle \Leftrightarrow U^\dagger U = 1$$

\*Dies ist der Grund, warum einige physikalische Größen nur diskrete, d.h. „gequantelte“ Werte annehmen können. Da die Operatoren als hermitisch vorausgesetzt wurden sind deren Eigenwerte reell und somit als physikalische Größen interpretierbar.

†Beim entarteten Fall summiert man über alle zum Eigenwert gehörenden entarteten Eigenvektoren  $P(a_n) = \sum_{i=1}^{g_n} |\langle u_n^{(i)} | \psi \rangle|^2$ .

‡Im entarteten Fall ist der Folgezustand die normierte Projektion  $\frac{\hat{P}_n |\psi\rangle}{\sqrt{\langle \psi | \hat{P}_n | \psi \rangle}}$  von  $|\psi\rangle$  auf den mit  $a_n$  assoziierten Eigenunterraum wobei  $\hat{P}_n = \sum_{i=1}^{g_n} |u_n^{(i)}\rangle \langle u_n^{(i)}|$ .

§Die Konstante  $\hbar$  ist definiert als  $\frac{h}{2\pi}$ , wobei  $h$  das berühmte Planck'sche Wirkungsquantum ist. Dies ist eine Naturkonstante mit dem Wert  $6,6260693(11) \cdot 10^{-34}$  Joule Sekunden.

**Beweis.** Dazu schreibt man die Schrödingergleichung in differentieller Form als

$$\hat{H}(t_0) |\psi(t_0)\rangle dt = i\hbar (|\psi(t_0 + dt)\rangle - |\psi(t_0)\rangle) = i\hbar \left( \hat{U}(dt, t_0) |\psi(t_0)\rangle - |\psi(t_0)\rangle \right)$$

Für den Zeitentwicklungsoperator lässt sich also schreiben:

$$i\hbar(\hat{U}(dt, t_0) - 1) = \hat{H}(t_0)dt \implies \hat{U}(dt, t_0) = \frac{1}{i\hbar}\hat{H}(t_0)dt + 1$$

Der Hamiltonoperator ist als Observable der Energie hermitisch ( $\hat{H}^\dagger = \hat{H}$ ) und es folgt:

$$\hat{U}(dt, t_0)\hat{U}^\dagger(dt, t_0) = \left( \frac{1}{i\hbar}\hat{H}(t_0)dt + 1 \right) \left( -\frac{1}{i\hbar}\hat{H}^\dagger(t_0)dt + 1 \right) = 1 + \frac{1}{\hbar^2}\hat{H}^2 dt^2$$

Wegen  $dt^2 = 0$  folgt die Behauptung. ■

Dies heißt, dass sämtliche Operationen, die ein Quantencomputer ausführen kann, unitär sein müssen. Wegen  $\hat{U}^{-1} = \hat{U}^\dagger$  ist der Zeitentwicklungsoperator insbesondere immer invertierbar.

Die Schrödingergleichung hat wie die Eigenwertgleichung jeder Observablen viele Lösungen. Da der Hamiltonoperator linear ist, gilt für zwei Lösungen der Schrödingergleichung

$$i\hbar \frac{d}{dt} |\psi_1(t)\rangle = \hat{H}(t) |\psi_1(t)\rangle \quad \text{und} \quad i\hbar \frac{d}{dt} |\psi_2(t)\rangle = \hat{H}(t) |\psi_2(t)\rangle$$

dass auch jede Linearkombination  $|\phi(t)\rangle = c_1 |\psi_1(t)\rangle + c_2 |\psi_2(t)\rangle$  Lösung der Schrödingergleichung ist:

$$\begin{aligned} i\hbar \frac{d}{dt} |\phi(t)\rangle &= c_1 i\hbar \frac{d}{dt} |\psi_1(t)\rangle + c_2 i\hbar \frac{d}{dt} |\psi_2(t)\rangle \\ &= c_1 \hat{H}(t) |\psi_1(t)\rangle + c_2 \hat{H}(t) |\psi_2(t)\rangle \\ &= \hat{H}(t) (c_1 |\psi_1(t)\rangle + c_2 |\psi_2(t)\rangle) = \hat{H}(t) |\phi(t)\rangle \end{aligned}$$

Dies steht im krassen Widerspruch zur klassischen Physik und wird sich als der entscheidende Vorteil eines Quantencomputers gegenüber einem klassischen Computer erweisen.

## 2.2 Quantenregister

Bis jetzt sind die genannten Definitionen noch sehr abstrakt. Man fragt sich: Wie soll man ein Skalarprodukt zwischen zwei Zuständen berechnen? Wie sehen die Vektoren aus und wie die Operatoren? In jedem Vektorraum und so auch in diesem, kann man erst rechnen, wenn man eine konkrete Basis wählt, in der man alle Vektoren und Operatoren darstellen kann. Man wählt dazu die vollständigen Orthonormalsysteme der Eigenvektoren von Observablen. Das zu betrachtende physikalische System wird ein Quantenregister sein, der Hauptspeicher des Quantencomputers, der durch unitäre Operationen manipuliert werden kann. Die wichtigste Observable ist natürlich die Zahl, die in einem Quantenregister gespeichert ist. In deren Eigenwertbasis werden alle Zustände und Operatoren angegeben.

**Qubit** Die elementare Speichereinheit des Quantencomputers ist das Qubit, das Analogon des Bit auf einem klassischen Computer. Es wird durch ein physikalisches System implementiert, das in zwei Zuständen beobachtbar ist. Man denke beispielsweise an ein Photon, das von einer halbverspiegelten Scheibe reflektiert werden kann oder eben nicht. Die beiden Zustände seien mit  $|0\rangle$  und  $|1\rangle$  bezeichnet. Sie seien normierte Lösungen der Eigenwertgleichung einer Observablen  $A$  zu verschiedenen Eigenwerten  $a_0$  und  $a_1$  und sind damit orthogonal. Wie oben beschrieben, ist auch jede Linearkombination

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$$

ein möglicher Zustand, sodass auch jede Überlagerung von „0“ und „1“ auf Quantencomputern darstellbar ist. Als gültiger Zustand sollte  $|\psi\rangle$  ebenfalls normiert sein, was eine Nebenbedingung für  $c_0$  und  $c_1$  schafft:

$$\|\psi\|^2 = \langle\psi|\psi\rangle = (\langle 0|\bar{c}_0 + \langle 1|\bar{c}_1) (c_0 |0\rangle + c_1 |1\rangle) = |c_0|^2 + |c_1|^2 = 1$$

Will man nun wissen, mit welcher Wahrscheinlichkeit im Zustand  $|\psi\rangle$  „0“ oder „1“ (bzw. die entsprechenden Eigenwerte  $a_0$  oder  $a_1$ ) gemessen werden, wendet man Postulat 4 an und erhält:

$$P(a_0) = |\langle 0|\psi\rangle|^2 = |c_0|^2 \text{ und } P(a_1) = |\langle 1|\psi\rangle|^2 = |c_1|^2$$

Die eigentliche Stärke des Quantencomputers zeigt sich nun in der Verwendung von mehreren Qubits, also einem  $n$ -Qubit Register. Der Hilbertraum  $\mathcal{H}_n$  des  $n$ -Qubit Registers ergibt sich als  $n$ -faches Tensorprodukt der Ein-Qubit Hilberträume:  $\mathcal{H}_n = \mathcal{H} \otimes \dots \otimes \mathcal{H}$ . Das  $n$ -Qubit Register kann damit eine Überlagerung aller Zahlen  $i$  von 0 bis  $2^n - 1$  darstellen:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle \text{ mit } \sum_{i=0}^{2^n-1} |c_i|^2 = 1$$

Die Vorfaktoren  $c_i$  werden auch als *Amplituden* bezeichnet. Dabei bezeichnen die Basiszustände  $|i\rangle$  die Qubit-Darstellung der Zahl  $i$ . Also z.B. für  $i = 7$  und  $n = 4$ :

$$|7\rangle = |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |1\rangle \in \mathcal{H}_4$$

In Kurznotation schreibt man auch  $|0\rangle |1\rangle |1\rangle |1\rangle$  oder einfach  $|0111\rangle$ . Das Skalarprodukt zwischen zwei Vektoren  $|k\rangle = |k_n\rangle \otimes |k_{n-1}\rangle \otimes \dots \otimes |k_1\rangle$  und  $|l\rangle = |l_n\rangle \otimes |l_{n-1}\rangle \otimes \dots \otimes |l_1\rangle$  des  $n$ -fachen Produktraums  $\mathcal{H} \otimes \dots \otimes \mathcal{H}$  ist definiert als Produkt der Einzelskalarprodukte:

$$\langle k|l\rangle = \langle k_n|l_n\rangle \dots \langle k_1|l_1\rangle$$

Damit sind auch die neuen  $2^n$  Basiszustände wieder orthonormal. Die Wahrscheinlichkeit die Zahl  $i$  bzw. den  $i$ -ten Eigenwert zu messen beträgt nach Postulat 4:

$$P(a_i) = |\langle i|\psi\rangle|^2 = \left| \sum_{j=0}^{2^n-1} c_j \underbrace{\langle i|j\rangle}_{=\delta_{ij}} \right|^2 = |c_i|^2$$

In dieser Darstellung können nun Skalarprodukt, Vektoren und Operatoren konkretisiert werden. Dazu stellt man  $|\psi\rangle$  als den Spaltenvektor

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2^n-1} \end{pmatrix}$$

dar. Das Skalarprodukt zwischen  $|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$  und  $|\phi\rangle = \sum_{i=0}^{2^n-1} d_i |i\rangle$  ergibt sich zu

$$\langle \psi | \phi \rangle = \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \overline{c_i} d_j \underbrace{\langle i | j \rangle}_{=\delta_{ij}} = \sum_{i=0}^{2^n-1} \overline{c_i} d_i$$

Schreibt man den dualen Vektor als den konjugierten Zeilenvektor

$$\langle \psi | = (\overline{c_0} \quad \overline{c_1} \quad \dots \quad \overline{c_{2^n-1}}) = |\psi\rangle^\dagger$$

so ergibt sich das Skalarprodukt als normale Matrixmultiplikation eines Zeilenvektors mit einem Spaltenvektor. Da unsere Basiszustände  $|i\rangle$  mit  $i = 0, \dots, 2^n - 1$  ein VONS des Hilbertraums bilden ist die Summe aller Projektionen auf die Basisvektoren gerade die Identität  $\sum_{i=0}^{2^n-1} |i\rangle \langle i| = 1$ . Damit lässt sich jede Operatorgleichung

$$\hat{A} |\phi\rangle = |\psi\rangle$$

durch Anwendung von  $\langle i|$  von links und Einschieben von  $\sum_{j=0}^{2^n-1} |j\rangle \langle j|$  zwischen  $\hat{A}$  und  $|\phi\rangle$

$$\sum_{j=0}^{2^n-1} \langle i | \hat{A} |j\rangle \langle j | \phi \rangle = \langle i | \psi \rangle$$

als Matrixgleichung auffassen:

$$\sum_{j=0}^{2^n-1} A_{ij} d_j = c_i \quad \text{mit} \quad A_{ij} := \langle i | \hat{A} |j\rangle$$

Ist  $\hat{A}$  ein unitärer Operator, so gilt:

$$(A^{-1})_{ij} = \langle i | \hat{A}^{-1} |j\rangle = \langle i | \hat{A}^\dagger |j\rangle = \langle \hat{A} i | j \rangle = \overline{\langle j | \hat{A} i \rangle} = (A^\dagger)_{ij}$$

Wobei das letzte  $\dagger$  sich auf die Adjunktion der Matrix bezieht. Die Matrixdarstellung eines unitären Operators ist also auch unitär.

## 2.3 No-Cloning Theorem

Eine recht problematische Konsequenz der Quantenmechanik ist die Unmöglichkeit, einen unbekanntem Zustand eines Systems auf ein anderes zu übertragen. Dies würde nur mit nichtunitären Zeitenwicklungsoperatoren gelingen. Sei  $|k\rangle \in \mathcal{H}$  ein unbekannter

zu kopierender Zustand. Um diesen auf einen anderen (normierten) Zustand  $|\psi\rangle \in \mathcal{H}$  zu kopieren, müsste ein unitärer Operator  $U$  auf  $\mathcal{H} \otimes \mathcal{H}$  existieren, mit

$$U |k\rangle \otimes |\psi\rangle = |k\rangle \otimes |k\rangle$$

Um zu zeigen, dass ein solcher Operator das Skalarprodukt nicht invariant lassen kann, wählt man zwei zu kopierende Zustände  $|k_1\rangle$  und  $|k_2\rangle$ , wobei  $\langle k_1 | k_2 \rangle$  nur nicht 0 oder 1 sein soll. Dann gilt:

$$\begin{aligned} U |k_1\rangle |\psi\rangle &= |k_1\rangle |k_1\rangle \\ U |k_2\rangle |\psi\rangle &= |k_2\rangle |k_2\rangle \\ \Rightarrow \langle \psi | \langle k_1 | \underbrace{U^\dagger U}_{=1} |k_2\rangle |\psi\rangle &= (\langle k_1 | \langle k_1 |) (|k_2\rangle |k_2\rangle) \\ \Rightarrow \underbrace{\langle \psi | \psi \rangle}_{=1} \langle k_1 | k_2 \rangle &= \langle k_1 | k_2 \rangle \langle k_1 | k_2 \rangle \\ \Rightarrow \langle k_1 | k_2 \rangle &= \langle k_1 | k_2 \rangle^2 \end{aligned}$$

Dies ist aber nur möglich wenn  $\langle k_1 | k_2 \rangle$  gleich 0 oder 1 ist, was ausgeschlossen wurde. Bei der „Programmierung“ von Quantencomputern sieht man sich also mit den folgenden Problemen konfrontiert, die sich auf klassischen Computern nicht ergeben:

- Es ist unmöglich den Registereintrag eines Quantencomputers zu kopieren, eine Möglichkeit von der man in klassischen Programmen extrem häufig Gebrauch macht.
- Desweiteren muss jede Quantenoperation invertierbar sein. Klassische Operationen wie das logische „UND“ oder die Addition zweier Zahlen sind *nicht* invertierbar.
- Ein weiteres Problem des Quantencomputers ist, dass sein Zustand als Überlagerung nicht „auslesbar“ ist, da dies die Möglichkeit des Kopierens eines unbekanntem Zustands nach sich ziehen würde. Die Messungen können nur Aufschluss über das Betragsquadrat der Amplituden liefern.

Dennoch kann ein Quantencomputer dank seiner Möglichkeit, Berechnungen für viele Zahlen gleichzeitig durchzuführen, einige Probleme exponentiell schneller lösen als jeder bekannte Algorithmus auf klassischen Computern. Dazu ist jedoch eine völlig andere Art von Programmierung nötig.

## 3 Quanten-Komplexitätstheorie

### 3.1 Turingmaschine und Quanten-Turingmaschine

Wie in der Klassischen Komplexitätstheorie benötigt man auch für die Quanten-Komplexitätstheorie ein Rechenmodell, also eine Quanten-Turingmaschine (QTM). Um zu sehen, dass dieses Rechenmodell nicht stark von einer probabilistischen Turingmaschine abweicht, sei hier noch einmal an die Definition der klassischen Turingmaschine erinnert.

**Definition 3.1 (deterministische Turingmaschine).** Eine deterministische Turingmaschine (DTM) ist ein Quadrupel  $M = (Q, \Sigma, \Gamma, \delta)$ . Dabei ist

- $Q$  eine endliche Menge von Zuständen mit einem ausgezeichneten Anfangszustand  $q_0$  und einem Endzustand  $q_f \neq q_0$
- $\Sigma$  eine endliche Menge von Symbolen, in der das Blank-Symbol  $\sqcup$  nicht enthalten ist
- $\Gamma$  das Arbeitsalphabet mit  $\Sigma \cup \{\sqcup\} \subseteq \Gamma$
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$  die Überföhrungsfunktion

Die Turingmaschine besteht aus einem zweiseitig unendlichem Band, dessen Felder mit Zahlen aus  $\mathbb{Z}$  indiziert seien, und einem Lese/Schreib-Kopf, der sich entlang dieses Bandes bewegt.

Die Konfiguration einer DTM beschreibt eindeutig den Bandinhalt, die Kopfposition und den aktuellen Zustand. Die Folgekonfiguration ergibt sich durch Anwendung der Überföhrungsfunktion: Dem aktuell gelesenen Zeichen und dem aktuellen Zustand wird ein neues Zeichen, welches die Maschine auf das Band schreibt, ein Folgezustand und eine Kopfbewegung ( $L$  für eine Zelle nach links und  $R$  für eine Zelle nach rechts) zugeordnet. Durch  $K \rightarrow_M K'$  sei im Folgenden ausgedrückt, dass die DTM  $M$  in der Konfiguration  $K$  in einem Schritt in die Folgekonfiguration  $K'$  übergeht.

In der Anfangskonfiguration steht der Kopf auf der 0. Zelle, auf dem Band steht auf Position  $0, 1, 2, \dots$  die Eingabe  $x \in \Sigma^*$ . Die Maschine ist im Anfangszustand  $q_0$ .

Die DTM hält bei Eingabe  $x$ , wenn sie den Endzustand  $q_f$  erreicht. Die Laufzeit bei Eingabe  $x$  ist dann gerade die Anzahl der Konfigurationenübergänge. Wenn die Maschine hält, wird als Ausgabe die größte Zeichenkette ohne  $\sqcup$  bezeichnet, die das Zeichen auf Zelle 0 enthält.

**Bemerkung 3.2.** Es gibt viele alternative Definitionen einer Turingmaschine, welche z. B. ein einseitiges Band, ein Startsymbol und die Möglichkeit des Verharrens des Lese/Schreib-Kopfes auf einem Feld beinhalten. Diese unterscheiden sich aber nicht in ihrer Mächtigkeit. Auch eine Erhöhung der Anzahl der Bänder bringt maximal eine quadratische Beschleunigung der Berechnung. Aus der gegebenen Definition lässt sich jedoch besonders leicht eine Quanten-Turingmaschine ableiten, welche die wichtige Reservibilitätsbedingung erfüllen kann.

Nun wird der Übergang zu einer Quanten-Turingmaschine (QTM) vollzogen. In Abschnitt 2.1 wurde erklärt, dass sich ein quantenmechanisches System in einer Überlagerung von Zuständen, die Lösungen der Schrödingergleichung sind, befinden kann. Ähnlich zu einer nichtdeterministischen Turingmaschine oder einer probabilistischen Turingmaschine kann also auch eine QTM eine Menge von Folgekonfigurationen haben, die sich aus einer endlichen Menge von Anweisungen in einem Rechenschritt ergeben. Jeder Anweisung wird eine Amplitude  $c \in \mathbb{C}$  zugeordnet. Diese muss jedoch effizient berechenbar sein. Die Menge der effizient berechenbaren komplexen Zahlen  $\tilde{\mathbb{C}} \subset \mathbb{C}$  ist wie folgt definiert:

**Definition 3.3.**  $\tilde{\mathbb{C}}$  sei die Menge aller  $c \in \mathbb{C}$  deren  $n$ -tes Bit des Real- und Imaginärteils in Binärdarstellung in polynomieller Zeit in  $n$  deterministisch berechnet werden kann.

**Definition 3.4 (Quanten-Turingmaschine).** Eine Quanten-Turingmaschine (QTM)  $M$  ist definiert wie eine DTM mit einer geänderten Überföhrungsfunktion

$$\delta : Q \times \Gamma \mapsto \tilde{\mathbb{C}}^{\Gamma \times Q \times \{L,R\}}$$

die jeder Konfiguration  $K$  eine endliche Menge von Folgekonfigurationen  $\{K'_1, K'_2, \dots\}$  mit jeweils einer Amplitude  $c_{K \rightarrow MK'_i} \in \tilde{\mathbb{C}}$  zuordnet.

Jeder Konfiguration  $K$  kann man genau einen normierten Zustandsvektor in einem Hilbertraum  $\mathcal{H}_M$  zuordnen, welchen man Konfigurationsvektor nennt. Unterschiedliche Konfigurationsvektoren seien orthogonal zueinander. Der durch sie aufgespannte Raum  $\mathcal{K} \subset \mathcal{H}$  sei mit Zustandsraum von  $M$  bezeichnet.<sup>¶</sup> Die Maschine definiert einen linearen Operator  $\hat{U}_M$  auf  $\mathcal{K}$ , den Zeitentwicklungsoperator.  $\hat{U}_M$  wirkt wie folgt auf einen Zustandsvektor  $|\Psi\rangle = \sum_i c_i |K_i\rangle$ :

$$U_M |\Psi\rangle = \sum_{i,j} c_i \cdot c_{K_i \rightarrow MK_j} |K_j\rangle$$

Die Überföhrungsfunktion muss so gewöhlt werden, dass  $U_M$  unitär ist.

Die Maschine arbeitet durch wiederholtes anwenden von  $U_M$  auf ihren aktuellen Zustandsvektor und hält erst, wenn ihr Zustandsvektor nur aus einer Überlagerung von Endkonfigurationsvektoren besteht, also von Konfigurationsvektoren, die eine Konfiguration im Endzustand  $q_f$  darstellen.

Für eine Ausgabe  $s \in \Sigma^*$  sei  $\mathcal{K}_s$  die Menge aller Konfigurationsvektoren mit Ausgabe  $s$ , dann ist die Wahrscheinlichkeit, die Bandinschrift  $s$  im Endzustand  $|\Psi_F\rangle$  zu messen gegeben durch:

$$\text{Prob}(s) = \sum_{K \in \mathcal{K}_s} |\langle K | \Psi_F \rangle|^2$$

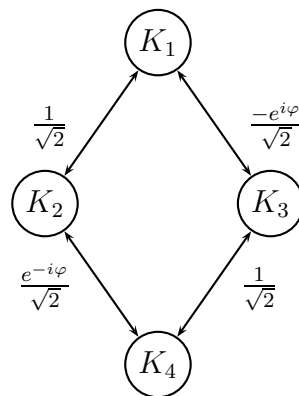
Der Unterschied in den Definitionen einer QTM und einer probabilistischen Turingmaschine (PTM) ist nicht besonders groß. Für eine PTM  $M$  gibt es zu jeder Konfiguration  $K$  eine endliche Menge von Folgekonfigurationen  $\{K'_1, K'_2, \dots\}$  denen jeweils die

<sup>¶</sup>Leider wird der Begriff *Zustand* hier in zwei Kontexten benutzt: als Element von  $Q$  und in den Begriffen Zustandsvektor und Zustandsraum. Ein Zustandsvektor ist aber *kein* Vektor von Zuständen, sondern ein Hilbertraumvektor, und der Zustandsraum ist *keine* Menge von Zuständen, sondern ein Unterraum des Hilbertraumes!

gleiche Übergangswahrscheinlichkeit  $p_{K \rightarrow_M K'_1} = p_{K \rightarrow_M K'_2} = \dots$  zugeordnet ist. Die Wahrscheinlichkeit für eine Berechnung  $\alpha = (K_1, K_2, \dots, K_m)$  ist gegeben durch

$$\text{Prob}(\alpha) = p_{K_1 \rightarrow_M K_2} \cdot p_{K_2 \rightarrow_M K_3} \cdots p_{K_{m-1} \rightarrow_M K_m}$$

Ähnlich multiplizieren sich bei einer QTM die Übergangsamplituden. Dass diese aus dem Bereich der komplexen Zahlen  $\tilde{\mathbb{C}}$  stammen, ist nicht von großem Vorteil. Wie Adleman, DeMarras und Huang zeigen konnten, stellt es keine Einschränkung für die Komplexitätsklasse BQP dar (welche später noch genauer betrachtet wird), wenn man QTM's betrachtet, deren Übergangsamplituden aus der Menge  $\{-1, -4/5, -3/5, 0, 3/5, 4/5, 1\}$  kommen [ADH]. Der entscheidende Vorteil einer QTM ist, dass sich nicht, wie im Fall einer PTM die Wahrscheinlichkeiten der Berechnungspfade, die zu einer bestimmten Ausgabe führen, addieren. Vielmehr addieren sich die *Amplituden* der Berechnungspfade und die Wahrscheinlichkeit einer bestimmten Ausgabe ergibt sich aus dem Betragsquadrat der Summe dieser Amplituden. Es kann zu so genannten *Interferenzen* mererer Berechnungspfade kommen, die die Wahrscheinlichkeit für eine Ausgabe sowohl verstärken, als auch abschwächen kann. Dies soll an einem kleinen Beispiel illustriert werden. Der folgende Graph stellt eine kleine QTM  $M_q$  bzw. PTM  $M_p$  dar. Dabei sei  $K_1$  jeweils die Startkonfiguration. Die Übergangsamplituden von  $M_q$  sind an den Kanten dargestellt und gelten für beide Richtungen.<sup>||</sup> Die Übergangswahrscheinlichkeiten der entsprechenden PTM  $M_p$  ergeben sich an jeder Kante zu  $\frac{1}{2}$ .



Die Entwicklung der PTM  $M_p$  für zwei Schritte ergibt sich zu:

$$K_1 \rightarrow_{M_p} \{K_2, K_3\} \rightarrow_{M_p} \{K_1, K_4\}$$

Die unitäre Entwicklung für zwei Schritte der QTM  $M_q$  verläuft wie folgt:

$$|K_1\rangle \rightarrow_{M_q} \frac{1}{\sqrt{2}} |K_2\rangle - \frac{e^{i\phi}}{\sqrt{2}} |K_3\rangle \rightarrow_{M_q} \frac{1}{2} (1 + e^{2i\phi}) |K_1\rangle + \frac{1}{2} (e^{-i\phi} - e^{i\phi}) |K_4\rangle$$

Es soll die Wahrscheinlichkeit bestimmt werden, die Maschine nach zwei Rechenschritten im Zustand  $K_4$  vorzufinden. Für die PTM  $M_p$  ergibt sich

$$\text{Prob}_{M_p}(K_4) = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$$

---

<sup>||</sup>Übergangswahrscheinlichkeit von unten nach oben sind wegen der Reversibilitätsbedingung unvermeidlich.

Im Gegensatz dazu ergibt sich für die QTM  $P_q$

$$\text{Prob}_{M_q}(K_4) = \left| \frac{1}{2}(e^{-i\varphi} - e^{i\varphi}) \right|^2 = |-\sin \varphi|^2 = \sin^2 \varphi$$

Je nach der Phase der Amplituden  $\varphi$  kann  $|K_4\rangle$  mit Wahrscheinlichkeit 0 bis 1 gemessen werden. Die beiden möglichen Pfade zu  $|K_4\rangle$  können also im Gegensatz zur PTM  $M_p$  weitreichend miteinander Wechselwirken.

**Bemerkung 3.5.** *Die Halte-Bedingung einer QTM scheint im Widerspruch zu den Quantenmechanischen Postulaten (2.1) zu stehen. In der physikalischen Realität muss man feststellen, wann eine Maschine im Endzustand ist, um dann ihren Bandinhalt zu lesen. Jede Messung des Zustands führt zum Wellenfunktionskollaps. Der Zustandsvektor der Maschine würde nach der Messung nur noch aus einer Überlagerung von Konfigurationsvektoren bestehen, die den gemessenen Zustand darstellen.*

*Die Lösung des Problems besteht darin, ein zusätzliches Qubit als Halte-Flag zu benutzen, welches mit Erreichen des Endzustandes  $q_f$  von  $|0\rangle$  auf  $|1\rangle$  gesetzt wird. Einmal auf  $|1\rangle$  gesetzt, arbeitet die Maschine weiter, ohne jedoch den Bandinhalt oder das Halte-Flag zu verändern. Nur die Kopfposition und der Zustand kann sich ändern. Außerdem wird in jedem Rechenschritt das Halteflag gemessen. Wird dabei der Zustand  $|1\rangle$  gemessen, endet die Berechnung und der Bandinhalt kann ebenfalls gemessen werden. Natürlich führt auch dies zu einem Wellenfunktionskollaps: Der Zustandsvektor kann nur aus einer Überlagerung von Konfigurationsvektoren bestehen, die auf Pfaden erreicht wurden, in denen der Endzustand enthalten war. Ozawa konnte jedoch zeigen, dass die Wahrscheinlichkeitsverteilung der am Ende gemessenen Bandinhalte davon unberührt bleibt [MO]. In der Praxis kann also eine quantenmechanische Berechnung früher abbrechen. Aber wie auch bei probabilistischen Turingmaschinen zählt der längste Berechnungspfad, was auf die gegebene Haltebedingung führt.*

## 3.2 Die Komplexitätsklassen EQP und BQP

Nun werden die zu P und BPP analogen Komplexitätsklassen EQP und BQP definiert. Da die folgenden QTM's Sprachen entscheiden, sollen sie ein Wort akzeptieren, indem sie 1 ausgeben und verwerfen indem sie 0 ausgeben.

**Definition 3.6 (EQP - error-free quantum polynomial time).** *Eine Sprache  $L \subseteq \Sigma^*$  ist in EQP wenn es eine QTM  $M$  und ein Polynom  $p$  gibt, sodass für ein  $x \in \Sigma^*$  die Maschine  $M$  nach  $p(|x|)$  Rechenschritten hält und falls  $x \in L$  immer akzeptiert und sonst immer verwirft.*

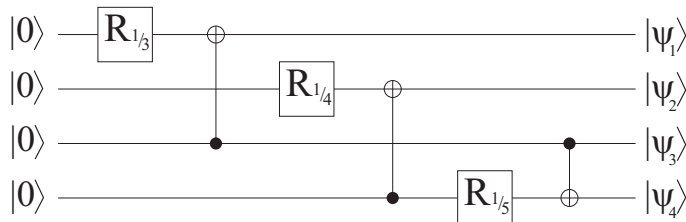
**Definition 3.7 (BQP - boundet error quantum polynomial time).** *Eine Sprache  $L \subseteq \Sigma^*$  ist in BQP wenn es eine QTM  $M$  und ein Polynom  $p$  gibt, sodass für ein  $x \in \Sigma^*$  die Maschine  $M$  nach  $p(|x|)$  Rechenschritten hält und falls  $x \in L$  mit einer Wahrscheinlichkeit größer  $2/3$  akzeptiert und falls  $x \notin L$  mit einer Wahrscheinlichkeit von mindestens  $2/3$  verwirft.*

**Bemerkung 3.8.** *Ein der realistischen Implementierung von Quantencomputern angepasstes Rechenmodell besteht aus einem  $n$ -Qubit Register, auf welchem in jedem Schritt*

ein Operator aus einem endlichen Satz von unitären ein- und zwei-Qubit Operatoren ausgeführt werden kann. In folgender Tabelle ist die Form dieser Operatoren mit ihren Wirkungen auf die Basiszustände und ihren Schaltsymbolen dargestellt. Dabei ist  $\theta \in \tilde{\mathbb{C}} \cap [0, 1)$ , also effizient berechenbar.

Operation	Abbildung	Schaltsymbol
Kontrollierte Negation CNOT (engl. controlled Not)	$ 00\rangle \mapsto  00\rangle$ $ 01\rangle \mapsto  01\rangle$ $ 10\rangle \mapsto  11\rangle$ $ 11\rangle \mapsto  10\rangle$	
Phasenschieber $P_\theta$	$ 0\rangle \mapsto  0\rangle$ $ 1\rangle \mapsto e^{2\pi i \theta}  1\rangle$	
Rotation $R_\theta$	$ 0\rangle \mapsto \cos(2\pi\theta)  0\rangle - \sin(2\pi\theta)  1\rangle$ $ 1\rangle \mapsto \sin(2\pi\theta)  0\rangle + \cos(2\pi\theta)  1\rangle$	

Ein Algorithmus kann dann als Hintereinanderausführung dieser elementaren Operationen als ein Quantenschaltkreis zum Beispiel dieser Form angegeben werden:



Existiert ein endlicher Satz von Operatoren  $G \subset \{CNOT, P_\theta, R_\theta \mid \theta \in \tilde{\mathbb{C}}\}$  und eine deterministische Turingmaschine, die für jede Eingabelänge  $n$  die Codierung eines Gatters  $C_n$  mit Operatoren aus  $G$  in polynomieller Zeit  $p(n)$  berechnet, spricht man von einer endlich polynomiell erzeugten Quantenschaltkreis-Familie  $\mathcal{C} = \{C_n\}$ .

Nishimura und Ozawa haben gezeigt, dass jede QTM mit polynomieller Laufzeit durch eine endlich polynomiell erzeugte Quantenschaltkreis-Familie perfekt simuliert werden kann, und umgekehrt [NO]. Die beiden Modelle sind also äquivalent.

Die hier behandelten Algorithmen geben nacheinander die benötigten unitären Transformationen an, und nutzen daher implizit das Rechenmodell des Quantengatters und nicht das einer QTM.

Die Unitaritätsbedingung der Zeitentwicklung einer QTM stellt eine starke Einschränkung dar. Für eine deterministische Turingmaschine (die ja im Allgemeinen nicht reversibel ist) kann nicht direkt eine QTM angegeben werden, die dieselbe Sprache entscheidet. Charles Bennet konnte jedoch zeigen, dass jede deterministische Turingmaschine effizient in eine reversible Turingmaschine umgewandelt werden kann, indem sie eine Historie der Berechnung speichert [CB]. Übertragen auf eine QTM ist jede Konfiguration aus maximal einer Vorgängerkonfiguration erreichbar und hat genau eine Nachfolgekonfiguration. Der entsprechende Zeitentwicklungsoperator führt also eine Basispermutation aus, welche immer unitär ist. Daher folgt [BV]:

### Theorem 3.9. $P \subseteq EQP$

Mit dieser Technik kann man auch zeigen, dass  $BPP \subseteq BQP$  gilt. Dazu simuliert man die probabilistische und durch ein Polynom  $p(n)$  zeitbeschränkte Turingmaschine, indem man deren Berechnungspfade als einen String  $y \in \{0, 1\}^{p(|x|)}$  kodiert. Die QTM erzeugt zu Beginn eine Überlagerung aller  $y \in \{0, 1\}^{p(|x|)}$  und führt überlagert jede der  $2^{p(|x|)}$  deterministischen Berechnungen aus, welche man ja in eine effiziente reversible Berechnung umformen kann. Das Akzeptanzkriterium der probabilistischen Turingmaschine überträgt sich auf die QTM. Damit folgt [BV]:

### Theorem 3.10. $BPP \subseteq BQP$

Da die Klasse BPP als die Menge der effizient entscheidbaren Sprachen angesehen wird, würde sich dies im Angesicht von Quantencomputern auf die Sprachen in BQP übertragen. Daher ist es sehr interessant, eine möglichst kleine Obermenge für BQP zu finden. Das beste bekannte Ergebnis dahingehend ist  $BQP \subseteq PP$ . Eine leichter nachvollziehbare Inklusion ist  $BQP \subseteq PSPACE$ , welche im Folgenden begründet werden soll. Dazu muss eine  $p(n)$ -zeitbeschränkte QTM  $M$  die eine Sprache in BQP entscheidet mit polynomiellen Platzaufwand simuliert werden, indem für eine Eingabe  $x$  die Akzeptanzwahrscheinlichkeit von  $M$  berechnet wird und akzeptiert wird, falls diese größer als  $2/3$  ist. Wie schon beschrieben, kann man davon ausgehen, dass die Übergangsamplituden aus der Menge  $\{-1, -4/5, -3/5, 0, 3/5, 4/5, 1\}$  gewählt sind und damit in polynomiellen Platz darstellbar sind. Nun addiert man die Betragsquadrate der Amplituden der erreichbaren akzeptierenden Endkonfigurationen, von denen es nur endlich viele gibt, da der Schreib-/Lesekopf von Zelle 0 aus maximal  $p(n)$  Zellen erreicht haben kann. Dazu sucht man jede dieser Konfigurationen, die sich in polynomiellen Platz kodieren lassen, mit Tiefensuche von der Startkonfiguration aus und multipliziert dabei ebenfalls mit polynomiellen Platzaufwand die einzelnen Übergangsamplituden zur Gesamtamplitude für die Endkonfiguration. Ist die Summe der Betragsquadrate größer  $2/3$  wird die Eingabe akzeptiert und ansonsten verworfen. Damit folgt [BV]:

### Theorem 3.11. $BQP \subseteq PSPACE$

Dieses Ergebnis zeigt auch, dass es nur mit weiteren Durchbrüchen in der klassischen Komplexitätstheorie möglich sein wird zu zeigen, dass  $BQP \neq BPP$  gilt. Dies würde  $BPP \neq PSPACE$  nach sich ziehen, was bisher nicht bewiesen werden konnte.

## 3.3 Orakeltechniken in der Quanten-Komplexitätstheorie

Es soll nun ein Argument angeführt werden, warum es wahrscheinlich ist, dass Quantencomputer mächtiger sind als klassische Computer. Dazu wird ein Orakelproblem definiert, welches von Quantencomputern in polynomiellem Aufwand berechnet werden kann und für probabilistische Turingmaschinen nur in exponentiellem Aufwand lösbar ist.

### Problem 3.12

**gegeben:** Ein  $n \in \mathbb{N}$  und ein Zufallsorakel  $O$  welches für jedes  $n$  eine Funktion  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  berechnet.

**promise:** Für die Konstruktion des Orakels  $O$  wird eine zufällige  $n$ -Bitfolge  $s_O(n) \neq 0\dots 0$  und ein Zufallsbit  $b_O(n)$  gewählt. Falls  $b_O(n) = 0$  ist, ist  $f$  eine gleichverteilt zufällig gewählte, bijektive Funktion. Falls  $b_O(n) = 1$  ist, ist  $f$  eine gleichverteilt zufällig gewählte Funktion mit folgender Eigenschaft: Für alle  $x, y \in \{0, 1\}^n$  gilt  $f(x) = f(y) \Leftrightarrow y = x \oplus s_O(n)$ . Hierbei bezeichnet  $\oplus$  die bitweise XOR-Operation

**gesucht:** Mithilfe von Orakelanfragen an  $O$  soll  $b_O(n)$  bestimmt werden

Simon konnte zeigen, dass keine probabilistische Turingmaschine  $b_O(n)$  mit höherer Wahrscheinlichkeit als  $1/2 + 2^{-n/2}$  (außer für endlich viele  $n$ ) mit weniger als  $2^{n/4}$  Orakelanfragen bestimmen kann [DS]. Für die Sprache  $L_O = \{1^n \mid b_O(n) = 1\}$  gilt also  $L_O \notin BPP^O$ . Jedoch existiert eine QTM, die mit einer Orakelanfrage und in  $n$  polynomieller Zeit  $s_O(n)$  und damit  $b_O(n)$  bestimmen kann. In Abschnitt 6.3.1 wird gezeigt, dass sich dies auf eine Instanz des abelschen HSP zurückführen lässt, für das im zugehörigen Kapitel ein allgemeiner Lösungsalgorithmus angegeben wird. Relativiert zum Orakel  $O$  gilt also  $BQP \neq BPP$ .

Man kann sich nun fragen, wie zwingend die Argumentation mittels Orakeltechnik ist. Immerhin zeigte Adi Shamir, dass  $IP = PSPACE$  [AS], obwohl relativ zu fast allen Orakeln  $IP \neq PSPACE$  [CCG] gilt. Allerdings wird das Orakel hier nicht als Hilfestellung zur Lösung eines Problems verwendet, sondern ist selbst Bestandteil des Problems, indem es als Blackbox die zu analysierende Funktion berechnet. In einer realen Rechenmaschine wäre das Orakel  $O$  eine Subroutine die effizient die Funktion  $f$  berechnet, ohne dass man der Routine effizient ansehen kann, welche Eigenschaften die berechnete Funktion besitzt. Dass man einem polynomiell zeitbeschränkten Algorithmus im allgemeinen nicht effizient ansehen kann, welche Klasse von Funktionen er berechnet, ist ähnlich plausibel wie die Annahme, dass  $P \neq NP$  oder dass Einwegfunktionen existieren.

Eine weitere Reihe von wichtigen Ergebnissen für die Einordnung der Klasse BQP lieferten Fortnow und Rogers [FR].

- Für beliebige Sprachen  $L \in BQP$  gilt  $PP^L = PP$ .

Eine probabilistische Turingmaschine, die eine Sprache mit einer Fehlerwahrscheinlichkeit kleiner als  $1/2$  entscheiden muss, wird also nicht mächtiger, wenn ihr ein Orakel, welches eine BQP-Sprache in einem Schritt entscheidet, zur Verfügung steht. Dies impliziert und ist eine stärkere Aussage als  $BQP \subseteq PP$ .

- Es existiert ein Orakel relativ zu dem  $P = BQP$  gilt und die Polynomialzeithierarchie echt ist.

Um zu zeigen, dass Quantencomputer echt mächtiger sind als klassische Computer, sind also nicht-relativierbare Beweistechniken vonnöten, da ein Orakel, relativ zu dem  $P$  und BQP identisch sind, nicht einmal notwendiger Weise zu einem Kollaps der Polynomialzeithierarchie führt. Von dieser wird vermutet, dass sie zumindest nicht auf niedriger Stufe kollabiert.

## 4 Darstellungstheorie

### 4.1 Grundlegende Definitionen der Gruppentheorie

In diesem Abschnitt soll dem mit Gruppentheorie unvertrauten Leser ein kurzer Überblick über einige grundlegenden Definitionen und Notationen der Gruppentheorie gegeben werden. Sie werden im Anschluss für die Behandlung der Darstellungstheorie benötigt.

**Definition 4.1.** Das Paar  $(G, \circ)$  mit einer Menge  $G$  und einer zweistelligen Verknüpfung  $\circ : G \times G \rightarrow G$  heißt Gruppe, wenn folgende Axiome erfüllt sind:

**Abgeschlossenheit:** Für alle Gruppenelemente  $g, h \in G$  gilt:  $g \circ h \in G$

**Assoziativität:** Für alle Gruppenelemente  $g, h$  und  $k$  gilt:  $(g \circ h) \circ k = g \circ (h \circ k)$

**Neutrales Element:** Es gibt ein neutrales Element  $e \in G$ , mit dem für alle Gruppenelemente  $g$  gilt:  $g \circ e = e \circ g = g$

**Inverses Element:** Zu jedem Gruppenelement  $g$  existiert ein Element  $g^{-1}$  mit  $g \circ g^{-1} = g^{-1} \circ g = e$

Eine Gruppe  $(G, \circ)$  heißt abelsch oder kommutativ, wenn die Verknüpfung  $\circ$  symmetrisch ist, d.h. wenn zusätzlich das folgende Axiom erfüllt ist:

**Kommutativität:** Für alle Gruppenelemente  $g$  und  $h$  gilt  $g \circ h = h \circ g$ .

Die Kardinalität der Gruppe  $G$  wird in dieser Arbeit mit  $\|G\|$  bezeichnet.

Man betrachte für eine endliche Menge  $G$  und ein  $g \in G$  die Menge  $\{g, g^2, g^3, \dots\}$ . Da diese Menge selbst endlich sein muss, existieren  $i, j \geq 1$  mit  $i < j$ , sodass  $g^i = g^j$ . Also existiert ein  $n = j - i$  mit  $g^n = e$ . Das kleinste  $n \geq 1$  mit dieser Eigenschaft nennt man die *Ordnung*  $\text{ord}(g)$  von  $g$ . Mit  $\langle g \rangle$  bezeichnet man die von  $g$  erzeugte Untergruppe  $\{e, g, g^2, \dots, g^{\text{ord}(g)-1}\}$ . Da für beliebige ganzzahlige  $k, l$  gilt, dass  $g^k g^l = g^l g^k$ , ist  $\langle g \rangle$  abelsch.

Besonders wichtig für diese Arbeit sind die so genannten *Untergruppen*.

**Definition 4.2.** Sei  $(G, \cdot)$  eine Gruppe und  $H \subseteq G$ , sodass  $(H, \cdot)$  die Gruppenaxiome erfüllt, so ist  $H$  eine Untergruppe von  $G$ . Man schreibt  $H \leq G$ .

Für eine Untergruppe  $H \leq G$  und ein  $g \in G$  ist  $gH = \{g \cdot h \mid h \in H\}$  die von  $g$  erzeugte *Linksnebenklasse* von  $H$  und  $Hg = \{h \cdot g \mid h \in H\}$  die von  $g$  erzeugte *Rechtsnebenklasse* von  $H$ . Da gilt, dass  $\|gH\| = \|H\|$ , hat jede Nebenklasse dieselbe Kardinalität. Die Relation  $\sim$  mit

$$g \sim g' \Leftrightarrow gH = g'H$$

ist eine Äquivalenzrelation, die  $G$  in gleichgroße Äquivalenzklassen der Kardinalität  $\|H\|$  aufteilt. Damit folgt der Satz von Lagrange, wonach für eine Untergruppe  $H \leq G$  die Kardinalität der Untergruppe  $\|H\|$  ein Teiler von  $\|G\|$  ist. Daraus folgt insbesondere, dass, wenn  $\|G\|$  eine Primzahl ist,  $G$  nur die trivialen Untergruppen  $\{e\}$  und  $G$  besitzt. Ist  $g$  also ein von  $e$  verschiedenes Element von  $G$ , so stimmt die von  $g$  erzeugte Untergruppe  $\langle g \rangle$  bereits mit  $G$  überein. Gruppen mit dieser Eigenschaft heißen *zyklisch* und sind immer abelsch.

Eine bedeutende nichtabelsche Gruppe ist die *symmetrische Gruppe*, die nun definiert wird.

**Definition 4.3.** Eine Permutation  $\pi$  auf einer Menge  $M$  ist eine bijektive Abbildung  $\pi : M \rightarrow M$ . Die symmetrische Gruppe  $\text{Sym}(M)$  bezeichnet die Menge aller Permutationen auf  $M$ , wobei als Gruppenoperation die Verknüpfung der Funktionen betrachtet wird. Für  $M = [n] = \{1, 2, \dots, n\}$  schreibt man für  $\text{Sym}(M)$  auch  $S_n$ .

Eine Untergruppe  $P \leq \text{Sym}(M)$  heißt Permutationsgruppe.

Sei  $(G, \cdot)$  eine Gruppe mit dem neutralen Element  $e$ . Jedes Gruppenelement  $g$  definiert dann für alle  $g' \in G$  eine Permutation  $\pi_g : G \rightarrow G$  auf der Menge  $M = G$  via  $\pi_g(g') = g \cdot g'$ . Wegen  $\pi_g \circ \pi_{g'} = \pi_{gg'}$  ist die Menge  $P_G = \{\pi_g \mid g \in G\}$  eine Untermenge von  $\text{Sym}(G)$  und damit eine Permutationsgruppe. Die Abbildung  $T : G \rightarrow P_G$  mit  $T(g) = \pi_g$  ist ein Gruppenisomorphismus, da

- $T$  nach Definition surjektiv ist,
- $T$  wegen  $T(g) = T(g') \Rightarrow \pi_g(e) = \pi_{g'}(e) \Rightarrow g = g'$  injektiv ist, und
- $T$  wegen  $T(g \cdot g') = \pi_{gg'} = \pi_g \circ \pi_{g'} = T(g) \circ T(g')$  ein Homomorphismus ist.

Damit folgt der Satz von Cayley, nach dem jede Gruppe  $G$  isomorph zu einer Permutationsgruppe  $P$  ist, wobei  $\|P\| \leq \|G\|$  ist.

Ein weiterer für die Darstellungstheorie wichtiger Begriff ist der der *Konjugiertheit* von Gruppenelementen.

**Definition 4.4.** Sei  $G$  eine Gruppe. Zwei Gruppenelemente  $g, g' \in G$  heißen zueinander konjugiert, wenn es ein  $h \in G$  gibt mit

$$g' = hgh^{-1}$$

Die Konjugiertheit bildet eine Äquivalenzrelation. Die Äquivalenzklassen heißen *Konjugationsklassen*.

**Definition 4.5.** Sei  $G$  eine Gruppe. Sei  $H \leq G$  eine Untergruppe, sodass für alle  $g \in G$  gilt  $gHg^{-1} = H$ , so bezeichnet man  $H$  als normale Untergruppe oder Normalteiler und schreibt  $H \triangleleft G$ .

Eine normale Untergruppe  $H \triangleleft G$  ist also eine Vereinigung von Konjugationsklassen von  $G$ .

**Definition 4.6.** Sei  $(G, \cdot)$  eine Gruppe und  $H \triangleleft G$  eine normale Untergruppe, so bezeichnet man mit

$$(G/H, \circ)$$

die Faktorgruppe, wobei  $G/H = \{g \cdot H, g \in G\}$  die Menge der Linksnebenklassen von  $H$  bezeichnet und die Gruppenoperation  $\circ$  definiert ist über

$$X \circ Y = \{x \cdot y \mid x \in X \text{ und } y \in Y\}$$

Die Norm von  $G/H$  ist wegen des Satzes von Lagrange  $\|G/H\| = \|G\| / \|H\|$ . Außerdem ist klar, dass in einer abelschen Gruppe jede Untergruppe eine normale Untergruppe ist, da immer  $gHg^{-1} = gg^{-1}H = H$  gilt.

**Definition 4.7.** Das direkte Produkt zweier Gruppen  $(G, \cdot)$  und  $(H, \bullet)$  mit den neutralen Elementen  $1_G$  und  $1_H$  ist die Menge der Tupel  $G \times H$  zusammen mit einer Operation  $\circ$ , die komponentenweise definiert ist über

$$(g, h) \circ (g', h') = (g \cdot g', h \bullet h') \text{ für } g, g' \in G, h, h' \in H$$

Dabei ist  $(G \times H, \circ)$  wieder eine Gruppe mit dem neutralen Element  $e = (1_G, 1_H)$ , die kurz mit  $G \times H$  bezeichnet wird. Sind  $G$  und  $H$  abelsch, so ist es auch  $G \times H$ .

**Definition 4.8.** Für eine Gruppe  $G$  und ein  $S \subseteq G$  ist  $\langle S \rangle$  die Menge aller endlichen Produkte von Elementen von  $S$  und ihren Inversen.

## 4.2 Darstellung von Gruppen

Wie schon erwähnt, ist die Fouriertransformation (FT) der Schlüssel zur Lösung des HSP auf Quantencomputern. Die FT ist hauptsächlich als Möglichkeit bekannt, eine Funktion im Frequenzraum darzustellen. Auf einer Gruppe  $G$  definiert, ist die FT eine Transformation die eine Funktion  $f : G \rightarrow \mathbb{C}$  in eine Funktion auf dem Raum der Darstellungen von  $G$  abbildet. Darstellungen bilden dabei  $G$  auf die Gruppe  $GL_{\mathbb{C}}(V)$  der linearen invertierbaren Abbildungen eines Vektorraums  $V$  über dem Körper  $\mathbb{C}$  auf sich selbst ab. Eine Darstellung ist wie folgt definiert:

**Definition 4.9 (Darstellung).** Sei  $G$  eine Gruppe. Als Darstellung von  $G$  bezeichnet man einen Homomorphismus  $\rho : G \rightarrow GL_{\mathbb{C}}(V)$ , d.h. es muss gelten

$$\rho(gh) = \rho(g) \circ \rho(h) \text{ für alle } g, h \in G \quad (1)$$

Da im Folgenden endliche Gruppen betrachtet werden, benötigt man nur einen Vektorraum endlicher Dimension  $d$ . Für eine gegebene Basis  $(e_i)$  des Vektorraums ist  $\rho(G)$  also eine Menge von invertierbaren  $d \times d$ -Matrizen die via Matrixmultiplikation auf Elemente  $v$  des Vektorraums  $V$  wirken. Für  $\rho(g)(v)$  wird im Folgenden manchmal auch kürzer  $\rho_g v$  geschrieben. Die Dimension des zu  $\rho$  gehörenden Darstellungsraumes  $V$  sei mit  $d_\rho$  bezeichnet.

### Beispiele für Darstellungen

**Triviale Darstellung.** Die triviale Darstellung einer Gruppe  $G$  ordnet jedem Gruppenelement die 1 zu. Sie wird mit  $1_G$  bezeichnet. Man überzeugt sich leicht, dass dies der Definition 4.9 genügt. Wenn dies hier auch noch nicht besonders sinnreich erscheint, wird diese Darstellung im Folgenden noch eine wichtige Rolle spielen.

**Permutationsdarstellung.** Sei  $G$  eine Permutationsgruppe einer endlichen Menge  $X = \{x_1, \dots, x_n\}$ . Als Vektorraum betrachte man  $V = \mathbb{C}^n$  mit einer Basis  $(e_{x_1}, \dots, e_{x_n})$ . Sei  $\pi \in G$  eine Permutation, dann ordnet ihr die Permutationsdarstellung  $perm(\pi)$ , eine Permutationsmatrix  $P$  über  $V$  zu mit

$$P_{ij} = \begin{cases} 1 & \text{wenn } \pi(x_i) = x_j \\ 0 & \text{sonst} \end{cases}$$

In jeder Zeile und Spalte der Permutationsmatrix steht genau eine 1.

**Reguläre Darstellung.** Jede Gruppe  $G$  definiert nach dem Satz von Cayley eine Permutationsgruppe auf  $G$  selbst, indem die Permutation  $\pi_g(h)$  für  $g, h \in G$  durch  $\pi_g(h) = g \circ h \in G$  definiert wird. Die Permutationsdarstellung für  $X = G$  heißt *reguläre Darstellung* und wird mit  $reg(g)$  bezeichnet. Die Darstellung  $reg_g$  transformiert dann einen Basisvektor  $e_h$  nach  $e_{gh}$ .

Mithilfe der Matrixdarstellung werden die *Fourierkoeffizienten*  $\rho_{ij} : G \rightarrow \mathbb{C}$  einer Darstellung  $\rho$  definiert als:

$$\rho_{ij}(g) = (\rho_g)_{ij} \quad (2)$$

Sei nun der Fall gegeben, dass für eine Darstellung  $\rho$  ein nichttrivialer Untervektorraum  $W \subset V$  existiert, der invariant unter der Wirkung von  $G$  ist, also für  $w \in W$  und  $g \in G$  ist wieder  $\rho_g w \in W$ . Die Einschränkung der linearen Abbildung  $\rho_g$  auf den Unterraum  $W$  sei mit  $\rho_g^W$  bezeichnet. Diese ist wieder eine Darstellung von  $G$ . Sei nun

$$W^\perp = \{v \in V \mid \text{für alle } w \in W \text{ gilt } \widetilde{(v|w)} = 0\}. \quad (3)$$

Dabei ist  $\widetilde{(v|w)} = \sum_{g \in G} (\rho_g v | \rho_g w)$  ein mit Hilfe des Standardskalarprodukts  $(|)$  definiertes Skalarprodukt auf  $V$ , das invariant unter der Wirkung von  $G$  ist. D.h. für beliebige  $h \in G$  und  $v, w \in V$  ist  $\widetilde{(\rho_h v | \rho_h w)} = \widetilde{(v|w)}$ . Damit gilt:

1.  $V = W \oplus W^\perp$ : Jeder Vektor  $v \in V$  kann in eindeutiger Weise als Summe  $v = w + w'$  mit  $w \in W$  und  $w' \in W^\perp$  geschrieben werden.
2.  $W^\perp$  ist ebenfalls invariant unter der Wirkung von  $G$
3. Sei  $d_W$  die Dimension von  $W$  und  $(e_1, \dots, e_{d_W})$  eine Basis von  $W$  und  $(e_{d_W+1}, \dots, e_{d_\rho})$  eine Basis von  $W^\perp$ . In der Basis  $\mathcal{B} = (e_1, \dots, e_{d_W}, \dots, e_{d_\rho})$  zerfallen auf Grund der Invarianz der Unterräume die Darstellungsmatrizen in Blöcke:

$$\rho_g = \begin{pmatrix} \rho_g^W & 0 \\ 0 & \rho_g^{W^\perp} \end{pmatrix}$$

Man sagt auch, dass die Darstellung  $\rho$  die *direkte Summe* der Darstellungen  $\rho_g^W$  und  $\rho_g^{W^\perp}$  ist, und schreibt  $\rho_g = \rho_g^W \oplus \rho_g^{W^\perp}$ .

4. Orthogonalisiert man die Basis  $\mathcal{B}$  bezüglich des Skalarprodukts  $\widetilde{(|)}$ , so sind die Matrizen  $\rho_g^W$ ,  $\rho_g^{W^\perp}$  und  $\rho_g$  unitär. Man spricht in diesem Fall von einer unitären Darstellung.

Findet man einen unter  $G$  invarianten Untervektorraum  $W \subseteq V$ , so kann man die Darstellung in eine direkte Summe von Darstellungen zerlegen. Dies führt auf den Begriff der *irreduziblen* Darstellung.

**Definition 4.10.** Eine Darstellung  $\rho : G \rightarrow GL_{\mathbb{C}}(V)$  einer endlichen Gruppe  $G$  heißt irreduzibel, falls für jeden Untervektorraum  $W \subseteq V$  gilt:

$$W \text{ ist unter } G \text{ invariant} \Leftrightarrow W = V \text{ oder } W = \{0\}$$

Da jede Darstellung nur endlich oft zerlegt werden kann, erhält man:

**Theorem 4.11.** Jede Darstellung ist eine Summe irreduzibler Darstellungen

### 4.3 Charaktere einer Darstellung

In der weiteren Behandlung der Darstellungstheorie erweisen sich die so genannten Charaktere der Darstellungen als nützlich. Wie zu sehen sein wird, charakterisieren sie Darstellungen dahingehend, dass äquivalente Darstellungen denselben Charakter haben werden.

**Definition 4.12 (Charakter).** Sei  $\rho : G \rightarrow GL_{\mathbb{C}}(V)$  eine Darstellung einer endlichen Gruppe  $G$ , so wird eine Funktion  $\chi_{\rho} : G \rightarrow \mathbb{C}$  mittels

$$\chi_{\rho}(g) = \text{Sp}(\rho_g) \text{ für alle } g \in G \quad (4)$$

definiert, welche Charakter der Darstellung  $\rho$  heißt. Mit  $\text{Sp}(\cdot)$  wird die Spurbildung bezeichnet.

Man kann durch geeignete Basiswahl voraussetzen, dass die Matrizen  $\rho_g$  unitär sind. Das heißt insbesondere, dass sie diagonalisierbar sind. Da die Spurbildung basisunabhängig ist, kann man davon ausgehen, dass die Matrizen in Diagonalform vorliegen, was schnell zu einigen im Folgenden wichtigen Eigenschaften von Charakteren führt:

1. Sei  $e$  das neutrale Element von  $G$ , so ist  $\chi_{\rho}(e) = \text{Sp}(\rho(e)) = \text{Sp}(1_{d_{\rho}}) = d_{\rho}$  die Dimension des Darstellungsraums
2.  $\chi_{\rho}(g) = \lambda_1 + \dots + \lambda_n$  ist die Summe der Eigenwerte von  $\rho_g$
3.  $\chi_{\rho}(hgh^{-1}) = \text{Sp}(\rho_h \rho_g \underbrace{\rho_{h^{-1}}}_{=\rho_h^{-1}}) = \chi_{\rho}(g)$ . D.h.  $\chi_{\rho}(g)$  ist konstant auf allen Elementen der Konjugationsklasse von  $g$ .
4. Da  $G$  endlich ist, existiert für jedes  $g \in G$  ein  $r$  mit  $g^r = e$ . Für dieses gilt

$$\rho_g^r = \begin{pmatrix} \lambda_1^r & & & \\ & \lambda_2^r & & \\ & & \dots & \\ & & & \lambda_n^r \end{pmatrix} = \rho(g^r = e) = 1_{d_{\rho}}$$

Also ist  $\lambda_i^r = 1$  für  $1 \leq i \leq n$ , womit man folgert, dass  $|\lambda_i| = 1$  und  $\lambda_i^{-1} = \overline{\lambda_i}$

5.  $\chi_{\rho}(g^{-1}) = \text{Sp}(\rho^{-1}(g)) = \lambda_1^{-1} + \dots + \lambda_n^{-1} = \overline{\lambda_1} + \dots + \overline{\lambda_n} = \overline{\chi_{\rho}(g)}$

Eine Funktion mit Eigenschaft 3 heißt *zentrale Funktion*:

**Definition 4.13.** Sei  $G$  eine Gruppe und  $A$  eine Menge. Eine Funktion  $f : G \rightarrow A$ , die konstant auf Konjugationsklassen von  $G$  ist, heißt zentrale Funktion von  $G$ .

## Beispiele für Charaktere

**Permutationsdarstellung.** In einer Permutationsmatrix  $P$  entspricht eine 1 in der Diagonalen einem fixierten Element der Menge. Es gilt also:

$$\chi_{perm}(g) = \text{Anzahl der durch } g \text{ fixierten Elemente}$$

**reguläre Darstellung.** Das neutrale Element ist eindeutig in einer Gruppe  $G$ , es gilt  $gh = h \Leftrightarrow g = e$  für  $g, h \in G$ . Daher ist  $reg_g$  eine Permutationsmatrix, die alle Elemente permutiert, außer wenn  $g = e$  das neutrale Gruppenelement ist. Es gilt somit:

$$\chi_{reg}(g) = \begin{cases} \|G\| & \text{wenn } g = e \\ 0 & \text{sonst} \end{cases} \quad (5)$$

**Definition 4.14 (Skalarprodukt).** Zwischen zwei komplexwertigen Funktionen  $f_1, f_2 : G \rightarrow \mathbb{C}$  auf einer endlichen Gruppe  $G$  ist ein Skalarprodukt definiert über

$$(f_1 | f_2) = \frac{1}{\|G\|} \sum_{g \in G} \overline{f_1(g)} f_2(g) \quad (6)$$

Geht man von einer unitären Darstellung aus, in der gilt  $\rho_g^{-1} = \rho_g^\dagger$ , so folgt für das Skalarprodukt zweier Fourierkoeffizienten

$$(\rho_{ij} | \rho'_{kl}) = \frac{1}{\|G\|} \sum_{g \in G} \rho_{ij}(g^{-1}) \rho'_{kl}(g)$$

Ebenso gilt für das Skalarprodukt der Charaktere wegen der 5. Eigenschaft:

$$(\chi_\rho | \chi_\tau) = \frac{1}{\|G\|} \sum_{g \in G} \chi_\rho(g^{-1}) \chi_\tau(g)$$

Um den Raum der Funktionen  $f : G \rightarrow \mathbb{C}$  und insbesondere der Untermenge der zentralen Funktionen zu analysieren, benötigt man vollständige Orthonormalsysteme auf diesen Funktionenräumen. Es wird sich zeigen, dass die Fourierkoeffizienten im ersteren und die Charaktere im letzteren Fall genau dies leisten. Um dies zu zeigen, benötigt man die Aussagen des Schur'schen Lemmas.

## 4.4 Schur'sches Lemma

**Definition 4.15 (Äquivalenz von Darstellungen).** Zwei Darstellungen  $\rho : G \rightarrow GL_{\mathbb{C}}(V)$  und  $\rho' : G \rightarrow GL_{\mathbb{C}}(W)$  sind äquivalent (geschrieben  $\rho \cong \rho'$ ), wenn ein Isomorphismus  $\Phi : V \rightarrow W$  existiert, sodass für alle  $g \in G$

$$\Phi \circ \rho_g = \rho'_g \circ \Phi$$

Dies heißt, dass sich die Darstellungsmatrizen äquivalenter Darstellungen durch einen Basiswechsel ineinander überführen lassen. Im Folgenden wird oft die Menge aller irreduziblen Darstellungen benötigt, wobei man von allen äquivalenten Darstellungen nur einen Repräsentanten auswählt. Wie später noch klar wird, muss man immer einen Repräsentanten wählen, der auf eine Menge von unitären Matrizen abbildet, was sich immer durch einen Basiswechsel erreichen lässt.

**Definition 4.16.** Zu einer Gruppe  $G$  bezeichne  $\hat{G}$  eine Menge aller irreduziblen, nichtäquivalenten unitären Darstellungen.

Die Zuordnung  $G$  zu  $\hat{G}$  ist nicht eindeutig, aber sämtliche Ausführungen werden unabhängig von der konkreten Wahl von  $\hat{G}$  sein.

**Beobachtung 4.17.** Man sieht sofort, dass wegen  $\mathrm{Sp}(\rho_g) = \mathrm{Sp}(\Phi^{-1}\rho'_g\Phi) = \mathrm{Sp}(\rho'_g)$ , zwei äquivalente Darstellungen denselben Charakter haben.

**Lemma 4.18 (Schur'sches Lemma [JPS]).** Es seien  $\rho : G \rightarrow \mathrm{GL}_{\mathbb{C}}(V)$  und  $\rho' : G \rightarrow \mathrm{GL}_{\mathbb{C}}(W)$  zwei irreduzible Darstellungen einer endlichen Gruppe  $G$  und  $f : V \rightarrow W$  linear, sodass für alle  $g \in G$  gilt  $\rho_g \circ f = f \circ \rho'_g$ . Dann gilt:

1.  $\rho$  nicht äquivalent zu  $\rho' \implies f \equiv 0$
2.  $V = W$  und  $\rho = \rho' \implies f \equiv \lambda \cdot \mathbb{1}_{d_\rho}$  mit  $\lambda \in \mathbb{C}$

**Beweis.** *ad(1):* Sei nicht  $f \equiv 0$  und  $x \in \ker f = \{v \in V \mid f(v) = 0\}$ . Dann ist  $0 = \rho'_g \circ f(x) = f \circ \rho_g(x)$  für beliebige  $g \in G$ . Also ist  $\rho_g(x) \in \ker f$  und damit  $\ker f$  invariant unter der Wirkung von  $G$ . Da nach Voraussetzung  $\rho$  irreduzibel ist, folgt daraus entweder  $\ker f = \{0\}$  oder  $\ker f = V$ , wobei der zweite Fall entfällt, da  $f \equiv 0$  ausgeschlossen wurde. Für beliebige  $v \in V$  und  $g \in G$  gilt  $\rho'_g \circ f(v) = f \circ \rho_g(v)$ . Also ist für jedes  $f(v) \in \mathrm{im}(f) = f(V)$  auch  $\rho'_g \circ f(v) \in \mathrm{im}(f)$ . Also ist auch  $\mathrm{im}(f)$  invariant unter der Wirkung von  $G$ . Es folgt wieder entweder  $\mathrm{im}(f) = 0$  oder  $\mathrm{im}(f) = W$ , wobei diesmal  $\mathrm{im}(f) = 0$  entfällt. Wegen  $\ker f = 0$  und  $\mathrm{im}(f) = W$  ist  $f$  ein Isomorphismus für den nach Voraussetzung gilt  $f \circ \rho_g(v) = \rho'_g \circ f(v)$ , womit die erste Aussage bewiesen ist.

*ad(2):* Sei  $V = W$  und  $\rho = \rho'$  und sei  $\lambda$  eine Lösung der Eigenwertgleichung  $f(v) = \lambda \cdot v$ , die über dem Körper  $\mathbb{C}$  immer existiert. Sei  $f' = f - \lambda$ , was mit  $\rho'_g \circ f' = f' \circ \rho_g$  wegen (1) impliziert, dass  $f' \equiv 0$ . Also  $f \equiv \lambda$ . ■

Mithilfe des Schur'schen Lemmas wird nun gezeigt, dass die Fourierkoeffizienten orthogonal sind. Daraus wird gefolgert, dass auch die Charaktere orthogonal sind. Die Menge  $\hat{G}$  bildet sogar ein vollständiges Orthonormalsystem (VONS) auf dem Funktionenraum der zentralen Funktionen. Dies wird zu der wichtigen Erkenntnis führen, dass es genauso viele nicht äquivalente irreduzible Darstellungen gibt, wie es Konjugationsklassen gibt.

**Satz 4.19.** Seien  $\rho : G \rightarrow \mathrm{GL}_{\mathbb{C}}(V)$  und  $\rho' : G \rightarrow \mathrm{GL}_{\mathbb{C}}(W)$  zwei irreduzible, nicht äquivalente und unitäre Darstellungen von  $G$ , dann gilt für beliebige  $i, j, k, l$

$$(\rho'_{ij} \mid \rho_{lk}) = 0 \tag{7}$$

$$(\rho_{ij} \mid \rho_{lk}) = \frac{1}{d_V} \delta_{il} \delta_{kj} \tag{8}$$

**Beweis.** Für eine gegebene lineare Abbildung  $h : V \rightarrow W$  sei

$$h^0 = \frac{1}{\|G\|} \sum_{g \in G} \rho'(g^{-1}) h \rho(g)$$

Damit gilt

$$\rho'(g)^{-1}h^0\rho(g) = \frac{1}{\|G\|} \sum_{s \in G} \underbrace{\rho'(g^{-1}s^{-1})}_{\rho'((sg)^{-1})} h \rho(sg) = h^0$$

Da also  $\rho'(g)h^0 = h^0\rho(g)$  kann man mit  $f = h^0$  das Schur'sche Lemma anwenden. Um die erste Aussage zu beweisen, betrachtet man Fall 1 aus dem Lemma in Matrixform. Wegen der Unitarität der Darstellungen gilt  $\rho'(g^{-1}) = \rho'(g)^{-1} = (\rho'(g))^\dagger$ .

$$0 = f_{jl} = h_{jl}^0 = \frac{1}{\|G\|} \sum_{g \in G} \sum_{ik} \underbrace{\rho'_{ji}(g^{-1})}_{\overline{\rho'_{ij}(g)}} h_{ik} \rho_{kl}(g)$$

Um dies für beliebige  $h_{kl}$  zu erfüllen, muss also bereits  $(\rho'_{ij} | \rho_{lk}) = 0$  sein.

Für die zweite Aussage nutzt man entsprechend den zweiten Fall des Schur'schen Lemmas, wobei man nun  $\rho' = \rho$  setzt. Für ein  $\lambda \in \mathbb{C}$  gilt also  $h^0 = \lambda \mathbb{1}_{d_\rho}$ . Man bestimmt  $\lambda$  mittels

$$\text{Sp}(h^0) = \frac{1}{\|G\|} \sum_{g \in G} \text{Sp}(\rho_g^{-1} h \rho_g) = \text{Sp}(h) = \lambda \cdot d_V \implies \lambda = \frac{\text{Sp}(h)}{d_V}$$

Damit folgt:

$$h_{jl}^0 = \frac{1}{\|G\|} \sum_{g \in G} \sum_{ik} \overline{\rho'_{ij}(g)} h_{ik} \rho_{kl}(g) = \lambda \delta_{jl} = \frac{1}{d_V} \sum_{ik} h_{ik} \delta_{ik} \delta_{jl}$$

Die zweite Aussage folgt dann, da wieder  $h_{kl}$  beliebig gewählt werden kann. ■

**Korollar 4.20.** Es sei  $\rho$  eine irreduzible Darstellung einer Gruppe  $G$ . Dann gilt:

$$\frac{1}{\|G\|} \sum_{g \in G} \rho(g)_{ij} = (1_G | \rho_{ij}) = \begin{cases} 1 & \text{falls } \rho = 1_G \\ 0 & \text{sonst} \end{cases}$$

Aus dem vorherigen Satz lässt sich nun leicht durch Spurbildung die Orthonormalität der Charaktere beweisen.

**Korollar 4.21.** Es seien  $\chi, \chi'$  die Charaktere zweier irreduzibler nicht äquivalenter Darstellungen  $\rho, \rho'$  einer Gruppe  $G$ . Dann gilt:

1.  $(\chi | \chi) = (\text{Sp}(\rho) | \text{Sp}(\rho)) = \sum_{ij} (\rho_{ii} | \rho_{jj}) = 1$
2.  $(\chi | \chi') = (\text{Sp}(\rho) | \text{Sp}(\rho')) = \sum_{ij} (\rho_{ii} | \rho'_{jj}) = 0$

**Satz 4.22.** Sei  $G$  eine endliche Gruppe, dann bildet die Menge der Charaktere  $\{\chi_\rho | \rho \in \hat{G}\}$  ein VONS des Funktionenraums der zentralen Funktionen  $f : G \rightarrow \mathbb{C}$  mit  $f(hgh^{-1}) = f(g)$  für alle  $g, h \in G$ .

**Beweis.** Die Orthogonalität wurde bereits gezeigt. Es bleibt nur noch die Vollständigkeit zu zeigen. Dazu beweist man, dass jede zentrale Funktion  $f$ , die zu allen Basisvektoren orthogonal ist, selbst nur Null sein kann. Für ein  $\rho \in \hat{G}$  sei  $\rho^{(f)} = \frac{1}{\|G\|} \sum_{g \in G} \overline{f(g)} \rho(g)$ . Dann folgt für beliebige  $h \in G$ :

$$\rho_h^{-1} \rho^{(f)} \rho_h = \frac{1}{\|G\|} \sum_{g \in G} \overline{f(g)} \rho(\underbrace{h^{-1}gh}_{=:u}) = \frac{1}{\|G\|} \sum_{u \in G} \overline{f(huh^{-1})} \rho(u) = \rho^{(f)}$$

Es gilt also  $\rho_h \rho^{(f)} = \rho^{(f)} \rho_h$  und man kann die zweite Aussage des Schur'schen Lemmas anwenden und folgern, dass  $\rho^{(f)} = \lambda \mathbb{1}_{d_\rho}$  für ein  $\lambda \in \mathbb{C}$ . Durch Spurbildung erhält man:

$$\text{Sp}(\rho^{(f)}) = \frac{1}{\|G\|} \sum_{g \in G} \overline{f(g)} \chi_\rho(g) = (f | \chi_\rho) = 0 \implies \lambda = 0$$

Es gilt also für beliebige  $\rho \in \hat{G}$ , dass  $\sum_{g \in G} \overline{f(g)} \rho(g) = 0$ . Wählt man für  $\rho = \text{reg}$  die reguläre Darstellung und multipliziert die Gleichung von rechts mit  $e_1$ , dem Basisvektor der Identität in  $G$ , so folgt:

$$\rho^{(f)} \cdot e_1 = \sum_{g \in G} \overline{f(g)} \text{reg}(g) \cdot e_1 = \sum_{g \in G} \overline{f(g)} e_g = 0$$

Dies zeigt, da jede Komponente des Vektors verschwinden muss, dass  $f \equiv 0$ . ■

Die Dimension des Funktionenraums der zentralen Funktionen wird durch die Anzahl  $\|\hat{G}\|$  der Charaktere gegeben, die wie gezeigt ein VONS bilden. Für eine Konjugationsklasse  $K \subseteq G$  sei

$$f_K(g) = \begin{cases} 1 & \text{falls } g \in K \\ 0 & \text{sonst} \end{cases}$$

die Indikatorfunktion von  $K \subseteq G$ . Die Indikatorfunktionen bilden ebenfalls ein vollständiges Funktionensystem der zentralen Funktionen. Man kann also folgern:

**Korollar 4.23.** Sei  $G$  eine endliche Gruppe, dann gilt

$$\|\hat{G}\| = \text{Anzahl der Konjugationsklassen in } G$$

Mit Hilfe dieses VONS kann man nun wichtige Aussagen der Darstellungstheorie leicht ableiten. Für eine Gruppe  $G$  sei  $\hat{G} = \{\rho_1, \dots, \rho_k\}$  die Menge der irreduziblen, nicht äquivalenten Darstellungen. Dann ist jede Darstellung  $\tau$  von  $G$  äquivalent zu einer direkten Summe der Darstellungen in  $\hat{G}$

$$\tau \cong m_1 \rho_1 \oplus \dots \oplus m_k \rho_k,$$

wobei  $m_i \rho_i = \underbrace{\rho_i \oplus \dots \oplus \rho_i}_{m_i \text{ Mal}}$  bedeutet. Da äquivalente Darstellungen denselben Charakter haben, kommt man durch Spurbilder der Gleichung zu:

$$\chi_\tau = m_1 \chi_{\rho_1} + \dots + m_k \chi_{\rho_k}$$

Nun ist aber  $(\chi_{\rho_i})_{1 \leq i \leq k}$  ein VONS. Man kann also  $\chi_\tau$  darstellen als:

$$\chi_\tau = (\chi_{\rho_1} | \chi_\tau) \chi_{\rho_1} + \cdots + (\chi_{\rho_k} | \chi_\tau) \chi_{\rho_k}$$

Das heißt also, eine irreduzible Darstellung  $\rho_i$  ist in jeder Darstellung  $\tau$  immer  $m_i = (\chi_{\rho_i} | \chi_\tau)$  Mal enthalten ist. Außerdem sieht man, dass auch die Umkehrung von Beobachtung 4.17 gilt. Da zwei Darstellungen  $\tau$  und  $\tau'$  äquivalent sind, wenn sie denselben Satz von Koeffizienten  $m_1, \dots, m_k$  besitzen, ist die Gleichheit ihrer Charaktere eine hinreichende Bedingung für ihre Äquivalenz. Es gilt also

**Korollar 4.24.** Für eine endliche Gruppe  $G$  und zwei Darstellungen  $\tau, \tau' \in \hat{G}$  gilt

$$\tau \cong \tau' \Leftrightarrow \chi_\tau = \chi_{\tau'}$$

Setzt man für  $\tau = \text{reg}$  die reguläre Darstellung ein, erhält man mit Gleichung 5:

$$m_i = (\chi_{\rho_i} | \chi_{\text{reg}}) = \frac{1}{\|G\|} \sum_{g \in G} \chi_{\rho_i}(g) \chi_{\text{reg}}(g) = \chi_{\rho_i}(e) = d_{\rho_i}$$

Jede irreduzible Darstellung  $\rho \in \hat{G}$  ist also in der regulären Darstellung  $d_\rho$ -Mal enthalten ist. Des weiteren sieht man, dass:

$$\|G\| = \chi_{\text{reg}}(e) = \text{Sp}(\text{reg}(e)) = \sum_{i=1}^k d_{\rho_i} \chi_{\rho_i}(e) = \sum_{\rho \in \hat{G}} d_\rho^2 \quad (9)$$

**Korollar 4.25.** Sei  $G$  eine endliche Gruppe, dann bildet die Menge der Fourierkoeffizienten  $\{\rho_{ij} \mid \rho \in \hat{G} \ 1 \leq i, j \leq d_\rho\}$  ein VONS des Funktionenraums der Funktionen  $f : G \rightarrow \mathbb{C}$ .

**Beweis.** Die Orthogonalität wurde in Satz 4.19 gezeigt. Der Funktionenraum hat die Dimension  $\|G\|$ . Z.B. wäre  $\{\delta_g(x) \mid g \in G\}$  ein VONS, wobei

$$\delta_g(x) = \begin{cases} 1 & \text{für } x = g \\ 0 & \text{sonst} \end{cases}$$

Die Anzahl der Fourierkoeffizienten ist  $\sum_{\rho \in \hat{G}} d_\rho^2$ , was nach Gleichung 9 gleich der Dimension des Funktionenraums ist. ■

## 4.5 Darstellung abelscher Gruppen

Warum kann man das Hidden Subgroup Problem für abelsche Gruppen auf Quantencomputern effizient lösen, jedoch i.A. nicht für nichtabelsche Gruppen? Dies liegt daran, dass abelsche Gruppen einen besonders einfachen Satz irreduzibler Darstellungen besitzen, der im Folgenden konstruiert werden soll.

In abelschen Gruppen ist wegen  $hgh^{-1} = hh^{-1}g = g$  in jeder Konjugationsklasse genau ein Element von  $G$ . Wegen Korollar 4.23 gilt also  $\|G\| = \|\hat{G}\|$ . Aus Gleichung 9 folgt dann

$$\|\hat{G}\| = \sum_{\rho \in \hat{G}} d_\rho^2 \quad (10)$$

was nur erfüllbar ist, wenn alle  $\rho \in \hat{G}$  die Dimension  $d_\rho = 1$  haben. Dies heißt auch, dass eine Darstellung identisch zu ihrem Charakter ist.

Es soll nun eine Menge von irreduziblen, nichtäquivalenten Darstellungen einer abelschen Gruppe angegeben werden. Dazu nutzt man, dass sich jede endliche abelsche Gruppe als Produkt zyklischer Gruppen darstellen lässt.

**Satz 4.26 (Struktursatz für endliche abelsche Gruppen).** *Es sei  $G$  eine endliche, abelsche Gruppe mit  $\|G\| > 1$ . Dann existieren eindeutig bestimmte Zahlen  $r, d_1, \dots, d_r \in \mathbb{N}$  mit  $1 < d_1 | d_2 | \dots | d_r$ , zu denen es Elemente  $b_i \in G$  mit  $\text{ord}(b_i) = d_i$  gibt, sodass*

$$G = \langle b_1 \rangle \times \dots \times \langle b_r \rangle$$

(o.B.)

Sei also zuerst eine zyklische Gruppe  $\langle a \rangle$  betrachtet.

**Satz 4.27.** *Für eine zyklische Gruppe  $G = \langle a \rangle$  mit  $\|G\| = \text{ord}(a) = n$  bilden folgende Darstellungen  $\rho_k : G \rightarrow GL_{\mathbb{C}}$  die Menge der irreduziblen, nicht äquivalenten Darstellungen  $\hat{G}$*

$$\rho_k(a^r) = \omega_n^{kr} \text{ für } k = 0, \dots, n-1$$

Wobei  $\omega_d = e^{\frac{2\pi i}{d}}$  die primitive  $d$ -te Einheitswurzel ist.

**Beweis.** *Es gilt für  $k = 0, \dots, n-1$*

$$\rho_k(a^r)\rho_k(a^s) = \omega_n^{kr}\omega_n^{ks} = \omega_n^{k(r+s)} = \rho_k(a^{r+s}) = \rho_k(a^r a^s)$$

Also sind die  $\rho_k$  Homomorphismen. Sie sind natürlich irreduzibel, da sie eindimensional sind. Korollar 4.24 zeigt, dass keine zwei Darstellungen äquivalent sind, da sich ihre Charaktere unterscheiden, die im eindimensionalen Fall ja gleich der Darstellungen selbst sind. Aus Gleichung 10 folgt, dass die komplette Menge  $\hat{G}$  angegeben wurde, da es  $n = \|G\| = \|\hat{G}\|$  inäquivalente Darstellungen gibt. ■

Um dies auf das direkte Produkt endlich vieler zyklischer Gruppen zu erweitern, benötigt man noch folgenden Satz:

**Satz 4.28.** *Sei  $(A, \cdot)$  eine abelsche Gruppe mit  $\hat{A} = \{\rho_1, \dots, \rho_m\}$  und  $G = (A \times \langle b \rangle, \bullet)$  das direkte Produkt von  $A$  und einer zyklischen Gruppe mit  $\text{ord}(b) = n$  Elementen, so bilden folgende Darstellungen  $\tau_{ik} : G \rightarrow GL_{\mathbb{C}}$  die Menge der irreduziblen, nicht äquivalenten Darstellungen  $\hat{G}$*

$$\tau_{ik}((a, b^r)) = \rho_i(a) \cdot \omega_n^{kr} \text{ für } i = 0, \dots, m-1, k = 0, \dots, n-1 \text{ und } a \in A$$

**Beweis.** *Es gilt für  $i = 0, \dots, m-1$  und  $k = 0, \dots, n-1$*

$$\begin{aligned} \tau_{ik}((a, b^r))\tau_{ik}((a', b^s)) &= \rho_i(a) \cdot \omega_n^{kr} \cdot \rho_i(a') \cdot \omega_n^{ks} \\ &= \rho_i(aa')\omega_n^{k(r+s)} \\ &= \tau_{ik}((aa', b^r b^s)) \\ &= \tau_{ik}((a, b^r) \bullet (a', b^s)) \end{aligned}$$

Da  $A$  abelsch ist, sind die  $\rho_i$  eindimensional, also auch die  $\tau_{ik}$ , womit Irreduzibilität gegeben ist. Die Inäquivalenz überträgt sich ebenso, mit derselben Begründung, wie im Beweis des vorangegangenen Satzes. Wegen  $\|G\| = \|A\| \cdot \|\langle b \rangle\| = \|\hat{A}\| \cdot n$  folgt, dass  $\hat{G}$  vollständig angegeben wurde. ■

**Korollar 4.29.** Sei  $G = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle$  mit  $\text{ord}(a_i) = n_i$ , so bilden folgende Darstellungen  $\rho_{l_1 \dots l_k} : G \rightarrow GL_{\mathbb{C}}$  die Menge der irreduziblen, nicht äquivalenten Darstellungen  $\hat{G}$

$$\rho_{l_1 \dots l_k} ((a_1^{r_1}, \dots, a_k^{r_k})) = \prod_{j=1}^k \omega_{n_j}^{l_j \cdot r_j}$$

für  $0 \leq l_1 \leq n_1 - 1, \dots, 0 \leq l_k \leq n_k - 1$ .

**Beweis.** Mittels Induktion über  $k$  mit Induktionsanfang aus Satz 4.27 und Induktionsschritt aus Satz 4.28. ■

## 5 Fouriertransformation für Gruppen

Kern jedes Quanten-Algorithmus über versteckte Untergruppen ist die Fouriertransformation für Gruppen. Im Spezialfall abelscher Gruppen wird sie sich als die vielleicht schon bekannte diskrete Fouriertransformation herausstellen.

**Definition 5.1 (Fouriertransformation über endlichen Gruppen).** Sei  $G$  eine endliche Gruppe und  $f : G \rightarrow \mathbb{C}$  eine komplexwertige Funktion auf  $G$ , so ist die Fouriertransformierte  $\hat{f}$  an der Stelle  $\rho$  als die  $d_\rho \times d_\rho$ -Matrix

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{\|G\|}} \sum_{g \in G} f(g) \rho(g)$$

definiert.

Wie kann man nun allgemein Funktionen  $f$  und  $\hat{f}$  auf Quantencomputern darstellen? Man speichert sie als Zustandsvektoren ihrer Funktionswerten als Amplituden ab.

Für Funktionen  $f : G \rightarrow \mathbb{C}$  wählt man als Basis das VONS  $\{\delta_g \mid g \in G\}$ , wobei

$$\delta_g(x) = \begin{cases} 1 & \text{für } x = g \\ 0 & \text{sonst} \end{cases}$$

Somit ist  $f = \sum_{g \in G} f(g) \delta_g$ . Sei  $G = \{g_1, \dots, g_n\}$ , dann repräsentiert man eine Basisfunktion  $\delta_{g_i}$  einfach durch die Zahl  $i$  und schreibt  $|g_i\rangle$  für den Zustandsvektor des Quantencomputers, der diese Zahl speichert. Dann wird eine Funktion  $f$  einfach gespeichert als

$$|f\rangle = \frac{1}{\|f\|^2} \sum_{g \in G} f(g) |g\rangle,$$

wobei der Zustand durch das Dividieren durch  $\|f\|^2 = \sum_{g \in G} |f(g)|^2$  normiert wird.

Für Funktionen  $\hat{f}$  wählt man entsprechend als Basis das VONS  $\{\delta_{\rho ij} \mid \rho \in \hat{G} \ 1 \leq i, j \leq d_\rho\}$ , wobei

$$\delta_{\rho ij}(\tau, k, l) = \begin{cases} 1 & \text{für } (\rho, i, j) = (\tau, k, l) \\ 0 & \text{sonst} \end{cases}$$

Dann ist  $\hat{f} = \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \hat{f}(\rho)_{ij} \cdot \delta_{\rho ij}$ . Sei  $\hat{G} = \{\rho_1, \dots, \rho_k\}$ , dann repräsentiert man eine Basisfunktion  $\delta_{\rho ij}$  durch das Tripel  $(l, i, j)$  und schreibt  $|\rho ij\rangle$  für den Zustandsvektor des Quantencomputers, der dieses Tripel speichert.

Dann wird eine Funktion  $\hat{f}$  gespeichert als

$$|\hat{f}\rangle = \hat{U}_{FT} |f\rangle = \frac{1}{\|f\|^2} \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \hat{f}(\rho)_{ij} |\rho ij\rangle$$

Die Normierung muss *nicht* angepasst werden, da die Fouriertransformation, wie noch zu sehen sein wird, unitär ist.

Um zu berechnen, wie die Fouriertransformation auf einen festen Basisvektor  $|g\rangle$  mit  $g \in G$  wirkt, setzt man einfach  $f = \delta_g$ . Dann folgt

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{\|G\|}} \rho(g)$$

Das heißt, die Fourier Transformation bildet einen Basisvektoren  $|g\rangle$  wie folgt ab:

$$|g\rangle \mapsto \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \sqrt{\frac{d_\rho}{\|G\|}} \rho_{ij}(g) |\rho_{ij}\rangle \quad (11)$$

Quantencomputer können aufgrund der physikalischen Gesetze nur unitäre Transformationen bezüglich des Skalarproduktes  $\langle \cdot | \cdot \rangle$  ausführen. Man muss also noch testen, ob auch die Fouriertransformation unitär ist. Dazu muss man davon ausgehen, dass die  $\rho \in \hat{G}$  unitär sind, was man jedoch immer kann. Damit beweist man zuerst folgendes Lemma

**Lemma 5.2.** *Sei  $G$  eine Gruppe, und  $g, g' \in G$ , dann gilt*

$$\sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \frac{d_\rho}{\|G\|} \overline{\rho_{ij}(g)} \rho_{ij}(g') = \begin{cases} 1 & \text{falls } g = g' \\ 0 & \text{sonst} \end{cases}$$

**Beweis.** *man benutzt, dass für die unitären Darstellungen gilt  $\overline{\rho_{ij}(g)} = \rho_{ji}^\dagger(g) = \rho_{ji}^{-1}(g) = \rho_{ji}(g^{-1})$ . Damit ist*

$$\sum_{i,j=1}^{d_\rho} \overline{\rho_{ij}(g)} \rho_{ij}(g') = \sum_{i,j=1}^{d_\rho} \rho_{ji}(g^{-1}) \rho_{ij}(g') = \text{Sp}(\rho(g^{-1})\rho(g')) = \chi_\rho(g^{-1}g')$$

Des Weiteren ist

$$\sum_{\rho \in \hat{G}} d_\rho \chi_\rho(g) = \chi_{\text{reg}}(g) = \begin{cases} \|G\| & \text{falls } g = e \\ 0 & \text{sonst} \end{cases}$$

womit die Behauptung folgt. ■

**Satz 5.3.** *Die Fouriertransformation  $\hat{U}_{FT}$  ist eine unitäre Transformation.*

**Beweis.** *Mithilfe des Lemmas 5.2 kann man leicht zeigen, dass die Fouriertransformation das Skalarprodukt invariant lässt:*

$$\begin{aligned} \langle \hat{f} | \hat{g} \rangle &= \sum_{\rho, \rho' \in \hat{G}} \sum_{i,j=1}^{d_\rho} \sum_{k,l=1}^{d_{\rho'}} \overline{\hat{f}(\rho)_{ij}} \cdot \hat{g}(\rho')_{kl} \underbrace{\langle \rho_{ij} | \rho'_{kl} \rangle}_{\delta_{\rho\rho'} \delta_{ik} \delta_{jl}} \\ &= \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \overline{\hat{f}(\rho)_{ij}} \cdot \hat{g}(\rho)_{ij} \\ &= \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \frac{d_\rho}{\|G\|} \sum_{g,g' \in G} \overline{f(g)} g(g') \overline{\rho_{ij}(g)} \rho_{ij}(g') \\ (\text{Lemma 5.2} \Rightarrow) &= \sum_{g \in G} \overline{f(g)} g(g) = \langle f | g \rangle \end{aligned}$$

Die Fouriertransformation ist also unitär. ■

Nun, da gezeigt wurde, dass die Fouriertransformation  $\hat{U}_{FT}$  unitär ist, kann man leicht ihre Inverse angeben, indem man die Transformationsmatrix adjungiert. Aus der Basistransformation

$$\hat{U}_{FT} |g\rangle = \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \sqrt{\frac{d_\rho}{\|G\|}} \rho_{ij}(g) |\rho ij\rangle$$

liest man die Matrixelemente ab:

$$\langle \rho ij | \hat{U}_{FT} |g\rangle = \sqrt{\frac{d_\rho}{\|G\|}} \rho_{ij}(g)$$

Wegen  $U^\dagger = U^{-1}$  sieht man, dass

$$\langle g | \hat{U}_{FT}^{-1} | \rho ij \rangle = \overline{\langle \rho ij | \hat{U}_{FT} | g \rangle} = \sqrt{\frac{d_\rho}{\|G\|}} \overline{\rho_{ij}(g)}.$$

Die inverse Fouriertransformation angewendet auf einen Basisvektor  $|\rho ij\rangle$  ist also

$$\hat{U}_{FT}^{-1} |\rho ij\rangle = \sqrt{\frac{d_\rho}{\|G\|}} \sum_{g \in G} \overline{\rho_{ij}(g)} |g\rangle.$$

Insbesondere ist damit die inverse Fouriertransformation der trivialen Darstellung  $1_G$ :

$$\hat{U}_{FT}^{-1} |1_G, 1, 1\rangle = \sqrt{\frac{1}{\|G\|}} \sum_{g \in G} |g\rangle,$$

was eine Möglichkeit liefert, eine Superposition aller Gruppenelemente zu erzeugen.

Es sei abschließend die Fouriertransformation der abelschen Gruppe  $G = \langle a \rangle$  mit  $\|G\| = \|\hat{G}\| = \text{ord}(a) = n$  betrachtet. Hier haben die Darstellungen die Form  $\rho_k(a^r) = \omega_n^{kr}$  für  $k = 0, \dots, n-1$ . Kodiert man ein Gruppenelement  $a^r$  mit dem Zustand  $|r\rangle$  und eine Darstellung  $\rho_k$  mit  $|k\rangle$ , vollzieht die Fouriertransformation die Abbildung

$$|r\rangle \mapsto \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{\frac{2\pi ikr}{n}} |k\rangle.$$

Ist  $n$  eine Zweierpotenz, lässt sich diese Transformation mit  $\mathcal{O}(n^2)$  elementaren Quantentransformationen berechnen. Sonst ist kein polynomieller Quantenalgorithmus bekannt, der die Fouriertransformation exakt berechnet. Es stellt sich generell das Problem, für eine gegebene Gruppe einen effiziente Quantenfouriertransformation zu finden.

## 6 Das Hidden Subgroup Problem

Zur Erinnerung, hier noch einmal die Definition des *Hidden Subgroup Problem* (HSP):

### Problem 6.1 (HSP)

**gegeben:** Eine Funktion  $f : G \rightarrow A$ , wobei  $G$  eine endliche Gruppe und  $A$  eine beliebige Menge ist.

**promise:** Es existiert eine Untergruppe  $H \leq G$ , sodass  $f$  auf unterschiedlichen Linksnebenklassen  $gH$  verschiedene Werte annimmt und auf allen Linksnebenklassen konstant ist.

**gesucht:** Ein vollständiger Satz von Generatoren  $S \subset G$  mit  $\langle S \rangle = H$

Um die Funktion  $f$  in einem Quantenalgorithmus zu nutzen, muss sie natürlich durch einen Quantenschaltkreis berechnet werden können. Das heißt, man muss  $A$  durch Zahlen repräsentieren und  $f$  mittels der unitären Transformation  $\hat{U}_f$  berechnen, die auf einen Zustand  $|g\rangle |b\rangle$  wie folgt wirkt:

$$\hat{U}_f(|g\rangle |b\rangle) = |g\rangle |b \oplus f(g)\rangle$$

wobei mit  $\oplus$  die bitweise Addition bezeichnet ist.

Fast alle auf Quantencomputern effizient lösbarere Probleme, für die kein effizienter klassischer Algorithmus bekannt ist, werden mithilfe des folgenden Quantenalgorithmus gelöst:

### Algorithmus 6.2

1. Präpariere den Anfangszustand  $|1_G, 1, 1\rangle |0\rangle$
2. Erzeuge eine Überlagerung aller Gruppenelemente (im Allgemeinen durch Anwendung von  $\hat{U}_{FT}^{-1}$ )

$$\frac{1}{\|G\|} \sum_{g \in G} |g\rangle |0\rangle$$

3. Wende  $\hat{U}_f$  an und erzeuge damit den Zustand

$$\frac{1}{\|G\|} \sum_{g \in G} |g\rangle |f(g)\rangle$$

4. Messe das letzte Register. Das Ergebnis sei  $x$ . Dann besteht das erste Register aus einer Überlagerung aller Gruppenelemente  $g \in G$  für die  $f(g) = x$  ist. Da  $f$  konstant auf allen Linksnebenklassen einer Untergruppe  $H \leq G$  ist, existiert ein  $c \in G$ , sodass sich der neue Zustand im ersten Register ergibt zu:

$$|cH\rangle = \frac{1}{\sqrt{\|H\|}} \sum_{h \in H} |ch\rangle$$

Da auch für den neuen Zustand  $\|cH\| = \sqrt{\langle cH | cH \rangle} = 1$  gelten muss, ändert sich der Vorfaktor entsprechend. Das letzte Register kann nun vernachlässigt werden.

5. Wende die Fouriertransformation an.

$$\hat{U}_{FT} |cH\rangle = \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \sqrt{\frac{d_\rho}{\|G\| \cdot \|H\|}} \sum_{h \in H} \rho(ch)_{ij} |\rho ij\rangle$$

6. Messe das erste Quantenregister  $|\rho\rangle$  (in der schwachen Form des Algorithmus) oder alle Register  $|\rho ij\rangle$  (in der starken Form) und bestimme  $\rho$  bzw. ein Tripel  $(\rho, i, j)$

7. Verwende  $\rho$  bzw.  $\rho, i$  und  $j$ , um klassisch ein Erzeugendensystem der versteckten Untergruppe zu berechnen.

Es soll nun erkundet werden, welche Information das Messen im vorletzten Schritt liefert. Die Wahrscheinlichkeit  $W_c(\rho, i, j)$ , einen bestimmten Zustand  $|\rho ij\rangle$  zu messen, unter der Voraussetzung, dass  $f$  gerade den Wert für die Linksnebenklasse  $cH$  geliefert hat, entspricht nach Postulat 4 dem Amplituden-Betragsquadrat:

$$W_c(\rho, i, j) = \frac{d_\rho}{\|G\| \cdot \|H\|} \left| \sum_{h \in H} \rho(ch)_{ij} \right|^2$$

## 6.1 Die schwache Form des Algorithmus

Man summiert über  $i$  und  $j$  auf, um die Wahrscheinlichkeit für das ausschließliche Messen der Darstellung  $\rho$  zu bestimmen.

$$W_c(\rho) = \sum_{i,j=1}^{d_\rho} W_c(\rho, i, j)$$

Für eine Matrix  $A$  kann man die folgende Norm definieren:

$$\|A\|^2 = \sum_{ij} |A_{ij}|^2 = \text{Sp}(A^\dagger A)$$

Damit kann man schreiben:

$$W(\rho)_c = \frac{d_\rho}{\|G\| \cdot \|H\|} \left\| \sum_{h \in H} \rho(ch) \right\|^2$$

Eine unitäre Matrix  $U$  mit  $U^\dagger U = 1$  verändert die Norm im folgenden Sinne nicht

$$\|UA\|^2 = \text{Sp}((UA)^\dagger UA) = \text{Sp}(A^\dagger U^\dagger UA) = \text{Sp}(A^\dagger A) = \|A\|^2$$

Da die Darstellung unitär gewählt wurden (das musste man schon, damit die Fouriertransformation selbst unitär ist), gilt  $\left\| \sum_{h \in H} \rho(ch) \right\| = \left\| \rho(c) \sum_{h \in H} \rho(h) \right\| = \left\| \sum_{h \in H} \rho(h) \right\|$  und man kann  $W(\rho)_c$  vereinfachen zu:

$$W(\rho)_c = \frac{d_\rho}{\|G\| \cdot \|H\|} \left\| \sum_{h \in H} \rho(h) \right\|^2$$

Damit können zwei wichtige Dinge festgestellt werden:

- Durch die Fouriertransformation ist die Zufälligkeit der Nebenklasse in der Überlagerung  $|cH\rangle = \frac{1}{\sqrt{\|H\|}} \sum_{h \in H} |ch\rangle$  eliminiert. Im Folgenden kann man also  $W(\rho)$  anstatt  $W_c(\rho)$  schreiben.
- Der Messwert  $x$  von  $f$  ist belanglos, da die Wahrscheinlichkeit für die Messung von  $\rho$  völlig unabhängig von ihm ist. Er liefert also keine zusätzliche Information.

Es soll nun versucht werden, das Ergebnis weiter zu vereinfachen.  $\rho$  ist eine irreduzible Darstellung für  $G$ , das heißt, es gibt keinen Untervektorraum der invariant ist unter der Wirkung von  $G$ . Dies muss jedoch nicht für die Untergruppe  $H \leq G$  gelten.  $\rho$  ist also i.A. keine irreduzible Darstellung für  $H$ . Beschränkt man  $\rho$  auf  $H$ , so kann  $\rho$  in einer geeigneten Basis wieder als direkte Summe irreduzibler, nichtäquivalenter Darstellungen  $\{\tau_1, \dots, \tau_k\}$  geschrieben werden:

$$\rho = (\chi_{\tau_1} | \chi_{\rho})_H \tau_1 \oplus \dots \oplus (\chi_{\tau_k} | \chi_{\rho})_H \tau_k$$

Dabei wurde das Skalarprodukt auf  $H$  beschränkt:

$$(\chi_{\tau} | \chi_{\rho})_H = \frac{1}{\|H\|} \sum_{h \in H} \overline{\chi_{\tau}(h)} \chi_{\rho}(h)$$

Es sei daran erinnert, dass in diesem Zusammenhang ein Vorfaktor dem mehrfachen Bilden einer direkten Summe entspricht, also:

$$(\chi_{\tau} | \chi_{\rho})_H \tau = \underbrace{\tau \oplus \dots \oplus \tau}_{(\chi_{\tau_i} | \chi_{\rho})_H \text{ mal}}$$

Man kann also schreiben:

$$\sum_{h \in H} \rho(h) = (\chi_{\tau_1} | \chi_{\rho})_H \sum_{h \in H} \tau_1(h) \oplus \dots \oplus (\chi_{\tau_k} | \chi_{\rho})_H \sum_{h \in H} \tau_k(h)$$

Für eine irreduzible Darstellung  $\tau$  gilt nach Korollar 4.20:

$$\sum_{h \in H} \tau(h) = \begin{cases} \|H\| & \text{falls } \tau = 1_H \\ 0 & \text{sonst} \end{cases}$$

Die Matrix hat also nur  $(\chi_{1_H} | \chi_{\rho})_H$  Einträge auf der Diagonalen, die zur trivialen Darstellung gehören. Alle anderen Komponenten sind Null.

Somit ist  $\|\sum_{h \in H} \rho(h)\|^2 = (\chi_{1_H} | \chi_{\rho})_H \|H\|^2$  und  $W(\rho)$  vereinfacht sich zu

$$W(\rho) = \frac{d_{\rho} \|H\|}{\|G\|} (\chi_{1_H} | \chi_{\rho})_H = \frac{d_{\rho}}{\|G\|} \sum_{h \in H} \chi_{\rho}(h) \quad (12)$$

Da die Spur unabhängig von der Basiswahl ist, gilt diese Gleichung basisunabhängig. Was sagt Gleichung 12 aus? Wenn man bei Messung eine Darstellung  $\rho$  ausgegeben wurde, weiß man, dass zumindest  $(\chi_{1_H} | \chi_{\rho})_H > 0$  ist. Dies liefert natürlich nur implizit Informationen über die versteckte Untergruppe. Es werden später einige Beispiele behandelt, bei denen diese implizite Information ausreicht, um mit polynomiellen Aufwand Generatoren der versteckten Untergruppe anzugeben.

## 6.2 Die starke Form des Algorithmus

Wenn man die Indizes  $i$  und  $j$  misst, ist die Wahrscheinlichkeitsverteilung  $W_c(\rho, i, j)$  i.A. nicht mehr von  $c$  unabhängig. Allerdings ist  $c$  nicht bekannt, daher mittelt man die Wahrscheinlichkeitsverteilung über alle möglichen uniform verteilten  $c \in G$  und definiert:

$$W(\rho, i, j) = \frac{1}{\|G\|} \sum_{c \in G} W_c(\rho, i, j)$$

Es wird nun bewiesen, dass allein das Messen des Spaltenindex  $j$  zusätzliche Informationen liefern kann. Dazu geht man von der Wahrscheinlichkeitsverteilung

$$W(\rho, i, j) = \frac{d_\rho}{\|G\|^2 \cdot \|H\|} \sum_{g \in G} \left| \sum_{h \in H} \rho(gh)_{ij} \right|^2$$

aus. Mithilfe der Schreibweise  $\rho(H) = \sum_{h \in H} \rho(h)$  kann man dies als

$$W(\rho, i, j) = \frac{d_\rho}{\|G\|^2 \cdot \|H\|} \sum_{g \in G} \left| \sum_{k=1}^{d_\rho} \rho(g)_{ik} \rho(H)_{kj} \right|^2$$

schreiben. Die Summe der Absolutquadrate kann als die Norm eines Vektors aufgefasst werden. Dazu wählen wir eine Nummerierung der Gruppenelemente  $G = \{g_1, \dots, g_{\|G\|}\}$ , womit sich folgende  $\|G\|$ -komponentige komplexwertige Vektoren  $\vec{v}_{ik}$  definieren lassen:

$$\vec{v}_{ik} = \begin{pmatrix} \rho(g_1)_{ik} \\ \vdots \\ \rho(g_{\|G\|})_{ik} \end{pmatrix}$$

Damit lässt sich  $W(\rho, i, j)$  als das Normquadrat  $\|\vec{v}\|^2 = (\vec{v}, \vec{v}) = \vec{v}^\dagger \vec{v}$  einer Linearkombination der Vektoren  $\vec{v}_{ik}$  darstellen:

$$W(\rho, i, j) = \frac{d_\rho}{\|G\|^2 \cdot \|H\|} \left\| \sum_{k=1}^{d_\rho} \rho(H)_{kj} \vec{v}_{ik} \right\|^2$$

Die  $\vec{v}_{ik}$  sind wegen der Orthogonalität der Fourierkoeffizienten ebenfalls bezüglich des Skalarprodukts  $(\vec{v}, \vec{w}) = \vec{v}^\dagger \vec{w}$  orthogonal:

$$(\vec{v}_{ik}, \vec{v}_{jl}) = \sum_{g \in G} \overline{\rho(g)_{ik}} \rho(g)_{jl} = \|G\| (\rho_{ik} | \rho_{jl}) = \frac{\|G\|}{d_\rho} \delta_{ij} \delta_{kl}$$

Daher folgt:

$$W(\rho, i, j) = \frac{d_\rho}{\|G\|^2 \cdot \|H\|} \sum_{k=1}^{d_\rho} |\rho(H)_{kj}|^2 \underbrace{\|\vec{v}_{ik}\|^2}_{=\|G\|/d_\rho} = \frac{1}{\|G\| \cdot \|H\|} \sum_{k=1}^{d_\rho} |\rho(H)_{kj}|^2 \quad (13)$$

Da die rechte Seite unabhängig von  $i$  ist, liefert der Zeilenindex keine Information. Es stellt sich die Frage, ob der gemessene Spaltenindex  $j$  Informationen über  $H$  liefert.

Grigni Schulman Vazirani und Vazirani zeigen in [GSV], dass bei einer zufälligen Basiswahl die Information von  $j$  vernachlässigbar ist, um zwischen konjugierten Untergruppen zu unterscheiden. Man muss also i.A die Eigenschaften einer geschickten gewählten Basis nutzen um das HSP zu lösen, wenn das Messen der Darstellung allein nicht weiterhilft. Wie im Folgenden erläutert wird, ist die schwache Form des Algorithmus im abelschen Gruppen immer ausreichend.

### 6.3 HSP für abelsche Gruppen

Das große Problem an Gleichung 12 ist, dass die Charakterfunktionen  $\chi_\rho$  zentrale Funktionen sind. Mit der Messung von  $\rho$  kann man also nicht zwischen konjugierten Untergruppen unterscheiden. Im abelschen Fall weiß man jedoch, dass jede Konjugationsklasse nur einelementig sein kann. Zwei verschiedene Untergruppen können also nicht konjugiert zueinander sein. Wichtiger noch, im Abelschen Fall sind die Darstellungen eindimensional und somit irreduzibel und identisch zu ihren Charakteren. Man kann also Satz 4.19 anwenden und schließen:

$$(\chi_{1_H} | \chi_\rho)_H = (1_H | \rho)_H = \begin{cases} 1 & \text{falls } \rho(h) = 1 \text{ für alle } h \in H \\ 0 & \text{sonst} \end{cases}$$

Jede gemessene Darstellung  $\rho$  ist also zumindest auf  $H$  gleich der trivialen Darstellung.

**Definition 6.3.** Für eine abelsche Gruppe  $G$  und eine Untergruppe  $H \leq G$  sei

$$H^\perp = \{\rho \in \hat{G} \mid \rho(h) = 1 \text{ für alle } h \in H\}$$

die orthogonale Gruppe der Darstellungen mit der Verknüpfung  $\circ$ . Diese ist definiert via  $(\rho \circ \tau)(h) = \rho(h) \cdot \tau(h)$ .

Dass für diese Menge sämtliche Gruppenaxiome erfüllt sind, lässt sich leicht überprüfen. Somit gilt für jedes gemessene  $\rho$ , dass  $\rho \in H^\perp$  ist.

Die Strategie ist also, solange Darstellungen zu messen, bis mit hoher Wahrscheinlichkeit eine vollständige Menge von Generatoren für  $H^\perp$  gefunden ist. Aus  $H^\perp$  muss dann  $H$  bestimmt werde.

Für den ersten Schritt hilft das folgende Theorem.

**Theorem 6.4.** Sei  $G$  eine endliche Gruppe und  $S$  eine Menge von  $t + \lceil \log \|G\| \rceil$  zufällig uniform gewählten Elementen  $g \in G$ . Die Wahrscheinlichkeit, dass  $S$  gerade die Gruppe generiert, also  $\langle S \rangle = G$  ist, lässt sich nach unten abschätzen durch

$$\text{Prob}(\langle S \rangle = G) \geq 1 - \frac{1}{2^t}$$

**Beweis (Skizze).** Sei  $r = \lceil \log \|G\| \rceil$ . Die Gruppe  $G$  mit  $\|G\| \leq 2^r$ , die für ihre Generation die größte Menge  $S \subset G$  benötigt, ist  $\mathbb{Z}_2^r$  (der  $r$ -dimensionale Vektorraum über  $\mathbb{Z}_2$ ). Er benötigt mindestens  $r$  Generatoren. Die Wahrscheinlichkeit, mit  $t + r$  zufällig gewählten Elementen  $G$  zu generieren, ist für diese Gruppe am geringsten. Es muss also die Wahrscheinlichkeit dafür nach unten abgeschätzt werden, dass ein  $S \subset G$  mit zufälligen  $t + r$  Elementen  $\mathbb{Z}_2^r$  aufspannt. Schreibt man die  $t + r$  Vektoren als Reihen einer  $(t + r) \times r$

Matrix, so muss diese vom (Spalten-)Rang  $r$  sein. Die Wahrscheinlichkeit, dass die erste Spalte nicht der Nullvektor ist, ist  $1 - 2^{-(r+t)}$ . Die Wahrscheinlichkeit, dass die zweite Spalte nicht der Nullvektor ist und linear unabhängig von der ersten ist, ist  $1 - 2^{-(r+t-1)}$ , u.s.w.. Also gilt für eine beliebige endliche Gruppe  $G$ :

$$\text{Prob}(\langle S \rangle = G) \geq \prod_{i=0}^{r-1} \left(1 - \frac{1}{2^{t+r-i}}\right)$$

Dieses Produkt lässt sich durch algebraische Umformung nach unten durch  $1 - 2^{-t}$  abschätzen. ■

Man kann also mit  $\mathcal{O}(\log(\|G\|))$  vielen Messungen von Darstellungen die Wahrscheinlichkeit exponentiell verkleinern, nicht die gesamte Gruppe  $H^\perp$  aufgespannt zu haben.

Für den zweiten Schritt, der Rekonstruktion von  $H$  aus  $H^\perp$ , definiert man zunächst:

$$H^{\perp\perp} = \{g \in G \mid \rho(g) = 1 \text{ für alle } \rho \in H^\perp\}$$

**Satz 6.5.** Sei  $G$  eine endliche abelsche Gruppe und  $H \leq G$  eine Untergruppe, so gilt

1.  $\|H^\perp\| = \frac{\|G\|}{\|H\|}$
2.  $H^{\perp\perp} = H$

**Beweis.** (ad 1) Es wird sich auf eine endliche Gruppe wie im Quantenalgorithmus 6.2 bezogen. Man kann also das Ergebnisse nutzen, die bisher über die Wahrscheinlichkeitsverteilung  $W(\rho)$  erarbeitet wurden. Die Fouriertransformation lässt das Skalarprodukt und damit insbesondere die Norm eines Quantenzustands invariant. Da der Ausgangszustand im Quantenalgorithmus auf 1 normiert war, gilt  $\sum_{\rho \in \hat{G}} W(\rho) = 1$ . Da im abelschen Fall gilt, dass

$$W(\rho) = \begin{cases} \frac{\|H\|}{\|G\|} & \text{falls } \rho \in H^\perp \\ 0 & \text{sonst} \end{cases}$$

kann man folgern, dass

$$\|H^\perp\| = \frac{\|G\|}{\|H\|}$$

(ad 2)  $H \subseteq H^{\perp\perp}$  lässt sich an der Definition ablesen.  $H^{\perp\perp} \subseteq H$  ist äquivalent zu der Aussage, dass für alle  $g \in G$  gilt

$$(\forall \rho \in H^\perp \rho(g) = 1) \Rightarrow g \in H$$

Zum Beweis wird die negierte Aussage zum Widerspruch geführt. Es wird also davon ausgegangen, dass ein  $g \notin H$  existiert, sodass für alle  $\rho \in H^\perp$  gilt  $\rho(g) = 1$ . Es wird ein solches gewählt und  $g_0$  genannt. Die Fourierkoeffizienten bilden ein VONS auf dem Funktionenraum der Funktionen  $f : G \rightarrow \mathbb{C}$ . Die Dimension des von  $H^\perp$  gebildeten Funktionenraumes ist also gerade  $\|H^\perp\|$ .

Da  $\rho \in H^\perp$  auf  $H$  konstant ist, ist es dies auch für alle Nebenklassen  $gH$ , wobei zumindest auf  $H$  und  $g_0H$  derselbe Wert angenommen wird. Der Funktionenraum kann also

durch höchstens  $\frac{\|G\|}{\|H\|} - 1$  Indikatorfunktionen für die Nebenklassen aufgespannt werden. Es folgt:

$$\|H^\perp\| \leq \frac{\|G\|}{\|H\|} - 1$$

Dies ist ein Widerspruch zu (1), was Aussage (2) beweist. ■

Der allgemeine Algorithmus für das Auffinden einer versteckten Untergruppe  $H$  in einer abelschen Gruppe  $G$  läuft also wie folgt ab:

### Algorithmus 6.6

1. Wende  $m = k + \lceil \log \|G\| \rceil$  mal den Quantenalgorithmus 6.2 an und messe Darstellungen  $R = \{\rho_1, \dots, \rho_m\}$ , um mit Wahrscheinlichkeit  $P_1 \geq 1 - 2^{-k}$  einen vollständigen Satz von Generatoren für  $H^\perp$  zu finden (d.h.  $\langle R \rangle = H^\perp$ ).
2. Um einen vollständigen Satz von Generatoren für  $H$  zu bestimmen, gelte nun, dass  $\langle \rho_1, \dots, \rho_m \rangle = H^\perp$ . Dann kann man nutzen, dass nach Satz 6.5 gilt:

$$h \in H \Leftrightarrow (\rho(h) = 1 \text{ für alle } \rho \in H^\perp) \Leftrightarrow (\rho_i(h) = 1 \text{ für } i = 1, \dots, m)$$

Es müssen also zufällig  $n = l + \lceil \log \|G\| \rceil$  gleichverteilte Lösungen des Gleichungssystems

$$\begin{aligned} \rho_1(h) &= 1 \\ \rho_2(h) &= 1 \\ &\vdots \\ \rho_m(h) &= 1 \end{aligned} \tag{14}$$

bestimmt werden, um mit Wahrscheinlichkeit  $P_2 \geq (1 - 2^{-k})(1 - 2^{-l})$  einen vollständigen Satz von Generatoren für  $H$  zu finden.

Das Gleichungssystem 14 lässt sich als lineares Gleichungssystem darstellen und in polynomieller Zeit lösen. In Abschnitt 4.5 wurde dargelegt, dass jede endliche abelsche Gruppe  $G$  gleich dem Produkt zyklischer Gruppen ist:

$$G = \langle a_1 \rangle \times \dots \times \langle a_k \rangle$$

Wobei jedes  $a_i$  die Ordnung  $\text{ord}(a_i) = n_i$  habe. Dann bildet

$$\rho_{l_1 \dots l_k}((a_1^{r_1}, \dots, a_n^{r_n})) = \prod_{j=1}^k \omega_{n_j}^{l_j \cdot r_j} = \exp\left(2\pi i \sum_{j=1}^k \frac{l_j \cdot r_j}{n_j}\right)$$

für  $0 \leq l_1 \leq n_1 - 1, \dots, 0 \leq l_k \leq n_k - 1$  eine vollständige Menge irreduzibler, nichtäquivalenter Darstellungen  $\hat{G}$ . Die gemessenen Darstellungen  $\rho_i$  sind dann eindeutig für  $i = 1, \dots, n$  durch Tupel  $r_i = (l_1^{(i)}, \dots, l_k^{(i)})$  bestimmt. Entsprechend wird ein Gruppenelement  $g = (a_1^{r_1}, \dots, a_n^{r_n}) \in G$  durch ein Tupel  $\gamma_g = (r_1^{(g)}, \dots, r_n^{(g)})$  bestimmt. Sei  $d = \text{kgV}(n_1, \dots, n_k)$  und  $\alpha_i = \frac{d}{n_i}$ , dann ist

$$\rho_i(g) = 1 \iff \sum_{j=1}^k \alpha_j \cdot l_j^{(i)} \cdot r_j^{(g)} \equiv 0 \pmod{d}$$

Das Gleichungssystem 14 entspricht dann der Matrixgleichung

$$\begin{pmatrix} \alpha_1 l_1^{(1)} & \alpha_2 l_2^{(1)} & \dots & \alpha_k l_k^{(1)} \\ \alpha_1 l_1^{(2)} & \alpha_2 l_2^{(2)} & \dots & \alpha_k l_k^{(2)} \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1 l_1^{(n)} & \alpha_2 l_2^{(n)} & \dots & \alpha_k l_k^{(n)} \end{pmatrix} \cdot \begin{pmatrix} r_1^{(g)} \\ r_2^{(g)} \\ \vdots \\ r_n^{(g)} \end{pmatrix} \equiv 0 \pmod{d}$$

Wählt man für die Anzahl  $k$  der Messungen in Schritt 1 und die Anzahl  $l$  der Lösungen, die in Schritt 2 zufällig bestimmt werden,  $k = l = \lceil \log \|G\| \rceil + 1$ , gibt der Algorithmus in einer Rechenzeit von  $\log \|G\|^{O(1)}$  einen vollständigen Satz von Generatoren für  $H$  mit einer Wahrscheinlichkeit von mindestens  $1 - \frac{1}{\|G\|}$  aus.

### 6.3.1 Beispiel: Simon's Problem

Es wird nun das Orakelproblem betrachtet, welches in Abschnitt 3.3 benutzt wurde, um die Klassen BQP und BPP relativ zu einem Orakel zu trennen.

#### Problem 6.7

**gegeben:** Ein  $n \in \mathbb{N}$  und ein Zufallsorakel  $O$  welches für jedes  $n$  eine Funktion  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  berechnet.

**promise:** Für die Konstruktion des Orakels  $O$  wird eine zufällige  $n$ -Bitfolge  $s_O(n) \neq 0 \dots 0$  und ein Zufallsbit  $b_O(n)$  gewählt. Falls  $b_O(n) = 0$  ist, ist  $f$  eine gleichverteilt zufällig gewählte, bijektive Funktion. Falls  $b_O(n) = 1$  ist, ist  $f$  eine gleichverteilt zufällig gewählte Funktion mit folgender Eigenschaft: Für alle  $x, y \in \{0, 1\}^n$  gilt  $f(x) = f(y) \Leftrightarrow y = x \oplus s_O(n)$ . Hierbei bezeichnet  $\oplus$  die bitweise XOR-Operation

**gesucht:** Mithilfe von Orakelanfragen an  $O$  soll  $b_O(n)$  bestimmt werden

Dies lässt sich auf das einfache abelsche HSP zurückführen, welches als Simon's Problem bekannt ist:

#### Problem 6.8

**gegeben:** Eine Gruppe  $G = (\mathbb{Z}_2^n, \oplus)$  und eine Funktion  $f : G \rightarrow G$

**promise:** Es existiert eine Untergruppe  $H = \langle s \rangle = \{0, s\} \leq G$  mit  $s \in G$ , sodass  $f$  auf unterschiedlichen Linksnebenklassen  $gH$  verschiedene Werte annimmt und auf allen Linksnebenklassen konstant ist.

**gesucht:** Den vollständigen Satz  $\{s\}$  von Generatoren für  $H$

Findet man  $s = 0$ , so ist  $b_O(n) = 0$  ansonsten ist  $b_O(n) = 1$ . Für diese Gruppe kann leicht die Fouriertransformation berechnet werden. Die Gruppe  $\mathbb{Z}_2^n$  ist ein direktes Produkt von  $n$  Gruppen vom Grad Zwei. Die irreduzible Darstellung, wie sie in Abschnitt 4.5 entwickelt wurde, lautet

$$\rho_k(l) = -1^{k \cdot l}$$

mit  $k = (k_1, \dots, k_n) \in \mathbb{Z}_2^n$ ,  $l = (l_1, \dots, l_n) \in \mathbb{Z}_2^n$  und  $k \cdot l := \sum_{j=1}^n k_j \cdot l_j$ . Damit lautet die Fouriertransformation  $\hat{U}_W$  auf einen Basisvektor angewandt

$$\hat{U}_W |l\rangle = \sum_{\rho \in \hat{G}} \sum_{i,j=1}^{d_\rho} \sqrt{\frac{d_\rho}{\|G\|}} \rho_{ij}(d) |\rho ij\rangle = \sum_{k \in \mathbb{Z}_2^n} \frac{1}{\sqrt{2^n}} (-1)^{k \cdot l} |k\rangle$$

Die Matrixelemente lauten damit

$$\langle l | \hat{U}_W | k \rangle = \frac{1}{\sqrt{2^n}} (-1)^{k \cdot l}$$

Dies ist die Walsh-Hadamard Matrix, welche mit  $(W_n)_{l,k}$  bezeichnet werden soll. Um eine schnelle Berechnung der Fouriertransformation mit elementaren Operationen zu gewinnen, betrachte man die rekursive Zerlegung der Walsh-Hadamard Matrix  $W_n$ :

$$W_n = \frac{1}{\sqrt{2}} \begin{pmatrix} W_{n-1} & W_{n-1} \\ W_{n-1} & -W_{n-1} \end{pmatrix} \text{ mit } W_0 = 1$$

Mithilfe der Hadamard-Matrix  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  lässt sich dieses Ergebnis umschreiben zu

$$W_n = H \otimes W_{n-1} = \underbrace{H \otimes \dots \otimes H}_{n\text{-mal}}$$

Ein  $l = (l_1, \dots, l_n) \in \mathbb{Z}_2^n$  werde mittels eines  $n$ -Qubit Zustands  $|l\rangle = |l_1\rangle \otimes \dots \otimes |l_n\rangle$  gespeichert. Weiterhin bezeichne  $\hat{H}$  die unitäre 1-Qubit Transformation deren Matrixelemente der Hadamard-Matrix entsprechen, also  $\langle i | \hat{H} | j \rangle = H_{ij}$ . Die Fouriertransformation lässt sich also effektiv durch Hintereinanderausführen von  $n$  1-Qubit Transformationen wie folgt ausführen:

$$\hat{U}_W |l\rangle = (\hat{H} \otimes \dots \otimes \hat{H}) |l_1\rangle \otimes \dots \otimes |l_n\rangle = (\hat{H} |l_1\rangle) \otimes \dots \otimes (\hat{H} |l_n\rangle)$$

### 6.3.2 Beispiel: Primzahlfaktorisierung mit dem Algorithmus von Shor

Mit dem von Peter Shor 1994 entwickelten Algorithmus ist es möglich, eine Zahl  $N$  in polynomieller Zeit (bzgl. der Anzahl  $n$  der sie darstellenden Bits) in ihre Primfaktoren zu zerlegen [PS]. Es wird im Folgenden beschrieben, wie sich das Problem der Faktorisierung auf das Auffinden einer Untergruppe  $\langle r \rangle$  der abelschen Gruppe  $\mathbb{Z}_N = (\{0, \dots, N-1\}, +_{(\text{mod } N)})$  zurückführen lässt. Die Gruppenoperation ist hier die Addition „+“ modulo  $N$ . Um die Erfolgswahrscheinlichkeit des Faktorisierungsalgorithmus anzugeben, benötigt man folgendes zahlentheoretisches Lemma, welches z.B. in [EJ] bewiesen wird:

**Lemma 6.9.** Für ein  $N \in \mathbb{N}$ ,  $N > 0$  sei  $\mathbb{Z}_N^* = \{y \in \mathbb{Z}_N \mid \text{GGT}(N, y) = 1\}$ . Sei  $N$  ungerade und aus  $k \geq 2$  Primfaktoren  $p_1, \dots, p_k$  zusammengesetzt. Es existieren also ganzzahlige Potenzen  $\alpha_1, \dots, \alpha_k \geq 1$  mit

$$N = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

Für ein  $y \in \mathbb{Z}_N^*$  sei  $r_y$  die Periode der Funktion  $f(a) = y^a \pmod{N}$ , dann gilt

$$\text{Prob}_{y \in \mathbb{Z}_N^*} (r_y \text{ ist ungerade oder } y^{r_y/2} + 1 \equiv 0 \pmod{N}) \leq 2^{-(k-1)}$$

**Korollar 6.10.** Für eine ungerade ganze Zahl  $N$ , die aus mindestens zwei unterschiedlichen Primfaktoren besteht und eine zufällige ganze Zahl  $y \leq N$ , wobei  $\text{GGT}(y, N) = 1$ , gilt mit Wahrscheinlichkeit  $P \geq 1/2$ , dass

$$\text{GGT}(y^{r/2} + 1, N) \cdot \text{GGT}(y^{r/2} - 1, N) = N$$

wenn  $r$  die Periode der Funktion  $f(a) = y^a \pmod{N}$  ist.

**Beweis.** Sei  $r$  die (kleinste) Periode der Funktion  $f$  für die für beliebige ganze Zahlen  $c$  gilt, dass  $f(c) = f(c + r)$ . Damit ist  $r$  die kleinste Zahl für die gilt:

$$y^r \equiv y^0 \equiv 1 \pmod{N} \text{ oder } y^r - 1 \equiv 0 \pmod{N} \quad (15)$$

Damit weiß man, dass

$$(y^{r/2} + 1)(y^{r/2} - 1) \equiv y^r - 1 \equiv 0 \pmod{N}$$

Da  $r$  die kleinste Zahl ist für die Gleichung 15 gilt, ist  $y^{r/2} - 1 \not\equiv 0 \pmod{N}$ . Da außerdem  $N$  aus  $k > 2$  Primfaktoren besteht, ist die Wahrscheinlichkeit, dass  $r$  ungerade ist oder  $y^{r/2} + 1 \equiv 0 \pmod{N}$  nach obigem Lemma durch  $1/2$  beschränkt.

Daher sind  $y^{r/2} + 1$  und  $y^{r/2} - 1$  Vielfache der Primfaktoren von  $N$ . Da auch  $N$  natürlich selbst Vielfaches seiner Primfaktoren ist, sind  $\text{GGT}(y^{r/2} + 1, N)$  und  $\text{GGT}(y^{r/2} - 1, N)$  Primfaktoren von  $N$ .

Damit kann nun das Faktorisierungsproblem einer Zahl  $N$  auf das folgende Problem zurückgeführt werden:

### Problem 6.11

**gegeben:** Die Gruppe  $G = \mathbb{Z}_N$  und ein  $y \in \mathbb{Z}_N^*$ .

**promise:** Die Funktion  $f_y(a) = y^a \pmod{N}$  ist konstant 1 auf der Untergruppe  $H = \langle r_y \rangle = \{0, r_y, 2r_y, 3r_y, \dots\}$  der Vielfachen der Periode  $r_y$  der Funktion  $f_y$ , nimmt auf unterschiedlichen Linksnebenklassen  $g + \langle r_y \rangle$  verschiedene Werte an und ist auf allen Linksnebenklassen konstant.

**gesucht:**  $r_y$ .

Gesucht ist hier kein Satz von Generatoren von  $\langle r_y \rangle$  sondern  $r_y$  selbst. Ansonsten ist dies ein Spezialfall des Hidden Subgroup Problems auf abelschen Gruppen und kann ebenso gelöst werden. Eine schnelle Quanten Fouriertransformation ist nur auf Gruppen  $\mathbb{Z}_q$  bekannt, wenn  $q$  eine Zweierpotenz ist. Man sucht zuerst so ein  $q$  mit  $N^2 \leq q \leq 2N^2$  und arbeitet auf der Gruppe  $\mathbb{Z}_q$  ( $f$  wird natürlich nicht verändert). Da hier eine besonders einfache abelsche Gruppe vorliegt, kann mit hoher Wahrscheinlichkeit aus einem Element der orthogonalen Gruppe  $\rho_l \in H^\perp$  bereits  $r_y$  bestimmt werden. Da die Gruppenoperation die Addition ist, hat  $\rho_l$  für ein  $m \in \mathbb{Z}_q$  die Form

$$\rho_l(m) = \omega_q^{lm} = e^{2\pi i \frac{lm}{q}}$$

Aus der Form von  $\rho_l$  sieht man, dass:

$$\rho_l(m) = 1 \text{ für alle } m \in \langle r_y \rangle \iff \text{ex. } s \in \mathbb{N} \text{ mit } l = s \cdot \frac{q}{r_y}$$

Es wurde gezeigt, dass jede gemessene Darstellung auf der Untergruppe gleich der trivialen Darstellung ist. Dies ist hier nicht mehr unbedingt der Fall, da hier  $q \neq N$  ist. Sei  $l$  eine gemessene Zahl deren Darstellung  $\rho_l$  trivial auf  $\langle r_y \rangle$  ist. Man misst mit der höchsten Wahrscheinlichkeit immer noch solch ein  $l$ . Mit hoher Wahrscheinlichkeit sind dann  $s$  und  $r_y$  teilerfremd und man kann durch Kürzen  $r_y$  bestimmen. Die Wahrscheinlichkeit ein  $l'$  zu messen, das nicht zu einer auf  $\langle r_y \rangle$  trivialen Darstellung gehört, ist nur in kleinen Umgebungen von  $l$  relevant. Wegen der Wahl von  $q \geq N^2$ , kann immer noch durch Partialbruchzerlegung  $r_y$  in polynomieller Zeit rekonstruiert werden. Eine sehr detaillierte Ausführung mit allen nötigen Beweisen über den Shor'schen Algorithmus findet man in [EJ].

In diesem Beispiel wurde deutlich, dass es prinzipiell möglich ist die exakte Fouriertransformation einer Gruppe (hier  $\mathbb{Z}_N$ ) durch eine effizient berechenbare Fouriertransformation einer anderen Gruppe (hier  $\mathbb{Z}_q$ ) zu approximieren und das HSP zu lösen. Kitaev konnte zeigen, dass dies für alle abelsche Gruppen möglich ist [AK]. Das HSP ist also in jedem Fall effizient auf Quantencomputern lösbar.

## 6.4 HSP für nichtabelsche Gruppen

In Abschnitt 6.3 wurde erläutert, wie für *abelsche* Gruppen das Auffinden von versteckten Untergruppen auf Quantencomputern in polynomiellen Aufwand möglich ist. Geht man nun den Schritt zu *nichtabelschen* Gruppen, steht man vor gewichtigen Problemen

- Mit der Messung einer Darstellung  $\rho$  allein kann nicht zwischen konjugierten Untergruppen unterschieden werden. Da die gesuchte Untergruppe  $H$  konjugiert zu einer anderen Untergruppe sein kann, muss man auch den Zeilen- und Spaltenindex von  $\rho$  betrachten und die starke Form des Algorithmus 6.2 verwenden.
- Für eine gegebene Gruppe  $G$  ist die Wahl des Satzes von irreduziblen Darstellungen  $\hat{G}$  nur noch eindeutig bis auf eine Basistransformation. Der gemessene Zeilen- und Spaltenindex ist also basisabhängig. Welche Basis führt zum Erfolg?

Die bisher betrachteten Probleme im abelschen Fall sind leider nur mathematischer Natur oder wichtig für die Kryptographie. Von viel größerem Nutzen wäre jedoch das effiziente Lösen des nicht-abelschen Falls, womit so wichtige Probleme wie das Auffinden einer *Graphisomorphie* (GI) effizient lösbar wären. Im Folgenden werden positive und negative Resultate für den nichtabelschen Fall betrachten, um auszuloten, was mit den aktuell bekannten algorithmischen Verfahren auf Quantencomputern lösbar ist.

### 6.4.1 Normale Untergruppen

Für spezielle Klassen von Gruppen oder spezielle Klassen von versteckten Untergruppen führt der generische Algorithmus trotz der Hindernisse zum Erfolg. Der einfachste Fall ist der der *normalen Untergruppe*. Startpunkt ist wieder das Resultat aus Gleichung 12 aus, welches für den allgemeinen Fall der schwachen Form des Quantenalgorithmus abgeleitet wurde.

$$W(\rho) = \frac{d_\rho \|H\|}{\|G\|} (\chi_{1_H} | \chi_\rho)_H = \frac{d_\rho}{\|G\|} \sum_{h \in H} \chi_\rho(h)$$

Im abelschen Fall konnte man nun ausnutzen, dass die irreduziblen Darstellungen ein-dimensional sind und daher wegen  $(\chi_{1_H} | \chi_\rho)_H = (1_H | \rho)_H$  jede gemessene Darstellung auf der Untergruppe  $H$  gleich der trivialen Darstellung ist. Von da ausgehend konnte man über die Definition von  $H^\perp$  und  $H^{\perp\perp}$  zeigen, wie sich  $H$  von einer polynomiellen Anzahl von Messungen von Darstellungen rekonstruieren lässt.

Dies ist in ähnlicher Weise möglich, falls  $H \triangleleft G$  eine normale Untergruppe ist, wie das folgende Lemma zeigt.

**Lemma 6.12.** *Sei  $G$  eine Gruppe und  $H \triangleleft G$  eine normale Untergruppe, so ist die Wahrscheinlichkeit  $W(\rho)$  die Darstellung  $\rho \in \hat{G}$  in der schwachen Form des Algorithmus 6.2 zu messen, gegeben durch*

$$W(\rho) = d_\rho^2 \frac{\|H\|}{\|G\|} \cdot \begin{cases} 1 & \text{wenn } \rho(h) = \mathbb{1}_{d_\rho} \text{ für alle } h \in H \\ 0 & \text{sonst} \end{cases}$$

**Beweis.** Die Darstellung  $\tau : G \rightarrow GL_{\mathbb{C}}(V)$  sei definiert wie die Permutationsdarstellung der Faktorgruppe  $G/H$  wirkt. Man ordnet also jeder Nebenklasse  $gH$  von  $H$  einen Basisvektor  $e_{gH}$  des  $\frac{\|G\|}{\|H\|}$ -dimensionalen Vektorraums  $V$  zu. Die Darstellung  $\tau(g')$  ist dann eine Permutationsmatrix, die jeden Basisvektor  $e_{gH}$  auf den Basisvektor  $e_{g'gH}$  abbildet.

Da  $H$  eine normale Untergruppe ist, gilt für alle  $h \in H$  und  $g \in G$

$$hgH = hHg = Hg = gH \implies e_{hgH} = e_{gH} \implies \tau(h) = \mathbb{1}_{d_\tau}$$

Andererseits gilt für ein  $g' \in G \setminus H$  immer  $g'H \neq H$ , weswegen  $\tau(g')$  eine Permutationsmatrix ist, die alle Basisvektoren permutiert, deren Diagonaleinträge also alle Null sind. Damit kann man den Charakter von  $\tau$  angeben:

$$\chi_\tau(g) = \begin{cases} \frac{\|G\|}{\|H\|} & \text{falls } g \in H \\ 0 & \text{sonst} \end{cases}$$

Damit folgt für ein  $\rho \in \hat{G}$

$$\begin{aligned} (\chi_\tau | \chi_\rho) &= \frac{1}{\|G\|} \sum_{g \in G} \overline{\chi_\tau(g)} \chi_\rho(g) \\ &= \frac{1}{\|G\|} \frac{\|G\|}{\|H\|} \sum_{h \in H} \chi_\rho(h) \\ &= (\chi_{1_H} | \chi_\rho)_H \end{aligned}$$

Da letztlich die Wahrscheinlichkeit der Messung einer Darstellung nur von deren Spur abhängt, kann wieder von einer geeigneten Basiswahl ausgegangen werden, in der sich  $\tau$  als direkte Summe von irreduziblen, nichtäquivalenten Darstellungen  $\hat{G} = \{\rho_1, \dots, \rho_k\}$  schreiben lässt. Also  $\tau = (\chi_{\rho_1} | \chi_\tau) \rho_1 \oplus \dots \oplus (\chi_{\rho_k} | \chi_\tau) \rho_k$

Wenn für alle  $h \in H$  die Matrix  $\tau(h)$  gleich der Einheitsmatrix ist, so muss dies auch für alle Matrizen  $\rho_i$  gelten für die  $(\chi_{\rho_i} | \chi_\tau) \neq 0$  ist. Man kann also für ein beliebiges  $\rho \in \hat{G}$  folgern:

$$(\forall h \in H \rho(h) = \mathbb{1}_{d_\rho}) \iff (\chi_\rho | \chi_\tau) = \frac{1}{\|H\|} \sum_{h \in H} \chi_\rho(h) \neq 0$$

Damit kann abgeleitet werden, dass

$$\sum_{h \in H} \chi_\rho(h) = \begin{cases} d_\rho \|H\| & \text{wenn } \rho(h) = \mathbb{1}_{d_\rho} \text{ für alle } h \in H \\ 0 & \text{sonst} \end{cases}$$

Und es folgt aus Gleichung 12 direkt die Behauptung. ■

Für eine Darstellung  $\rho \in \hat{G}$  sei deren Kern definiert als  $\ker(\rho) = \{g \in G \mid \rho(g) = \mathbb{1}_{d_\rho}\}$ . Misst man nun Darstellungen  $\{\rho_1, \dots, \rho_k\}$ , dann gilt wegen Lemma 6.12 für die versteckte Untergruppe  $H \subseteq \bigcap_{i=1}^r \ker(\rho_i)$ . Dass eine polynomielle Anzahl von Messungen ausreicht, um die gesamte versteckte Untergruppe zu bestimmen, konnten Hallgren Russell und Ta-Shma in [HRT] beweisen. Sie zeigen folgenden Satz:

**Satz 6.13.** Seien  $\{\rho_1, \dots, \rho_k\}$  unabhängig nach dem Quantenalgorithmus gemessene Darstellungen mit  $k = c \log_2 \|G\|$ , dann gilt

$$\text{Prob} \left( H \neq \bigcap_{i=1}^r \ker(\rho_i) \right) \leq e^{-\frac{(c-2)^2}{2c} \log_2 \|G\|}$$

Nach diesem Resultat sollte man jedoch nicht vergessen, dass im Allgemeinen auch für eine versteckte *normale* Untergruppe zwei Hürden im Weg stehen:

- Die Fouriertransformation der Gruppe muss in Polynomialzeit auf Quantencomputern berechenbar sein
- Zur Bestimmung der versteckten Untergruppe musste in Algorithmus 6.6 für  $k$  gemessene Darstellungen  $\rho_1, \dots, \rho_k$  zufällige Lösungen des Gleichungssystems  $\rho_i(g) = 1$  für  $1 \leq i \leq k$  bestimmt werden. Für die irreduziblen Darstellungen im abelschen Fall war dies effizient möglich. Es ist jedoch kein allgemeiner effizienter Algorithmus für die Berechnung der Schnittmenge der Kerne der gemessenen Darstellungen im nichtabelschen Fall bekannt.

## 6.4.2 Einige effizient lösbare Fälle des nichtabelschen HSP

Trotz der auftretenden Probleme konnten für einige nichtabelsche Fälle des HSP effiziente Quantenalgorithmen gefunden werden. Da jedoch das Verständnis der Ergebnisse einen tieferen Einstieg in die Gruppentheorie benötigt, werden hier nur einige Ergebnisse exemplarisch genannt.

**Definition 6.14.** Für jedes ganzzahlige  $n$  und  $q$  und jeden Gruppenhomomorphismus  $\phi : \mathbb{Z}_q \rightarrow \text{Aut}(\mathbb{Z}_n)$  von der Gruppe  $\mathbb{Z}_q$  in die Gruppe der Automorphismen auf  $\mathbb{Z}_n$  ist das semidirekte Produkt  $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_q$  die Menge  $\{(a, b) \mid a \in \mathbb{Z}_n, b \in \mathbb{Z}_q\}$  mit der Gruppenoperation  $(a_1, b_1)(a_2, b_2) = (a_1 + \phi(b_1)(a_2), b_1 + b_2)$ .

**Beispiel 6.15.** Die Diedergruppe  $D_n$  ist die Symmetriegruppe der Drehungen und Spiegelungen eines regelmäßigen  $n$ -Ecks. Also  $D_n = \langle r, s \mid r^n = s^2 = e, srs = r^{-1} \rangle$ . Diese Gruppe ist isomorph zu  $\mathbb{Z}_n \rtimes_{\phi} \mathbb{Z}_2$  wobei  $\phi(0)$  die Identität und  $\phi(1)$  die Inversion beschreibt. Dass diese Gruppe gerade die Bedingungen der Diedergruppe erfüllt, ist leicht einzusehen, wenn man  $r = (1, 0)$  und  $s = (0, 1)$  setzt.

**Beispiel 6.16.** Die  $q$ -hedralen Gruppen sind gegeben durch  $\mathbb{Z}_{p^r} \rtimes_{\phi} \mathbb{Z}_q$  wobei  $r \geq 1$  ist und  $p$  und  $q$  Primzahlen sind, für die gilt  $q \mid p - 1$ . Man kann wie in [IG] zeigen, dass für beliebige  $\phi$  die  $q$ -hedralen Gruppen isomorph sind. Man schreibt daher kürzer  $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_q$ .

Einige Probleme, die nun vorgestellt werden, sind zwar nicht beweisbar in BQP aber das polynomiell häufige Anwenden des Quantenalgorithmus 6.2 liefert Messergebnisse aus denen sich prinzipiell die versteckte Untergruppe rekonstruieren lässt, auch wenn die klassische Nachbearbeitungszeit exponentiell ansteigen kann. Dies wird als *mess-rekonstruierbar* bezeichnet (aus dem Engl. *measurement reconstructible* wie in [CM]). Es ist dennoch ein wichtiges Ergebnis, da i.A. das Messen der Darstellung für das Auffinden nicht normaler versteckter Untergruppen in nichtabelschen Gruppen unzureichend ist, da so nicht zwischen konjugierten Nebenklassen unterschieden werden kann. Dazu ist immer zumindest auch das Messen des Zeilenindex der Darstellungsmatrix  $\rho$  nötig (starke Form des Algorithmus 6.2). Lange Zeit war nicht klar, ob man Gruppen  $G$  und Mengen irreduzibler Darstellungen  $\hat{G}$  finden kann, für die die starke Form Vorteile gegenüber der schwachen Form hat. Die folgenden Ergebnisse aus [CM] zeigen dies jedoch.

**Satz 6.17.** Seien  $p$  und  $q$  Primzahlen mit  $q = (p - 1)/\text{polylog}(p)$ , dann ist das HSP über  $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$  in BQP.

Sei  $p$  eine Primzahl und  $q$  ein Teiler von  $p - 1$ , dann ist das HSP über der  $q$ -hedralen Gruppe  $G = \mathbb{Z}_p \rtimes \mathbb{Z}_q$  mess-rekonstruierbar.

Inui und Le Gall konnten in [IG] des weiteren zeigen:

**Satz 6.18.** Sei  $p$  eine Primzahl und  $r > 1$  eine ganze Zahl, dann ist das HSP über  $G = \mathbb{Z}_{p^r} \rtimes \mathbb{Z}_p$  in BQP.

Für den anschaulichen Fall der Diedergruppe zeigten Ettinger und Høyer in [EH]:

**Satz 6.19.** Das HSP über der Diedergruppe  $D_n = \mathbb{Z}_n \rtimes_{\phi} \mathbb{Z}_2$  ist mess-rekonstruierbar.

Dazu verwenden sie statt der Fouriertransformation über die nichtabelsche Gruppe  $\mathbb{Z}_n \rtimes_{\phi} \mathbb{Z}_2$  die Fouriertransformation über die abelsche Gruppe  $\mathbb{Z}_n \times \mathbb{Z}_2$ , welche ausreicht um genügend Informationen über die versteckte Untergruppe zu erlangen.

## 6.5 Das Graphisomorphieproblem als negatives Resultat

Eine weiterhin offene Frage ist, ob das wichtige Graphisomorphieproblem (GI) in BQP liegt. Viele Resultate der letzten Jahre zeigen, dass sich dieses Problem mit den herkömmlichen Mitteln der Quanten-Fourieranalyse nicht effizient lösen lässt. Zunächst soll das Graphisomorphieproblem definiert werden.

Für einen ungerichteten Graphen  $G = (V, E)$  und eine Bijektion  $\phi : V \rightarrow W$  sei  $\phi(E) = \{\{\phi(v), \phi(w)\} \mid \{v, w\} \in E\}$  und  $\phi(G) = (W, \phi(E))$ .

**Definition 6.20.** Zwei ungerichtete Graphen  $G_1 = (V_1, E_1)$  und  $G_2 = (V_2, E_2)$  heißen isomorph zueinander (geschrieben  $G_1 \cong G_2$ ), falls eine Bijektion  $\phi : V \rightarrow W$  existiert, sodass für alle  $v, w \in V$

$$\{v, w\} \in E_1 \Leftrightarrow \{\pi(v), \pi(w)\} \in E_2$$

Die Bijektion  $\phi$  heißt Isomorphismus zwischen  $G_1$  und  $G_2$  und es gilt  $\phi(G_1) = G_2$ . Ein Automorphismus für  $G_1$  ist eine Permutation  $\pi$  auf  $V$ , sodass für alle  $v, w \in V$

$$\{v, w\} \in E_1 \Leftrightarrow \{\pi(v), \pi(w)\} \in E_1$$

Es gilt  $\pi(G) = G$

Die Menge der Automorphismen  $\text{Aut}(G)$  eines Graphen  $G = (V, E)$  ist immer eine Untergruppe der symmetrischen Gruppe  $\text{Sym}(V)$ . Die folgenden Probleme sind im weiteren Verlauf von Belang.

**Problem 6.21 (Graphisomorphieproblem)**

**gegeben:** Zwei ungerichtete Graphen  $G_1$  und  $G_2$

**gefragt:** Ist  $G_1$  isomorph zu  $G_2$ ?

**Problem 6.22 (Graphautomorphieproblem)**

**gegeben:** Ein ungerichteter Graphe  $G$

**gefragt:** Existiert ein Automorphismus  $\pi \neq \text{id}$  von  $G$

Das Graphisomorphieproblem ist ein für die Komplexitätstheorie sehr interessantes Problem, da es ein Kandidat für ein Problem ist, das weder in P liegt noch NP-vollständig ist. Köbler, Schöning und Torán zeigen in [KST], dass, wenn GI NP-vollständig ist, die Polynomialzeithierarchie auf  $\text{BP} \cdot \text{NP}$  kollabiert, wovon man nicht ausgeht.

Wie lässt sich GI für zwei ungerichtete Graphen  $G_1$  und  $G_2$  auf eine Instanz des HSP zurückführen? Man kann ohne Beschränkung der Allgemeinheit davon ausgehen, dass  $G_1 = (\{1, \dots, n\}, E_1)$  und  $G_2 = (\{n+1, \dots, 2n\}, E_2)$  zusammenhängend sind. Sind die Graphen nicht zusammenhängend, kann dies immer durch Komplementierung der Kantenmenge der Graphen erreicht werden. Sei nun  $G = ([2n], E_1 \cup E_2)$  die disjunkte Vereinigung der beiden Graphen. Dabei bezeichne  $[2n]$  die Menge der natürlichen Zahlen von 1 bis  $2n$ .

Eine Permutation  $\pi$  auf  $\{1, \dots, n\}$  oder  $\{n+1, \dots, 2n\}$  sei durch die Identität auf ganz  $[2n]$  fortgesetzt. Sei nun  $H = \{\pi_1 \circ \pi_2 \mid \pi_1 \in \text{Aut}(G_1), \pi_2 \in \text{Aut}(G_2)\}$  die Mengen der Automorphismen von  $G_1$  und  $G_2$ . Falls  $G_1$  und  $G_2$  isomorph sind, beschreibe  $\sigma \in S_{2n}$  einen Isomorphismus zwischen  $G_1$  und  $G_2$ .

Damit gilt, da  $G_1$  und  $G_2$  zusammenhängend sind Folgendes:

- Sind  $G_1$  und  $G_2$  nicht isomorph, dann gilt  $\text{Aut}(G) = H$
- Sind  $G_1$  und  $G_2$  isomorph, dann gilt  $\text{Aut}(G) = H \cup \sigma H$

Kennt man also die Untergruppe  $\text{Aut}(G) \leq S_{2n}$ , so kann man entscheiden ob  $G_1$  und  $G_2$  isomorph sind. Man muss eigentlich nur wenige Elemente von  $\text{Aut}(G)$  kennen, da im Fall 2 die Hälfte der Elemente in  $\sigma H$  sind, welche man daran erkennen kann, dass  $\pi(1) > n$  für diese gilt. Mit Lösung des folgenden nichtabelschen HSP könnte man also GI lösen.

### Problem 6.23

**gegeben:** Die Symmetriegruppe  $S_n$  eines Graphen  $G = ([n], E)$

**promise:** Die Funktion  $f(\pi) = \pi(G)$  für  $\pi \in S_n$  ist konstant auf der Untergruppe  $\text{Aut}(G) \leq S_n$  und allen ihrer Linksnebenklassen, wobei  $f$  auf unterschiedlichen Linksnebenklassen unterschiedliche Werte annimmt.

**gefragt:** Existiert ein  $\sigma \in \text{Aut}(G)$  mit  $\pi(1) > n$  ?

### 6.5.1 Darstellungstheorie der symmetrischen Gruppe

Im Folgenden soll kurz die Darstellungstheorie der symmetrischen Gruppe behandelt werden, da sie einen Grundbaustein der danach folgenden Ergebnisse bildet. Sie ist eine wichtige mathematische Theorie, die viele Anwendungen in der Theorie der symmetrischen Funktionen, der Kombinatorik und auch der Physik der Elementarteilchen hat. Eine ausführliche Einleitung findet man in [FH]. Die symmetrische Gruppe  $S_n$  besteht aus  $n!$  Permutationen, die man explizit als  $\pi = [\pi(1)\pi(2) \dots \pi(n)]$  angeben kann. Das neutrale Element der Gruppe ist also  $id = [1\ 2 \dots n]$ . Jede Permutation lässt sich in eindeutiger Weise als Produkt von disjunkten zyklischen Vertauschungen von Untermengen von  $[n]$  angeben, was an folgendem Beispiel klar wird

**Beispiel 6.24.** Die Permutation  $\pi = [1\ 6\ 5\ 2\ 3\ 4]$  besteht aus den Zyklen  $1 \rightarrow 1$ ,  $3 \rightarrow 5 \rightarrow 3$  und  $2 \rightarrow 6 \rightarrow 4 \rightarrow 2$  der Ordnung 1, 2 und 3, welche die Menge der zyklisch vertauschten Elemente angibt.

Die Summe der Ordnung der Zyklen ist natürlich  $n$ . Ordnet man sie absteigend der Größe nach sortiert an, erhält man eine *Partition* von  $n$ .

**Definition 6.25.** Eine Partition von  $n \in \mathbb{N} \setminus \{0\}$  ist eine Sequenz

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$$

von natürlichen Zahlen größer Null mit  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$  und  $\lambda_1 + \lambda_2 + \dots + \lambda_k = n$ . Dies sei mit  $\lambda \vdash n$  gekennzeichnet.

**Bemerkung 6.26.** Für die Anzahl  $p(n)$  der für ein  $n \in \mathbb{N}$  möglichen Partitionen  $\lambda \vdash n$  konnte bisher keine explizite Formel gefunden werden. Dennoch weiß man, dass asymptotisch gilt:

$$p(n) \sim \frac{1}{\alpha n} e^{\beta \sqrt{n}}$$

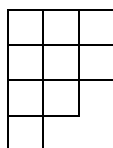
mit  $\alpha = 4\sqrt{3}$  und  $\beta = \sqrt{2/3}$ .

Die durch eine Permutation  $\pi$  definierte Partition  $\lambda = \lambda(\pi)$  von  $n$  nennt man *Zyklentyp* (engl. *cycle type*) von  $\pi$ . Es zeigt sich, dass zwei Permutationen genau dann konjugiert zueinander sind, wenn sie denselben Zyklentyp haben. Dazu mache man sich klar, dass für zwei konjugierte Permutationen  $\pi, \pi'$  mit  $\pi = \sigma \pi' \sigma^{-1}$  die Permutation  $\sigma$  nur zu einer Umbenennung der Objekte in der Zyklenbeschreibung der Permutation  $\pi'$  führt. Der Zyklentyp von  $\pi$  und  $\pi'$  ist also derselbe. Andererseits lässt sich für zwei Permutationen  $\pi, \pi'$  mit selbem Zyklentyp immer eine Umbenennung der Elemente  $\sigma$  finden, sodass  $\pi = \sigma \pi' \sigma^{-1}$ .

Man kann also jede Konjugationsklasse von  $S_n$  eindeutig durch eine Partition  $\lambda \vdash n$  benennen. Da nach Korollar 4.23 die Anzahl der irreduziblen Darstellungen  $\|\hat{S}_n\|$  gleich der Anzahl der Konjugationsklassen ist, kann auch jede Darstellung  $\rho \in \hat{S}_n$  durch eine Partition  $\lambda \vdash n$  benannt werden.

**Die irreduziblen Darstellungen von  $S_n$**  Die Zuordnung von Partitionen  $\lambda \vdash n$  zu irreduziblen Darstellungen von  $S_n$  soll hier kurz erläutert werden, da sie die Grundlage des folgenden Lemmas 6.27 darstellt. Da hier aber nicht der Beweis des Lemmas erfolgen soll, kann man auch ab Abschnitt 6.5.2 weiterlesen, ohne den Ursprung des Lemmas zu kennen.

Jede Partition  $\lambda \vdash n$  kann man durch ein so genanntes *Young-Diagramm* graphisch darstellen. Dazu zeichnet man für  $\lambda = (\lambda_1, \dots, \lambda_k)$  zuerst  $\lambda_1$  Quadrate nebeneinander, darunter linksbündig  $\lambda_2$  Quadrate u.s.w. bis  $\lambda_k$ . Zum Beispiel ist für  $\lambda = (3, 3, 2, 1)$  das zugehörige Young-Diagramm



Nummeriert man die Boxen eines Young-Diagramms mit Zahlen 1 bis  $n$  durch, sodass in jeder Zeile und Spalte die Zahlen in aufsteigender Reihenfolge auftreten, erhält man ein *Standard-Young-Tableau* (SYT). Ein SYT einer Partition  $\lambda$  wird als  $\lambda$ -SYT bezeichnet. Zum Beispiel ist für  $\lambda = (3, 3, 2, 1)$  das folgende Young-Tableau ein  $\lambda$ -SYT:

1	3	5
2	4	8
6	9	
7		

Zwei  $\lambda$ -SYT's seien äquivalent, wenn in jeder Zeile dieselben Zahlen auftreten. Die Äquivalenzklasse eines  $\lambda$ -SYT  $t$  bezeichnet man als  $\lambda$ -*Tabloid*, welches im Folgenden durch  $\{t\}$  gekennzeichnet wird. Ist  $\lambda \vdash n$  so wirkt die symmetrische Gruppe  $S_n$  in natürlicher Weise auf ein  $\lambda$ -SYT durch Vertauschung der Nummerierung. Wirkt  $\pi \in S_n$  auf ein  $\lambda$ -SYT  $t$  wird dies als  $\pi t$  geschrieben.

Es bezeichne  $M^\lambda$  einen Vektorraum mit der Basis  $(e_{\{t\}} \mid \{t\} \text{ ist ein } \lambda\text{-Tabloid})$ . Für  $\lambda \vdash n$  sei für jedes  $\lambda$ -SYT  $t$

$$C(t) = \{\pi \in S_n \mid \pi \text{ tauscht innerhalb der Spalten von } t\}$$

Dann definiert jedes  $t$  einen Vektor in  $M^\lambda$

$$\vec{v}_t = \sum_{\pi \in C(t)} \text{sgn}(\pi) e_{\{\pi t\}}$$

Wobei  $\text{sgn}(\pi)$  das Signum der Permutation ist, das gleich 1 ist falls  $\pi$  eine gerade Permutation ist und 0 sonst. Sei  $\lambda = (\lambda_1, \dots, \lambda_r)$  der Zyklentyp von  $\pi$ , dann ist  $\text{sgn}(\pi) =$

$-1^{\lambda_1+\dots+\lambda_r+r}$ . Damit kann für jede Partition  $\lambda \vdash n$  ein Unterraum  $S^\lambda$  von  $M^\lambda$  definiert werden, der als *Specht-Modul* bezeichnet wird und wie folgt definiert ist:

$$S^\lambda = \text{span}\{\vec{v}_t \mid t \text{ ist ein } \lambda\text{-SYT}\}$$

Jede Permutation  $\pi \in S_n$  induziert in natürlicher Weise eine Transformationsmatrix  $T_\pi$  in  $S^\lambda$  die jeden Vektor  $\vec{v}_t$  auf den Vektor  $\vec{v}_{\pi t}$  abbildet. Damit kann für jede Partition  $\lambda \vdash n$  eine Darstellung  $\rho_\lambda$  von  $S_n$  definiert werden mit

$$\rho_\lambda(\pi) = T_\pi \in GL(S^\lambda) \text{ für alle } \pi \in S_n$$

Es zeigt sich, dass die  $\rho_\lambda$  einen Satz von irreduziblen Darstellungen von  $S_n$  bilden, also

$$\hat{S}_n = \{\rho_\lambda \mid \lambda \vdash n\}$$

Wie man sich schnell klarmachen kann, ist für  $\lambda = (n)$  die Darstellung  $\rho_\lambda$  gleich der trivialen Darstellung und für  $\lambda = (1, \dots, 1)$  die eindimensionale Darstellung, die jeder Permutation  $\pi$  ihr Signum  $\text{sgn}(\pi)$  zuordnet. Die Dimension  $d_{\rho_\lambda}$  solch einer Darstellung  $\rho_\lambda$  mit  $\lambda \vdash n$  ist gegeben durch die Anzahl der  $\lambda$ -Standard-Young-Tableaux. Diese Anzahl lässt sich anschaulich mit der bemerkenswerten *Hook Length* Formel angeben.

$$d_{\rho_\lambda} = \frac{n!}{\prod_x \text{hook}(x)}$$

Dabei läuft das Produkt über alle Zellen des Young Tableau und für eine Zelle  $x$  bezeichnet  $\text{hook}(x)$  die Anzahl der Zellen in derselben Zeile rechts von  $x$  plus der Anzahl der Zellen in derselben Spalte unterhalb von  $x$  plus 1. In folgendem Diagramm ist  $\text{hook}(x)$  in alle Zellen  $x$  eingetragen.

6	4	2
5	3	1
3	1	
1		

Mithilfe des entwickelten Satzes von irreduziblen Darstellungen der symmetrischen Gruppe und den Eigenschaften der Young Tableaux lassen sich wichtige Aussagen über die Charaktere der irreduziblen Darstellungen beweisen. Eine dieser Eigenschaften stellt das nun folgende Lemma 6.27 dar. Näheres zu Young-Tableaux findet man in [WF].

### 6.5.2 GI ist nicht mithilfe des Quantenalgorithmus lösbar

Für den zu  $\rho_\lambda$  gehörenden Charakter  $\chi_\lambda$  konnten Hallgren Russel und Ta-Shma in [HRT] folgende Abschätzung beweisen

**Lemma 6.27.** *Sei  $\lambda \vdash n$  eine Partition von  $n$ , dann gilt für den Charakter  $\chi_\lambda$  der Darstellung  $\rho_\lambda$  und für alle  $\pi \in S_n$*

$$|\chi_\lambda(\pi)| \leq 4^n (2\sqrt{n})^{n/2}$$

Damit kann nun bewiesen werden, dass GI nicht durch die schwache Form des Quantenalgorithmus lösbar ist. Dazu wird der folgende Spezialfall des Graphisomorphieproblems für zwei ungerichtete Graphen  $G_1 = (\{1, \dots, n\}, E_1)$  und  $G_2 = (\{n+1, \dots, 2n\}, E_2)$  betrachtet, die keinen nichttrivialen Automorphismus besitzen ( $\text{Aut}(G_1) = \text{Aut}(G_2) = \{id\}$ ). Sei nun  $G = ([2n], E_1 \cup E_2)$  wieder die disjunkte Vereinigung der Graphen, dann folgt

- $G_1 \not\cong G_2 \Rightarrow \text{Aut}(G) = \{id\}$
- $G_1 \cong G_2 \Rightarrow \text{Aut}(G) = \{id, \sigma\}$  wobei  $\sigma$  eine Permutation mit  $n$  disjunkten Zyklen der Ordnung 2 ist, die Knoten aus  $G_1$  und  $G_2$  vertauschen.

Um zu beweisen, dass die Information des schwachen Quantenalgorithmus nicht ausreicht, führt man eine Norm ein, die es gestattet, Wahrscheinlichkeitsverteilungen der Messung von  $\rho$  zu vergleichen. Dazu sei für zwei Wahrscheinlichkeitsverteilungen  $W_1, W_2 : \hat{G} \rightarrow [0, 1]$  der Abstand  $\|W_1 - W_2\|_1 = \sum_{\rho \in \hat{G}} |W_1(\rho) - W_2(\rho)| \in [0, 2]$  definiert. Mit dieser Definition lässt sich der folgende Satz formulieren:

**Satz 6.28.** *Für zwei Graphen  $G_1 = (\{1, \dots, n\}, E_1)$  und  $G_2 = (\{n+1, \dots, 2n\}, E_2)$  mit  $\text{Aut}(G_1) = \text{Aut}(G_2) = \{id\}$  sei  $G = ([2n], E_1 \cup E_2)$  die disjunkte Vereinigung der Graphen. Es soll das HSP für die versteckte Untergruppe  $H = \text{Aut}(G) \leq S_n$  gelöst werden. Sei  $W_1$  ( $W_2$ ) die Wahrscheinlichkeit der Messung von  $\rho \in \hat{S}_n$  in der schwachen Form von Algorithmus 6.2 wenn  $G_1 \cong G_2$  ( $G_1 \not\cong G_2$ ). Dann gilt für hinreichend große  $n$*

$$\|W_1 - W_2\|_1 \leq 2^{-\Omega(n)}$$

**Beweis.** *Es wurde bereits für den allgemeinen Fall abgeleitet, dass  $W(\rho) = \frac{d_\rho}{\|G\|} \sum_{h \in H} \chi_\rho(h)$ . Im Fall  $G_1 \cong G_2$  ist  $H = \{id\}$  und damit  $W_1 = \frac{d_\rho^2}{n!}$ . Im Fall  $G_1 \not\cong G_2$  ist  $H = \{id, \sigma\}$  mit  $\sigma \neq id$ . Damit ist  $W_2 = \frac{d_\rho}{n!}(d_\rho + \chi_\rho(\sigma))$ .*

*Es folgt also*

$$\begin{aligned} \|W_1 - W_2\|_1 &= \sum_{\rho \in \hat{S}_n} |W_1(\rho) - W_2(\rho)| \\ &= \sum_{\rho \in \hat{S}_n} \left| \frac{d_\rho}{n!} \chi_\rho(\sigma) \right| \\ \text{Lemma 6.27} \Rightarrow &\leq \sum_{\rho \in \hat{S}_n} \frac{d_\rho}{n!} 4^n (2\sqrt{n})^{n/2} \\ &\leq \frac{2^{\mathcal{O}(n)} \sqrt{n}^{n/2}}{\sqrt{n}!} = 2^{\mathcal{O}(n)} \sqrt{\frac{\sqrt{n}^n}{n!}} \\ &\leq \frac{2^{\mathcal{O}(n)}}{(\sqrt{n}/e)^n \sqrt{2\pi n}} \ll 2^{-\Omega(n)} \end{aligned}$$

*Die zweite Ungleichung folgt, da wegen Gleichung 9 gilt  $\sum_{\rho \in \hat{S}_n} d_\rho^2 = \|S_n\| = n!$ . Also ist  $d_\rho \leq \sqrt{n!}$ . Da zusätzlich für das in Bemerkung 6.26 definierte  $p(n)$  gilt  $\|\hat{S}_n\| = p(n)$ ,*

kann man für hinreichend große  $n$  ableiten:

$$\sum_{\rho \in \hat{S}_n} d_\rho \leq \left\| \hat{S}_n \right\| \sqrt{n!} \leq \sqrt{n!} \cdot 2^{\mathcal{O}(\sqrt{n})}$$

Die letzte Ungleichung folgt aus der Stirling Formel für große  $n$

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n} \left(1 + \frac{1}{12n} + \dots\right)$$

Damit folgt die Behauptung. ■

Da sich die Wahrscheinlichkeitsverteilungen für die zwei Fälle nur exponentiell wenig unterscheiden, müssen exponentiell viele Messungen durchgeführt werden, um den isomorphen vom nicht isomorphen Fall zu unterscheiden. Dieses Ergebnis ist nicht allzu überraschend, da natürlich von vornherein klar war, dass die schwache Form des Quantenalgorithmus nicht zwischen konjugierten Untergruppen unterscheiden kann und damit den allgemeinen Fall von GI nicht lösen kann. Jedoch sind die Gruppen  $\{id\}$  und  $\{id, \sigma\}$  dieses Spezialfalles *nicht* konjugiert zueinander. Dennoch unterscheiden sich die zugehörigen Wahrscheinlichkeitsverteilungen zu wenig, um sie zu unterscheiden. Außerdem hilft die Behandlung dieses recht einfachen Ergebnisses, den folgenden Satz zu verstehen und zu würdigen, dessen Beweis noch mehr des aktuellen Wissens über die Darstellung der symmetrischen Gruppe ausschöpft. Eine genauere Behandlung des Beweises, der von Moore, Russel und Schulmann gegeben wurde, findet sich in in [MRS].

**Satz 6.29.** Sei  $H = \{id, \sigma\} \leq S_n$  wobei  $\sigma$  zufällig gleichverteilt aus  $M = \{\pi [2\ 1\ 4\ 3 \dots n-1\ n] \pi^{-1} \mid \pi \in S_n\}$  gewählt wird. Für eine Darstellung  $\rho_\lambda$  sei  $B_\lambda = \{e_i\}$  ein beliebiges VONS des Darstellungsraums von  $\rho_\lambda$ . Sei  $W_\lambda(j)$  die Wahrscheinlichkeit in der starken Form des Algorithmus 6.2 den Spaltenindex  $j$  zu messen, wenn die Darstellung  $\rho_\lambda$  gemessen wurden, und sei  $U$  die Gleichverteilung auf  $\{1, \dots, d_{\rho_\lambda}\}$ . Dann existiert eine Konstante  $\delta > 0$ , sodass für hinreichend große  $n$  und für alle  $\lambda \vdash n$  mit mindestens Wahrscheinlichkeit  $1 - e^{-\delta n}$  gilt:

$$\|W_\lambda(j) - U\|_1 < e^{-\delta n}$$

Dieser Satz zeigt, dass neben dem Messen der Darstellung  $\rho_\lambda$  auch das zusätzliche Messen des Spaltenindex für eine allgemeine versteckte Untergruppe  $\sigma \in M$  wie sie beim GI auftritt, nur exponentiell wenig Information liefert. \*\* Dieses Ergebnis konnten Moore, Russel und Schulmann noch verallgemeinern. Danach liefert auch die Verwendung einer beliebigen vollständigen Basis des Darstellungsraumes anstatt einer Orthonormalbasis keinen Vorteil. Dies zeigt, dass die Anwendung des Quantenalgorithmus in seiner aktuellen Form zur Lösung des Graphisomorphieproblems unzureichend ist.

Ein weiterer hoffnungsvoller Ansatz basierte auf der Verwendung von  $k > 1$  Kopien des Zustandes  $|cH\rangle$ , auf denen die Fouriertransformation  $\hat{U}_{FT}^{\otimes k} |cH\rangle^{\otimes k}$  ausgeführt wird. Danach werden die Darstellungen  $\rho_1, \dots, \rho_k$  gemessen, allerdings erfolgt die Messung der Spaltenindizes *nicht* in der Standardbasis  $\{|i_1\rangle \otimes \dots \otimes |i_k\rangle\}$ , sondern in einer beliebigen orthogonalen Basis  $\mathcal{B}$ . Schon das Messen in einer anderen vollständigen orthonormalen

---

\*\*Der Zeilenindex lieferte, wie in Gleichung 13 gezeigt sowieso keine Information.

Basis entspricht einer Basistransformation durch eine unitäre Transformation, was eine sehr allgemeine Erweiterung darstellt. Die Anzahl  $k$  sollte also exponentiell klein gegen die Eingabelänge und somit gegen  $n$  sein. Hallgren, Rötteler und Sen konnten allerdings zeigen, dass selbst für den Spezialfall von GI mit zwei Graphen ohne nichttriviale Automorphismen  $k = \theta(n \log n)$  Kopien nötig und ausreichend sind [HRS]. Eine effiziente Lösung von GI auf Quantencomputern scheint also mit allen zur Zeit denkbaren algorithmischen Mitteln unmöglich.

## 7 Schlussbemerkung

Obwohl sich nicht beweisen lässt, dass BPP echt in BQP enthalten ist, also Quantencomputer eine größere Klasse von Problemen effizient lösen können als klassische Computer, wurde mit HSP eine Klasse von praktisch relevanten Problemen vorgestellt, die möglicherweise in BQP liegen. Im nichtabelschen Fall des HSP konnte man bisher jedoch nur wenige Spezialfälle in BQP ansiedeln. Es gibt jedoch auch ganz praktische Probleme in denen Quantencomputer den klassischen Pendanten überlegen sind. Grover konnte bereits 1996 einen Quantenalgorithmus angeben, der einen Eintrag in einer unsortierten Datenbank mit  $N$  Elementen in  $\mathcal{O}(\sqrt{N})$  finden kann [LG]. Auch wenn er keinen exponentielle Verbesserung gegenüber der klassischen Suche darstellt, könnte er benutzt werden, um die Lösung von NP-vollständigen Problemen zu beschleunigen. Ein weiteres sehr interessantes Einsatzgebiet ist das der Simulation von quantenmechanischen Systemen. Hier hilft die Fouriertransformation, die Lösungen der Differentialgleichung sehr viel schneller zu approximieren. Der praktisch sehr interessante Fall der Graphisomorphie scheint jedoch unüberwindbare Hürden bereitzuhalten. Ein weiteres in dieser Diplomarbeit gänzlich überangenes Problem ist das der praktischen Implementierung eines Quantencomputers. Ein physikalisches System, welches die Qubits implementiert, muss extrem gut gegenüber der Umgebung isoliert sein, da alles, was von außen über die Berechnung gemessen wird, zu einem Wellenfunktionskollaps und damit zu einer Störung der Berechnung führt. Andererseits muss das System sehr präzisen unitären Transformationen unterzogen werden. Diese gegensätzlichen Bestrebungen machen die Implementation extrem schwer. Auch wenn viele physikalische Systeme als Kandidaten für die Implementation vorgeschlagen wurden, gibt es trotz großer Fortschritte bisher kein System, welches sich praktisch für eine hohe Anzahl von Qubits implementieren lässt. Wir sind also wahrscheinlich noch viele Jahrzehnte vom ersten Quantencomputer entfernt, der eine Probleminstanz schneller als ein heutiger Laptop lösen kann. Ist die Beschäftigung mit der Quantenkomplexitätstheorie und Quantenalgorithmien angesichts dieser Hürden also sinnvoll? In theoretischem Sinne: auf jeden Fall! Wenn man sich damit auseinandersetzt, welche Probleme durch ein physikalisches Objekt effizient zu berechnen sind, sollte man nicht auf die Physik des 19. Jahrhunderts zurückgreifen. Und ist es praktisch sinnvoll? Abgesehen davon, dass sich diese Frage in der Wissenschaft beinahe verbietet, könnten die Ergebnisse z. B. für die Kryptographie von praktischem Nutzen sein. Moore, Russell und Vazirani weisen in [MRV] auf einen Kandidaten für eine Einwegfunktion hin, deren Umkehrfunktion schwerer als das Graphisomorphieproblem zu berechnen ist. Gelänge es nun noch eine Falltür in die Funktion einzubauen, könnte man ein Kryptographieverfahren entwickeln, welches selbst Quantencomputern widerstehen könnte. Die hier vorgestellten Ergebnisse könnten also zu einem sehr viel sichereren asymmetrischen Kryptographieverfahren führen.

## Literatur

- [ADH] L. Adleman, J. DeMarras und M. Huang. *Quantum Computability*. SIAM Journal on Computing, Vol. 26(5), S. 1524-1540, 1997.
- [AK] A. Kitaev. *Quantum Measurements and the Abelian Stabiliser Problem*. Vorabdruck <http://xxx.lanl.gov/abs/quant-ph/9511026>, 1995.
- [AS] A. Shamir. *IP = PSPACE*. Journal of the ACM Vol. 39(4) S. 869-877, 1992.
- [BV] E. Bernstein und U. Vazirani. *Quantum complexity theory*. SIAM Journal on Computing, Vol. 26, No. 5, S. 1411-1473, 1997.
- [CB] C. Bennett. *Logical reversibility of computation*. IBM J. Res. Develop., 17, S. 525-532, 1973.
- [CCG] R. Chang, B. Chor, O. Goldreich et al. *The Random Oracle Hypothesis is False*. Journal of Computer and System Sciences, Vol. 49(1) S. 24-39, 1994.
- [CL] C. Lomont. *The Hidden Subgroup Problem - Review and Open Problems*. Vorabdruck: arXiv:quant-ph/0411037 v1, 2004.
- [CM] C. Moore et al. *The Hidden Subgroup Problem in Affine Groups: Basis Selection in Fourier Sampling*. Vorabdruck arXiv:quant-ph/0211124v3, 2003.
- [DD] D. Deutsch. *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*. Proc. of the Royal Society of London, vol.400, S. 97-117, 1985.
- [DS] D. Simon. *On the Power of Quantum Computation*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, S. 116-123, 1994.
- [EH] M. Ettinger und P. Høyer. *On Quantum Algorithms for Noncommutative Hidden Subgroups*. Vorabdruck arXiv:quant-ph/9807029v1, 1998.
- [EJ] A. Ekert und R. Jozsa. *Quantum computation and Shor's factoring algorithm*. Rev. Mod. Phys. 68, S. 733, 1996.
- [FH] W. Fulton und J. Harris. *Representation Theory. A First Course*. Graduate Texts in Mathematics, 129, Springer-Verlag, 1991.
- [FR] L. Fortnow und J. Rogers. *Complexity limitations on quantum computation*. Journal of Computer and System Sciences, Vol. 59(2), S. 240-252, 1999.
- [HRS] S. Hallgren, M. Rötteler und P. Sen. *Limitations of Quantum Coset States for Graph Isomorphism*. Vorabdruck arXiv.org:quant-ph/0511148, 2005.
- [HRT] S. Hallgren, A. Russell und A. Ta-Shma. *Normal Subgroup Reconstruction and Quantum Computation Using Group Representation*. Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, S. 627-635, Portland, Oregon, 2000.

- [IG] Y. Inui und F. Le Gall. *An Efficient Algorithm for the Hidden Subgroup Problem over a Class of Semi-direct Product Groups*. Vorabdruck arXiv:quant-ph/0412033v2, 2005.
- [JPS] J.-P. Serre. *Linear Representation of Finite Groups*. Springer-Verlag, 1977.
- [KST] J. Köbler, U. Schöning und J. Torán. *The Graph Isomorphism Problem: Its Structural Complexity*. Birkhauser, 1993.
- [LG] L. Grover. *A fast quantum mechanical algorithm for database search*. Proceedings of the 28th ACM Symposium on Theory of Computing, S. 212-219, 1996.
- [GSV] M. Grigni, L. Schulman und U. Vazirani. *Quantum mechanical algorithms for the nonabelian hidden subgroup problem*. ACM Symposium on Theory of Computing, S. 68-74, 2001.
- [MO] M. Ozawa. *Quantum Nondemolition Monitoring of Universal Quantum Computers*. Physical Review Letters Vol. 80, S. 631, 1998.
- [MRV] C. Moore, A. Russell und U. Vazirani. *A classical one-way function to confound quantum adversaries*. Vorabdruck arXiv:quant-ph/0701115, 2007.
- [NO] H. Nishimura und M. Ozawa. *Perfect Computational Equivalence between Quantum Turing Machines and Finitely Generated Uniform Quantum Circuit Families*. Vorabdruck arXiv.org:quant-ph/0511117, 2005.
- [MRS] C. Moore, A. Russell und L. Schulman. *The Symmetric Group Defies Strong Fourier Sampling: Part I*. Vorabdruck arXiv.org:quant-ph/0501056, 2005.
- [PS] P. Shor. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing, Vol. 26, No. 5, 1484-1509, 1997.
- [RF] R. Feynman. *Simulating Physics with Computers*. International Journal of Theoretical Physics, Vol. 21, nos. 6/7, S. 467-488, 1982.
- [WF] W. Fulton. *Young Tableaux, with Applications to Representation Theory and Geometry*. Cambridge University Press, 1997.

**Selbständigkeitserklärung :**

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig und nur unter der Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Berlin, den

**Einverständniserklärung :**

Ich erkläre hiermit mein Einverständnis, dass die vorliegende Arbeit in der Bibliothek des Institutes für Informatik der Humboldt-Universität zu Berlin ausgestellt werden darf.

Berlin, den