Algorithmenentwurf für symmetrische Messungen auf Quantenrechnern

Zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften

der Fakultät für Informatik
der Universität Fridericiana zu Karlsruhe (TH)

genehmigte

Dissertation

von

Thomas Decker

aus Bruchsal

Tag der mündlichen Prüfung:	17. Juli 2006
Erster Gutachter:	Prof. Dr. Roland Vollmar
Zweiter Gutachter:	Prof. Dr. Gernot Alber

Dank

An erster Stelle möchte ich mich bei Herrn Professor Dr. Thomas Beth bedanken, ohne dessen Unterstützung die vorliegende Arbeit nicht möglich gewesen wäre. Er hat mein Interesse für die Quanteninformatik geweckt, und darüber hinaus verdanke ich ihm auch die algebraische Sicht auf dieses Gebiet. Leider hat er die Fertigstellung der Arbeit nicht mehr erlebt. Herrn Professor Dr. Roland Vollmar danke ich herzlich für die Fortsetzung der Betreuung der Arbeit. Herrn Professor Dr. Gernot Alber danke ich für die Übernahme des Korreferats. Meinen Kollegen am Institut für Algorithmen und Kognitive Systeme danke ich für die offene und freundschaftliche Arbeitsatmosphäre, die gute Zusammenarbeit sowie der Hilfsbereitschaft bei Fragen aller Art. Insbesondere möchte ich Herrn Dr. Dominik Janzing für eine Vielzahl von interessanten und fruchtbaren Diskussionen danken, die wesentlich zum Gelingen der Arbeit beigetragen haben.

Inhaltsverzeichnis

Einleitung

In der Quanteninformatik wird untersucht, wie Information mit Quantensystemen gespeichert, übertragen und algorithmisch verarbeitet werden kann. Dabei unterscheidet sich das Auslesen der Information bei Quantensystemen grundsätzlich von dem bei klassischen Systemen: Jede Messung eines klassischen Systems kann theoretisch so durchgeführt werden, daß sämtliche im System vorhandene Information erhalten bleibt und somit eine weitere Messung durchgeführt werden kann, falls vorhergehende Messungen nicht die gewünschte Information ergeben haben. Es existiert daher im Prinzip eine maximale Messung, die gleichzeitig alle Größen eines Systems *präzise* bestimmt. Dies ist bei Quantensystemen nicht der Fall, denn es gibt physikalische Größen wie beispielsweise der Ort und der Impuls eines Teilchens, deren gemeinsame, genaue Bestimmung nach der Heisenbergschen Unschärferelation nicht möglich ist. Dies zeigt, daß die Information, die über ein Quantensystem erhalten werden kann, von den durchgeführten Messungen abhängt, womit unmittelbar die Fragen folgen, welche Messungen für eine gegebene Aufgabe optimal sind und wie diese durchgeführt werden können.

Die bedeutendste Problemstellung bei der Optimierung von Messungen ist die Zustandsunterscheidung; diese spielt nicht nur bei der Übertragung und Speicherung von Information eine zentrale Rolle, sondern auch bei Quantenalgorithmen, denn das Resultat eines solchen Algorithmus ergibt sich durch die Messung eines Zustands, der die Lösung eines Problems beschreibt. In vielen Fällen ist hierbei die Aufgabe, Zustände einer Menge zu unterscheiden, die unter der Operation einer Symmetriegruppe invariant ist. In der vorliegenden Arbeit wird deshalb untersucht, wie diese Symmetrie genutzt werden kann, um die Suche nach optimalen Messungen zu vereinfachen. Bei einigen Optimalitätskriterien folgt hierbei, daß es optimale Messungen gibt, welche dieselbe Symmetrie wie die zu unterscheidenden Zustände aufweisen. Damit kann die Optimierung durch die Beschränkung auf solche Messungen in zahlreichen Fällen sehr stark vereinfacht werden.

Die Tatsache, daß die optimale Unterscheidung von symmetrischen Zustandsmengen mit symmetrischen Messungen möglich ist, hat nicht nur für die *Bestimmung* der optimalen Messungen eine große Bedeutung, sondern auch für die daran anschließende Frage, wie diese *effizient* durchgeführt werden können. Hierbei wird für die Durchführung angenommen, daß ein Quantenrechner zur Verfügung steht; dieser bietet neben bestimmten Grundoperationen auf den Zuständen auch von-Neumann-Messungen, denn diese stellen eine Klasse gut untersuchter Messungen dar, für die zum Teil auch physikalische Realisierungen bekannt sind. Eine beliebige Messung kann unter diesen Voraussetzungen implementiert werden, indem der zu messende Zustand durch geeignete Operationen an eine von-Neumann-Messung angepaßt wird. Diese Reduktion auf von-Neumann-Messungen ist zwar prinzipiell immer möglich, jedoch kann der Aufwand schon bei Messungen von einfachen Systemen beliebig groß sein. Zur Lösung dieses Problems werden

in der vorliegenden Arbeit darstellungstheoretische Verfahren der algorithmischen Signalverarbeitung herangezogen, mit denen beispielsweise auch effiziente Schaltkreise für Fourier-Transformationen konstruiert werden können. Durch die Erweiterung dieser Verfahren können allgemeine Entwurfsprinzipien abgeleitet werden, die zeigen, daß es für eine symmetrische Messung immer eine Durchführung gibt, welche explizit die Symmetrie nutzt. Gleichzeitig wird neben dieser Existenzaussage auch ein konstruktives Verfahren entwickelt, mit dem anhand einiger Beispiele demonstriert werden kann, daß die Entwurfsprinzipien nicht nur ein theoretisches Resultat darstellen, sondern auch die Konstruktion effizienter Implementierungen für konkrete Messungen ermöglichen.

Einordnung und Hauptbeiträge der Arbeit

In der vorliegenden Arbeit werden bekannte Existenzaussagen für optimale symmetrische Messungen verallgemeinert und symmetriebasierte Konstruktionsprinzipien für Meßverfahren entworfen. Darüber hinaus werden durch die Untersuchungen der Struktur symmetrischer Messungen auch Beiträge für die Grundlagen der Quanteninformatik geleistet. Die Darstellung der Resultate folgt den Arbeiten [DJB04, DJR05, JD06, Dec05].

Der Hauptbeitrag dieser Arbeit im Bereich optimaler Messungen ist **Satz 3.24**, der die Anwendung bekannter Existenzaussagen (Davies-Theoreme, siehe Satz 3.22 und 3.23) auf eine größere Klasse von Problemen zuläßt. Durch diese Verallgemeinerung kann in Abschnitt 3.6.2 bei einem Beispiel numerisch bewiesen werden, daß eine bestimmte Messung optimal ist. Die ursprünglichen Aussagen sind bei diesem Beispiel nicht anwendbar, und die Optimalität der Messung wurde bisher nur vermutet.

In der Literatur waren keine Entwurfsprinzipien für Meßverfahren zu finden, welche auf der Symmetrie einer Messung beruhen; nur einige einfache Beispiele von Messungen wurden untersucht und zum Teil auch experimentell durchgeführt. Hauptresultat der vorliegenden Arbeit ist ein allgemeines Konstruktionsprinzip für symmetriebasierte Meßalgorithmen. Die Ergebnisse sind in **Satz 4.9** und **Satz 5.8** zusammengefaßt und werden dabei so formuliert, das sie unmittelbar auf eine vorgegebene Messung angewandt werden können. Die Nützlichkeit der Entwurfsprinzipien wird in den Abschnitten 4.4 und 5.5 durch die Konstruktion effizienter Durchführungsverfahren für einige Familien von Messungen nachgewiesen.

Gliederung der Arbeit

Das **erste Kapitel** umfaßt die grundlegenden Definitionen und Notationen des Standardmodells der Quantenrechner. Neben den Modellierungen der Zustände und der zeitlichen Zustandsentwicklung beinhaltet das erste Kapitel auch das Quantenschaltkreismodell sowie die Beschreibung verallgemeinerter Messungen.

Im **zweiten Kapitel** werden die Eigenschaften von Darstellungen endlicher Gruppen zusammengefaßt, die für die folgenden Untersuchungen notwendig sind. Es wird gezeigt, wie Darstellungen zu Symmetriebegriffen für Zustände, Messungen und Matrizen führen. Da sich die Matrizen mit Symmetrie als wichtiges Hilfsmittel herausstellen, werden diese mit darstellungstheoretischen Methoden untersucht.

Im **dritten Kapitel** werden für symmetrische Zustände Eigenschaften optimaler Messungen betrachtet, wobei verschiedene Optimalitätskriterien herangezogen werden. Dabei

wird für ein Kriterium die Existenz optimaler Messungen nachgewiesen, die eine bestimmte Symmetrie haben. Diese Existenzaussage wird genutzt, um für zwei Beispiele anhand numerischer Rechnungen die Eigenschaften optimaler Messungen zu analysieren.

Im **vierten Kapitel** wird gezeigt, wie aus der Symmetrie einer Messung ein Entwurfsprinzip für Meßalgorithmen auf Quantenrechnern folgt. Anhand einiger Beispiele wird gezeigt, daß die angegebenen Prinzipien durch Ausnutzung der Symmetrie zu effizienten Meßverfahren führen können.

Im **fünften Kapitel** wird das Entwurfsprinzip des vierten Kapitels auf Verfahren für Messungen erweitert, die eine minimale Störung des Systemzustands bewirken. Mit Beispielen wird auch hier demonstriert, daß durch Nutzung der Symmetrie effiziente Meßverfahren konstruiert werden können.

Im **sechsten Kapitel** werden einige Probleme diskutiert, für die möglicherweise mit den in der vorliegenden Arbeit dargestellten Verfahren neue Lösungsansätze gewonnen werden können.

Kapitel 1

Modellierung von Quantenrechnern

Im ersten Kapitel wird die in der Quanteninformatik vorherrschende Modellierung von Quantenrechnern zusammenfassend dargestellt, da Quantenrechner in den folgenden Untersuchungen als grundlegendes Hilfsmittel für die Durchführung von Messungen dienen. Ein Quantenrechner ist in diesem Modell ein Quantensystem, das durch einen endlichdimensionalen Vektorraum beschrieben werden kann und für das geeignete Grundoperationen zur Verfügung stehen. Neben den Systemzuständen und deren zeitlichen Entwicklung, die durch das Quantenschaltkreismodell veranschaulicht wird, umfaßt dieses Kapitel auch die Modellierung der Messungen.

1.1 Bra-Ket-Notation der Quantenmechanik

Viele Rechnungen mit Vektoren, Matrizen (in der Quanteninformatik auch als Operatoren bezeichnet), Skalarprodukten und orthogonalen Projektionen können durch die Bra-Ket-Notation der Quantenmechanik vereinfacht werden. Diese Notation (siehe z. B. Abschnitt 1.1.1 in [Aud05]) basiert auf der Auftrennung des Standard-Skalarprodukts

$$\langle\Phi|\Psi\rangle := \left(\overline{\Phi}_0, \ldots, \overline{\Phi}_{d-1}\right) \begin{pmatrix} \Psi_0 \\ \vdots \\ \Psi_{d-1} \end{pmatrix} = \sum_{j=0}^{d-1} \overline{\Phi}_j \Psi_j$$

in die beiden Matrizen

$$\langle\Phi| := \left(\overline{\Phi}_0, \ldots, \overline{\Phi}_{d-1}\right) \quad \text{und} \quad |\Psi\rangle := \begin{pmatrix} \Psi_0 \\ \vdots \\ \Psi_{d-1} \end{pmatrix}.$$

Definition 1.1 (Bras und Kets) *Ein Vektor $\Phi \in \mathcal{H}$ eines komplexen Vektorraums $\mathcal{H}$ wird als $|\Phi\rangle$ geschrieben und als Ket bezeichnet; der transponierte und elementweise konjugierte Vektor wird als $\langle\Phi|$ geschrieben und Bra genannt.*

Die Rechenregeln für Matrizen gelten auch für Bras und Kets: Neben den Additionen $|\Phi\rangle + |\Psi\rangle$ und $\langle\Phi| + \langle\Psi|$ sowie der Multiplikation von $\langle\Phi|$ oder $|\Phi\rangle$ mit $\alpha \in \mathbb{C}$ ist auch die Multiplikation von Bras mit Kets möglich. Hierbei wird durch die Bildung des Produkts $\langle\Phi||\Psi\rangle := \langle\Phi|\Psi\rangle$ von $\langle\Phi|$ und $|\Psi\rangle$ das Skalarprodukt erhalten. Durch die Vertauschung

von $\langle\Phi|$ und $|\Psi\rangle$ in diesem Produkt wird eine Matrix $|\Psi\rangle\langle\Phi| \in \mathbb{C}^{d\times d}$ erhalten. Mit solchen Matrizen können beliebige Matrizen aufgebaut werden: Es sei dazu $|\Phi_0\rangle, \ldots, |\Phi_{d-1}\rangle$ eine Orthonormalbasis (ONB) von $\mathbb{C}^d$ und $A \in \mathbb{C}^{d\times d}$ eine Matrix. Dann kann A als

$$A = \sum_{j=0}^{d-1} (A|\Phi_j\rangle)\,\langle\Phi_j| = \sum_{j=0}^{d-1} \left(\sum_{k=0}^{d-1} \alpha_{j,k}|\Phi_k\rangle \right) \langle\Phi_j| = \sum_{j,k=0}^{d-1} \alpha_{j,k}|\Phi_k\rangle\langle\Phi_j| \;\text{ mit }\; \alpha_{j,k} \in \mathbb{C}$$

geschrieben werden. In dieser Darstellung ist A die lineare Kombination von Matrizen $|\Phi_k\rangle\langle\Phi_j|$, die alle den Rang eins haben. Für hermitesche Matrizen kann diese Zerlegung durch die Wahl einer orthonormalen Eigenvektorbasis vereinfacht werden; hierbei werden von den Matrizen $|\Phi_k\rangle\langle\Phi_j|$ nur die Elemente $|\Phi_j\rangle\langle\Phi_j|$ benötigt.

Definition 1.2 (Hermitesche Matrix) *Sei $A \in \mathbb{C}^{m\times n}$ eine Matrix. Dann ist die transponierte und elementweise komplex konjugierte Matrix*

$$A^\dagger := \overline{A}^T$$

die zu A adjungierte Matrix. Eine Matrix $A = A^\dagger$ heißt hermitesch.

Eine hermitesche Matrix A ist insbesondere eine normale Matrix, d. h. es gilt die Gleichung $A^\dagger A = AA^\dagger$. Damit garantiert der Spektralsatz (siehe Satz 1 in §2 und Satz 2 in §4, Kap. VIII in [Lor96]) die Existenz einer orthonormalen Eigenvektorbasis:

Satz 1.3 (Spektralsatz für hermitesche Matrizen) *Es sei $A \in \mathbb{C}^{d\times d}$ eine hermitesche Matrix. Dann kann A geschrieben werden als*

$$A = \sum_{j=0}^{s-1} \lambda_j |\Phi_j\rangle\langle\Phi_j|$$

mit den Eigenwerten $\lambda_j \in \mathbb{R}$ und den Matrizen $|\Phi_j\rangle\langle\Phi_j|$, die zu den Vektoren $|\Phi_j\rangle$ einer ONB von Eigenvektoren gebildet werden. Diese Zerlegung wird als Spektralzerlegung von A bezeichnet.

Gilt in der Spektralzerlegung von A für alle j die Gleichung $\lambda_j = 0$ oder $\lambda_j = 1$, so folgt aufgrund der Orthogonalität der $|\Phi_j\rangle$, daß A und A^2 gleich sind. Damit ist A eine orthogonale Projektion auf den von den Eigenvektoren aufgespannten Raum (siehe Abschnitt 1.1.6 in [Aud05]).

Lemma 1.4 (Orthogonale Projektion) *Die orthogonale Projektion $\Pi \in \mathbb{C}^{d\times d}$ auf den von der ONB $|\Phi_0\rangle, \ldots, |\Phi_{s-1}\rangle \in \mathbb{C}^d$ aufgespannten Unterraum von $\mathbb{C}^d$ ist*

$$\Pi = \sum_{j=0}^{s-1} |\Phi_j\rangle\langle\Phi_j| \in \mathbb{C}^{d\times d}\,.$$

1.2 Systemzustände

Die Modellierung der Zustände von endlich-dimensionalen Quantensystemen beruht auf Dichtematrizen und Zustandsvektoren. Für zweidimensionale Quantensysteme besteht daneben zusätzlich die Möglichkeit, einen Zustand anschaulich in der Bloch-Kugel darzustellen. Werden mehrere solche zweidimensionalen Systeme zusammen betrachtet, so ist es aber nicht immer möglich, deren gemeinsamen Zustand durch die zugehörigen Bloch-Kugeln vollständig zu erfassen, denn es ist eine grundlegende Eigenschaft von Quantensystemen, daß sich der Zustand eines Systems nicht immer allein durch die Zustände der Teilsysteme beschreiben läßt. Dies führt bei der Modellierung zusammengesetzter Quantensysteme zu dem Begriff der Verschränkung.

1.2.1 Einzelsysteme

Die Zustände von Quantensystemen werden durch Dichteoperatoren auf Hilbert-Räumen beschrieben, deren Dimension durch die physikalischen Eigenschaften festgelegt ist. In der Quanteninformatik werden hauptsächlich endlich-dimensionale Systeme untersucht, womit die Zustände durch Dichtematrizen (siehe z. B. Abschnitt 4.1.3 in [Aud05]) beschrieben werden können:

Definition 1.5 (Dichtematrix) *Der Zustand eines d-dimensionalen Quantensystems wird durch eine Dichtematrix $\rho \in \mathbb{C}^{d\times d}$ beschrieben, die eine hermitesche, semipositive Matrix mit Spur $\operatorname{tr}(\rho) = 1$ ist.*

Da eine Dichtematrix ρ hermitesch und damit auch normal ist, kann sie nach Satz 1.3 als $\rho = \sum_j \lambda_j |\Phi_j\rangle\langle\Phi_j|$ geschrieben werden. Aufgrund der Semipositivität und der Spurnormierung $\operatorname{tr}(\rho) = 1$ ist für normierte $|\Phi_j\rangle$ diese Summe eine Konvexkombination, d. h. es gelten $\lambda_j \geq 0$ und $\sum_j \lambda_j = 1$. Dies kann als eine Wahrscheinlichkeitsverteilung $p(j)$ auf den Zuständen $\rho_j := |\Phi_j\rangle\langle\Phi_j|$ gedeutet werden, womit die Dichtematrix den Systemzustand beschreibt, falls die Zustände ρ_j jeweils mit der Wahrscheinlichkeit $p(j)$ auftreten (siehe z. B. Abschnitt 4.1.2 in [Aud05]).

Definition 1.6 (Ensemble) *Ein Ensemble ist eine Familie $\rho_0, \ldots, \rho_{m-1}$ von Zuständen eines Systems mit den zugehörigen Wahrscheinlichkeiten $p(j)$. Ein gemäß $p(j)$ gewählter Zustand wird durch die Dichtematrix $\rho = \sum_{j=0}^{m-1} p(j)\rho_j$ beschrieben und Mischung der ρ_j genannt.*

Eine besondere Art von Ensemble liegt vor, falls es nur einen Zustand umfaßt, der selbst keine Mischung ist (siehe z. B. Abschnitt 4.1.1 in [Aud05]):

Definition 1.7 (Reiner Zustand, Zustandsvektor) *Ein Zustand $\rho \in \mathbb{C}^{d\times d}$ ist rein, falls er als $\rho = |\Phi\rangle\langle\Phi|$ mit einem normierten $|\Phi\rangle \in \mathbb{C}^d$ geschrieben werden kann. Der Vektor $|\Phi\rangle$ wird Zustandsvektor genannt.*

Die Resultate einiger Rechnungen mit Dichtematrizen können auch durch die einfachere Rechnung mit Zustandsvektoren erhalten werden. So kann zum Beispiel die Konjugation $\rho \mapsto U\rho U^\dagger$ eines Zustands ρ mit der unitären Matrix U auch auf den Vektoren $|\Phi_j\rangle$ der Spektralzerlegung $\rho = \sum_{j=0}^{s-1} \lambda_j |\Phi_j\rangle\langle\Phi_j|$ untersucht werden. Hierbei entspricht

die Konjugation der Multiplikation $|\Phi_j\rangle \mapsto U|\Phi_j\rangle$. Das Resultat der Konjugation wird durch die Linearität der Multiplikation erhalten:

$$U\rho U^\dagger = U\left(\sum_{j=0}^{s-1}\lambda_j|\Phi_j\rangle\langle\Phi_j|\right)U^\dagger = \sum_{j=0}^{s-1}\lambda_j\left(U|\Phi_j\rangle\right)\left(U|\Phi_j\rangle\right)^\dagger.$$

Der Zustandsvektor eines reinen Zustands ist nicht eindeutig, denn die Zustandsvektoren $|\Phi\rangle$ und $e^{i\alpha}|\Phi\rangle$ entsprechen für alle $\alpha \in \mathbb{R}$ demselben Zustand $|\Phi\rangle\langle\Phi|$. Der Faktor $e^{i\alpha}$ wird globale Phase genannt, da alle Komponenten von $|\Phi\rangle$ mit ihm multipliziert werden. Diese Phasenfaktoren können in vielen Fällen bei der Beschreibung eines Zustands mit Vektoren vernachlässigt werden, da diese beim Übergang auf Dichtematrizen verloren gehen und daher physikalisch keine Bedeutung haben.

1.2.2 Qubits und die Bloch-Kugel

Die einfachsten nichttrivialen Quantensysteme werden durch zweidimensionale Vektorräume beschrieben. Sie sind die Grundbausteine von Quantenrechnern wie es die Bits für Rechner sind.

Definition 1.8 (Qubit) *Ein Qubit ist ein zweidimensionales Quantensystem. Die Vektoren der Standardbasis werden als* $|0\rangle := (1,0)^T$ *und* $|1\rangle := (0,1)^T$ *bezeichnet.*

Bei d-dimensionalen Systemen werden analog zu den Qubits die Vektoren der Standardbasis als $|j\rangle := (0,\ldots,0,1,0,\ldots,0)^T$ mit der Eins in der Komponente j geschrieben. Die Zustände von Qubits können in der Bloch-Kugel veranschaulicht werden. Grundlage sind hierfür die Pauli-Matrizen (siehe z. B. Abschnitt 3.1 in [Aud05]), die zusammen mit der Einheitsmatrix bezüglich des Spurskalarprodukts eine Orthogonalbasis des $\mathbb{R}$-linearen Raums der hermiteschen Matrizen der Größe 2×2 bilden.

Definition 1.9 (Pauli-Matrizen) *Die Pauli-Matrizen sind die Matrizen*

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \textit{und} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Jeder Zustand $\rho \in \mathbb{C}^{2\times 2}$ eines Qubits kann aufgrund der Normierung $\mathrm{tr}(\rho) = 1$ bezüglich der Basis $\{I_2, \sigma_x, \sigma_y, \sigma_z\}$ als

$$\rho = \frac{1}{2}(I_2 + x\sigma_x + y\sigma_y + z\sigma_z)$$

mit $(x,y,z)^T \in \mathbb{R}^3$ geschrieben werden (siehe Abschnitt 3.1 in [Aud05]). Der Vektor $(x,y,z)^T$ wird Bloch-Vektor genannt und legt den Zustand eindeutig fest. Die Bloch-Vektoren können mit den Punkten der Einheitskugel $x^2+y^2+z^2 \leq 1$ im $\mathbb{R}^3$ identifiziert werden, die unter dieser Zuordnung Bloch-Kugel genannt wird.

Definition 1.10 (Bloch-Vektor) *Einem Zustand* $\rho \in \mathbb{C}^{2\times 2}$ *wird der Bloch-Vektor*

$$\begin{pmatrix} \mathrm{tr}(\rho\sigma_x) \\ \mathrm{tr}(\rho\sigma_y) \\ \mathrm{tr}(\rho\sigma_z) \end{pmatrix} \in \mathbb{R}^3$$

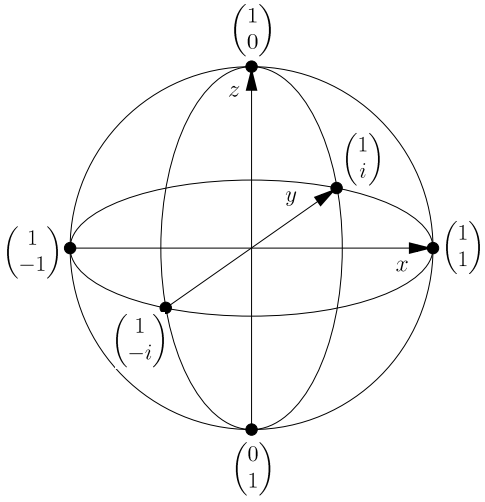

Abbildung 1.1: Die Bloch-Kugel mit den Zuständen aus Bsp. 1.11. Die zugehörigen Zustandsvektoren sind zur Vereinfachung der Notation ohne Normierung angegeben. (Abbildung aus [DJB04] entnommen.)

zugeordnet. Umgekehrt entspricht der Bloch-Vektor $(x, y, z)^T \in \mathbb{R}^3$ *mit* $x^2 + y^2 + z^2 \leq 1$ *dem Zustand*

$$\frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \in \mathbb{C}^{2\times 2}.$$

Orthogonale Zustände werden in der Bloch-Kugel auf Punkte abgebildet, die um den Mittelpunkt gespiegelt sind (siehe Abschnitt 3.2 in [Aud05]).

Beispiel 1.11 (Bloch-Vektoren) *Die zu den Zustandsvektoren*

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \sqrt{\frac{1}{2}}\begin{pmatrix} 1 \\ \pm 1 \end{pmatrix} \text{ und } \sqrt{\frac{1}{2}}\begin{pmatrix} 1 \\ \pm i \end{pmatrix}$$

gehörenden Bloch-Vektoren sind in Abb. 1.1 dargestellt.

Mit der Darstellung von Zuständen in der Bloch-Kugel lassen sich die reinen Zustände einfach charakterisieren (siehe Abschnitte 3.2 und 4.4 in [Aud05]):

Lemma 1.12 (Reine Zustände in der Bloch-Kugel) *Die reinen Zustände eines Qubits entsprechen genau den Punkten auf der Oberfläche der Bloch-Kugel.*

1.2.3 Zusammengesetzte Systeme

Es seien unabhängige Quantensysteme mit den zugehörigen Vektorräumen $\mathcal{H}_0, \ldots, \mathcal{H}_{n-1}$ und den Zuständen $\rho_0, \ldots, \rho_{n-1}$ gegeben. Das Gesamtsystem, das aus diesen Systemen besteht, wird durch das Tensorprodukt beschrieben (siehe z. B. Abschnitt 2.2.8 in [NC00]).

Lemma 1.13 (Zusammengesetztes System) *Der Raum des zusammengesetzten Systems ist* $\mathcal{H}_0 \otimes \ldots \otimes \mathcal{H}_{n-1}$. *Der Zustand des Gesamtsystems unmittelbar nach der Zusammensetzung wird durch die Dichtematrix* $\rho_0 \otimes \ldots \otimes \rho_{n-1}$ *beschrieben.*

Die grundlegenden Komponenten eines Rechners sind die Bits, die zu Registern zusammengefaßt werden. Analog werden bei Quantenrechnern die Quantenregister erhalten (siehe Abschnitt 12.1 in [Aud05]):

Definition 1.14 (Quantenregister) *Ein Quantenregister ist ein Quantensystem, das aus mehreren Qubits besteht. Die 2^n Basisvektoren eines Registers mit n Qubits können binär als $|x_0 \dots x_{n-1}\rangle := |x_0\rangle \otimes \dots \otimes |x_{n-1}\rangle$ mit $x_j \in \{0, 1\}$ geschrieben werden.*

Der Zustand des Gesamtsystems, der unmittelbar nach der Zusammensetzung der Teilsysteme vorliegt, kann nach Lemma 1.13 alleine durch die Zustände $\rho_0, \dots, \rho_{n-1}$ der Teilsysteme beschrieben werden. Ist hingegen ein beliebiger Zustand auf dem Gesamtsystem gegeben, so muß dieser nicht ein Zustand sein, der durch das Zusammenfügen der Teilsysteme entsteht (siehe Abschnitt 7.2.1 in [Aud05]):

Definition 1.15 (Verschränkung reiner Zustände bipartiter Systeme) *Ein reiner Zustand $|\Phi\rangle\langle\Phi|$ mit $|\Phi\rangle \in \mathcal{H}_0 \otimes \mathcal{H}_1$ eines Systems, das aus den durch $\mathcal{H}_0$ und $\mathcal{H}_1$ beschriebenen Teilsystemen besteht, ist unverschränkt, falls er als $|\Phi\rangle = |\Phi_0\rangle \otimes |\Phi_1\rangle$ mit $|\Phi_0\rangle \in \mathcal{H}_0$ und $|\Phi_1\rangle \in \mathcal{H}_1$ geschrieben werden kann. Die anderen Zustände sind verschränkt.*

Die Definition von Verschränkung kann auf Systeme, die aus mehr als zwei Teilsystemen bestehen, und gemischte Zustände verallgemeinert werden (siehe z. B. [Bru02] oder Kap. 8 in [Aud05]).

1.3 Zeitliche Entwicklung

Die zeitliche Entwicklung des Zustands eines Quantensystems wird durch die Schrödinger-Gleichung beschrieben. Diese zeitliche Entwicklung gilt nur für abgeschlossene Systeme, also nicht für Systeme, die in Wechselwirkung mit anderen Quantensystemen stehen (siehe z. B. Abschnitt 2.1.2 in [Aud05]).

Definition 1.16 (Schrödinger-Gleichung) *Es sei $|\Phi(t)\rangle$ der Zustandsvektor zur Zeit t. Dann gilt mit dem zeitabhängigen Hamilton-Operator $H(t)$ die Schrödinger-Gleichung*

$$i\hbar \frac{d}{dt} |\Phi(t)\rangle = H(t) |\Phi(t)\rangle \,,$$

wobei $2\pi\hbar$ das Plancksche Wirkungsquantum ist.

Die Schrödinger-Gleichung ist eine lineare Differentialgleichung, die für einen zeitunabhängigen Hamilton-Operator $H(t) = H$ durch Exponentiation gelöst werden kann (siehe z. B. Abschnitt 2.2.2 in [NC00]):

Lemma 1.17 (Zeitentwicklung) *Liegt für ein System mit Hamilton-Operator H zur Zeit $t = 0$ der durch $|\Phi(0)\rangle$ beschriebene Zustand vor, so liegt zum Zeitpunkt t der durch $|\Phi(t)\rangle = U_t |\Phi(0)\rangle$ beschriebene Zustand mit $U_t := e^{-iHt/\hbar}$ vor.*

Aufgrund der Hermitezität des Hamilton-Operators ist U_t eine unitäre Matrix, womit die Zeitentwicklung durch unitäre Transformationen beschrieben wird (siehe z. B. Abschnitt 2.1.2 in [Aud05]). Die Zustände zu aufeinander folgenden Zeitpunkten können

demnach durch eine Folge $U_0, \ldots, U_{m-1}$ unitärer Transformationen erfaßt werden: Zum Zeitpunkt t_j liegt der durch $|\Phi(t_j)\rangle = U_{j-1}|\Phi(t_{j-1})\rangle$ beschriebene Zustand vor. Im Standardmodell der Quanteninformatik wird angenommen, daß der Hamilton-Operator und damit auch die zeitliche Entwicklung eines Systems beeinflußt werden können, beispielsweise durch Anlegen eines äußeren Felds. Damit wird eine bestimmte Menge unitärer Transformationen festgelegt, die unmittelbar durchführbar sind. Eine Grundfrage ist, welche Operationen notwendig sind, um beliebige Transformation zusammensetzen zu können (siehe z. B. Abschnitt 4.5 in [NC00]):

Definition 1.18 (Universelle Operationen) *Eine Menge von unitären Tranformationen ist universell auf $n \geq 1$ Qubits, falls über dieser Menge jede Matrix aus $\mathcal{U}(2^n)$ in ein endliches Produkt faktorisiert werden kann, wobei $\mathcal{U}(d)$ die Menge der unitären $(d \times d)$-Matrizen bezeichnet.*

Ein weiterer Universalitätsbegriff ist die approximative Universalität (siehe z. B. Abschnitt 8.2 in [KSV02]). Eine Menge von Transformationen, die nach Def. 1.18 universell ist, wird durch die Ein-Qubit-Operationen und die CNOT-Operationen gebildet (*controlled not*, siehe Abschnitt 4.5.2 in [NC00]). Die Grundidee ist hierbei, daß die beiden Arten von Operationen auf höchstens zwei Qubits eines Registers angewandt werden, denn bei einigen möglichen Realisierungen von Quantenrechnern, beispielsweise bei Ionenfallen, sind solche Operationen experimentell durchführbar (siehe z. B. Abschnitt 7.6 in [NC00]). Die Operationen auf dem gesamten Register können durch das Tensorprodukt bestimmt werden:

Lemma 1.19 (Operationen auf zusammengesetzten Systemen) *Werden auf den Teilsystemen jeweils die Operationen U_j durchgeführt, so beschreibt $U_0 \otimes \ldots \otimes U_{n-1}$ die Operation auf dem Gesamtsystem.*

Alle Operationen der Form $U_0 \otimes \ldots \otimes U_{n-1}$ können durch die Hintereinanderausführung von Ein-Qubit-Operationen erhalten werden:

Definition 1.20 (Ein-Qubit-Operation) *Eine Ein-Qubit-Operation auf dem Qubit j, $j \in \{0, \ldots, n-1\}$, eines Registers mit n Qubits wird durch*

$$I_2^{\otimes j} \otimes U \otimes I_2^{\otimes k}$$

für k mit $j + k = n - 1$ sowie einer unitären Matrix $U \in \mathcal{U}(2)$ beschrieben. Hierbei bezeichnet $I_2^{\otimes \ell}$ das Tensorprodukt $I_2 \otimes \ldots \otimes I_2$ mit ℓ Komponenten I_2.

Da die Ein-Qubit-Operationen keine Wechselwirkung zwischen den verschiedenen Qubits bewirken, werden beispielsweise noch die CNOT-Operationen benötigt, um eine universelle Menge zu erhalten:

Definition 1.21 (CNOT-Operation) *Die für $j \neq k$ durch*

$$|x_0\rangle \otimes \ldots \otimes |x_{n-1}\rangle \;\mapsto\; |x_0\rangle \otimes \ldots \otimes |x_{j-1}\rangle \otimes |x_j \oplus x_k\rangle \otimes |x_{j+1}\rangle \otimes \ldots \otimes |x_{n-1}\rangle$$

festgelegte Operation, wobei $\oplus$ die binäre XOR-Verknüpfung bezeichnet, ist die von Qubit k gesteuerte CNOT-Operation auf dem Qubit j.

Die Abbildung eines beliebigen Zustands durch eine CNOT-Operation wird durch die lineare Fortsetzung der Abbildung aus Def. 1.21 erhalten. Die CNOT-Operation führt auf dem j-ten Qubit die unitäre Transformation σ_x genau dann durch, falls sich das steuernde k-te Qubit im Zustand $|1\rangle\langle 1|$ befindet.

Die Universalität der Ein-Qubit- und CNOT-Operationen kann konstruktiv gezeigt werden. Dabei wird auch eine Schranke für die Anzahl benötigter Ein-Qubit- und CNOT-Operationen erhalten (siehe [VMS04] und auch [BBC$^+$95, Cyb01]).

Lemma 1.22 (Zerlegung unitärer Matrizen) *Es sei $U \in \mathcal{U}(2^n)$ eine unitäre Transformation auf n Qubits. Dann kann U in ein Produkt von $O(4^n)$ Ein-Qubit-und CNOT-Operationen zerlegt werden.*

Die Zerlegungsverfahren für beliebige unitäre Transformationen sind aufgrund der in der Registergröße exponentiellen Anzahl von Ein-Qubit-und CNOT-Operationen nur für Quantenregister mit sehr wenigen Qubits brauchbar. Werden spezielle Operationen betrachtet, so können durch andere Verfahren einfachere Zerlegungen gefunden werden. Von besonderem Interesse sind hierbei die Operationen, die mit einer polynomial beschränkten Anzahl von Ein-Qubit- und CNOT-Operationen durchgeführt werden können (siehe z. B. Def. 1.8 und 1.11 in [Röt01]).

Definition 1.23 (Effizient durchführbare Transformationen) *Eine Familie von unitären Transformationen U_{2^n}, wobei U_{2^n} auf einem Register mit n Qubits operiert, ist effizient durchführbar, falls U_{2^n} in ein Produkt von $m(n)$ Ein-Qubit- und CNOT-Operationen zerlegt werden kann, wobei $m(n)$ polynomial in n beschränkt ist. Die Zerlegung von U_{2^n} muß hierbei uniform sein, d. h. die Zerlegung kann mit polynomialem Aufwand gefunden werden.*

Ein Beispiel für eine effizient durchführbare Familie ist durch die diskreten Fourier-Transformationen (DFT, siehe z. B. Abschnitt I.2 in [Bet84]) gegeben.

Definition 1.24 (DFT) *Die DFT der Größe n ist durch*

$$F_n := \sqrt{\frac{1}{n}} \left(\omega_n^{jk}\right)_{j,k=0}^{n-1} \in \mathbb{C}^{n\times n}$$

festgelegt. Hierbei bezeichnet $\omega_n := e^{2\pi i/n}$ eine n-te Einheitswurzel.

Es sind Verfahren bekannt, welche die DFT F_{2^k} in $O(k^2)$ Ein-Qubit- und CNOT-Operationen zerlegen (siehe z. B. Satz 3.1 in [Röt01] oder Abschnitt 5.1 in [NC00]). Damit sind die DFTs F_{2^k} auf Quantenrechnern effizient durchführbar.

1.4 Quantenschaltkreise

Mit Schaltkreisen kann die Berechnung Boolescher Funktionen durch die Verknüpfung von UND-, ODER- und NICHT-Gattern erreicht werden. An diese Schaltkreise lehnt sich das Quantenschaltkreismodell an, das eine für Quantenregister geeignete Notation unitärer Transformationen darstellt. Die unitären Transformationen, die auf dem Register des Quantenrechners operieren, werden hierbei als Gatter bezeichnet.

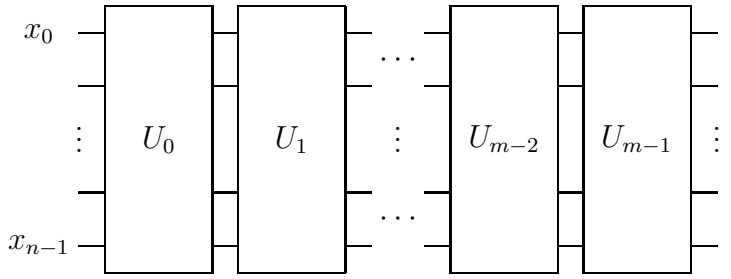

Abbildung 1.2: Quantenschaltkreis auf n Qubits mit den Gattern $U_0, \ldots, U_{m-1}$.

Definition 1.25 (Schaltkreis) *Ein Quantenschaltkreis, welcher der Durchführung der unitären Transformation $U_{m-1}U_{m-2}\ldots U_1U_0$ auf einem Register von n Qubits entspricht, besteht aus den von links nach rechts angeordneten Gattern $U_0, \ldots, U_{m-1}$. Hierbei werden benachbarte Gatter durch n übereinander liegende Leitungen verbunden.*

In Abb. 1.2 ist ein Quantenschaltkreis für n Qubits und m unitäre Transformationen U_j skizziert. Es werden zusätzlich zu den Verbindungen zwischen den Gattern noch jeweils n Leitungen an die Gatter U_0 und U_{n-1} als Ein- bzw. Ausgänge angebracht. Ferner wird festgelegt, daß die oberste Leitung der ersten Tensorkomponente von $|x_0 \ldots x_{m-1}\rangle$ entspricht, d. h. die oberste Leitung entspricht dem zu $|x_0\rangle$ gehörenden Qubit. Das Quantenschaltkreismodell beschreibt unitäre Transformationen besonders anschaulich, falls für spezielle Transformationen eigene Gattersymbole verwendet werden (siehe z. B. Abschnitte 4.2 und 4.3 in [NC00]).

Definition 1.26 (Quantengatter) *Ein Gatter, das der Transformation $A_0 \otimes \ldots \otimes A_{p-1}$ auf n Qubits mit den $(2^{n_j} \times 2^{n_j})$-Matrizen A_j für $n_0 + \ldots + n_{p-1} = n$ entspricht, wird wie in Abb. 1.3a) dargestellt. Das Gatter I_{2^k} entspricht k durchgezogenen Leitungen.*

Ein Gatter, das durch die Permutation $|x_0 \ldots x_{n-1}\rangle \mapsto |x_{\pi(0)} \ldots x_{\pi(n-1)}\rangle$ von n Qubits festgelegt ist, wird wie in Abb. 1.3b) dargestellt. Hierbei wird die $\pi(j)$-te Leitung auf der linken Seite mit der j-ten Leitung auf der rechten Seite verbunden.

Unitäre Transformationen $A_0, \ldots, A_{p-1} \in \mathcal{U}(2)$, die auf den Qubits $j_0, \ldots, j_{p-1}$ genau für die durch $|x_{k_0}\rangle = \ldots = |x_{k_{q-1}}\rangle = |1\rangle$ beschriebenen Basiszustände durchgeführt werden, sind in Abb. 1.3c) dargestellt. Hierbei sind alle k_ℓ und j_ℓ verschieden.

Die Symbole für die Ein-Qubit- und CNOT-Operationen aus Def. 1.20 und 1.21 sind in Abb. 1.3d) und 1.3e) dargestellt. Die Gatter aus Abb. 1.3b) und 1.3c) können effizient durchgeführt werden (siehe Satz 1.20 in [Röt01] und Kor. 7.6 in [BBC$^+$95]).

1.5 Messungen

Neben der unitären Zeitentwicklung von Quantensystemen, welche durch die Schrödinger-Gleichung festgelegt ist, existiert eine weitere Art von Zeitentwicklung, die durch Meßgeräte verursacht wird und sich grundsätzlich von der unitären Zeitentwicklung unterscheidet. Die Meßgeräte werden dabei durch die Wahrscheinlichkeiten der möglichen Meßresultate und die bei der Messung auftretenden Zustandsänderung modelliert.

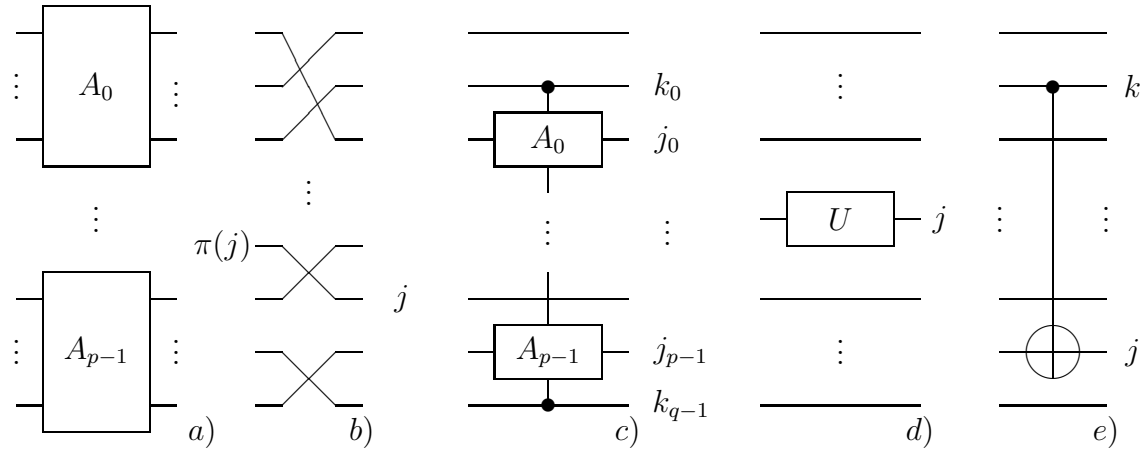

Abbildung 1.3: Symbole für die Transformationen aus Def. 1.26. Das Gatter A_j in a) hat jeweils n_j Ein- und Ausgänge. Die Symbole $\bullet$ geben die Qubits an, welche die Gatter steuern, falls die unitären Operationen wie in Def. 1.21 in der Standardbasis dargestellt werden. Das Gatter $\oplus$ entspricht σ_x.

1.5.1 Wahrscheinlichkeiten und Zustandsänderung

Werden Messungen mit einer endlichen Anzahl möglicher Resultate betrachtet, so können die Resultate durchnumeriert und mit ihrem Index identifiziert werden, d. h. die Resultate der Messung sind die Indizes. Jedem Resultat werden Operatoren zugeordnet, die das Verhalten des Meßgeräts beschreiben (siehe z. B. Abschnitt 4.2 in [Bar98]).

Definition 1.27 (Messungen und Kraus-Operatoren) *Jedem möglichen Resultat $j \in \{0, \ldots, n-1\}$ einer Messung eines d-dimensionalen Systems wird eine Operatoren-Familie $A_{j,k} \in \mathbb{C}^{d\times d}$ mit $k \in \{0, \ldots, n_j - 1\}$ zugeordnet. Dabei müssen sich die n semi-positiven Operatoren*

$$\Pi_j := \sum_{k=0}^{n_j-1} A_{j,k}^\dagger A_{j,k}$$

zu I_d aufsummieren. Die Operatoren $A_{j,k}$ werden Kraus-Operatoren genannt.

Die einem Meßresultat zugeordneten Operatoren legen die Wahrscheinlichkeiten des Resultats und den Zustand nach der Messung fest:

Definition 1.28 (Resultat einer Messung) *Bei der Messung eines Systems im Zustand ρ tritt das Resultat j mit der Wahrscheinlichkeit $\mathrm{tr}(\rho\Pi_j)$ auf. Der Zustand nach der Messung ist*

$$\frac{1}{\mathrm{tr}(\rho\Pi_j)} \sum_{k=0}^{n_j-1} A_{j,k}\rho A_{j,k}^\dagger. \tag{1.1}$$

Tritt das Resultat j auf, so ist nach Gl. (1.1) der Zustand nach der Messung eine Mischung von Zuständen, die zu demselben Wert j und zu verschiedenen k gehören. Dies kann als Messung mit den Resultaten (j,k) gedeutet werden, wobei die Komponente k eines Resultats unbekannt ist, weil beispielsweise das Meßgerät zwar intern das Resultat (j,k) ermittelt, aber nur j ausgibt (siehe Abschnitt II in [Bar00]).

1.5.2 POVMs

Ist der Zustand nach einer Messung nicht von Bedeutung, beispielsweise wenn die Messung am Ende eines Experiments durchgeführt wird, und werden daher nur die Wahrscheinlichkeiten der Resultate betrachtet, so kann zur Vereinfachung die Sicht auf die Operatoren Π_j einer Messung beschränkt werden (siehe z. B. Abschnitt 13.4 in [Aud05]):

Definition 1.29 (POVM) *Ein positiv-operatorwertiges Maß (POVM, positive operator-valued measure) besteht aus einer Familie* $\Pi_0, \ldots, \Pi_{n-1}$ *von semipositiven Operatoren* Π_j *mit* $\sum_{j=0}^{n-1} \Pi_j = I_d$.

Eine Definition für unendlich viele Resultate ist beispielsweise in Def. 1.1, Kap. 3 in [Dav76] zu finden. Auch für endlich-dimensionale Quantensysteme können POVMs unendlich viele mögliche Resultate haben (siehe z. B. [DLPS02]).

Die Kraus-Operatoren einer Messung sind durch die POVM-Operatoren Π_j nicht eindeutig festgelegt. Somit ist der Zustand nach der Messung eines POVMs ohne zusätzliche Annahmen nicht definiert, d. h. es gibt viele mögliche Meßgeräte mit verschiedenen Kraus-Operatoren, die einem bestimmten POVM entsprechen. Ein mögliches dieser Meßgeräte ordnet jedem Resultat j den einzelnen Operator $A_{j,0} := \sqrt{\Pi_j}$ zu, wobei $\sqrt{\Pi_j}$ die eindeutige semipositive Wurzel (siehe Th. 2.2.1 in [Mur90]) von Π_j ist.

Vor einer Messung kann gemäß einer Wahrscheinlichkeitsverteilung zwischen verschiedenen Meßgeräten gewählt werden. Diese Wahl entspricht der Konvexkombination der zugehörigen POVMs, falls die Entscheidung, welches Meßgerät genutzt wurde, abgespeichert wird. Eine besondere Eigenschaft der POVMs ist die Abgeschlossenheit unter dieser Operation, d. h. die Konvexkombination von POVMs ist wieder ein POVM. Diese Abgeschlossenheit kann beispielsweise bei der Optimierung von Messungen genutzt werden (siehe z. B. Kap. 3).

Definition 1.30 (Konvexkombination von POVMs) *Es seien* P *und* $\tilde{P}$ *zwei POVMs eines Systems mit den Operatoren* $\Pi_0, \ldots, \Pi_{m-1}$ *sowie* $\tilde{\Pi}_0, \ldots, \tilde{\Pi}_{n-1}$. *Dann bilden für* $\lambda \in [0, 1]$ *die Operatoren*

$$\lambda\Pi_0, \ \ldots, \ \lambda\Pi_{m-1}, \ (1-\lambda)\tilde{\Pi}_0, \ \ldots, \ (1-\lambda)\tilde{\Pi}_{n-1}$$

ein POVM, das als Konvexkombination $\lambda P + (1-\lambda)\tilde{P}$ *von* P *und* $\tilde{P}$ *definiert wird.*

Wie bei reinen Zuständen $\rho = |\Phi\rangle\langle\Phi|$, die durch Zustandsvektoren $|\Phi\rangle$ repräsentiert werden, kann bei POVMs mit Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ vom Rang eins jeder Operator durch einen Vektor $|\Psi_j\rangle$ beschrieben werden, der im Gegensatz zu einem Zustandsvektor nicht normiert sein muß. Die Wahrscheinlichkeit des Resultats j bei Vorliegen des Zustands $\rho = |\Phi\rangle\langle\Phi|$ kann dabei durch $\mathrm{tr}(\rho\Pi_j) = |\langle\Psi_j|\Phi\rangle|^2$ berechnet werden.

1.5.3 Orthogonale Messungen

Eine wichtige Teilmenge von POVMs bilden die orthogonalen Messungen. Diese werden auch als projektive Messungen oder von-Neumann-Messungen bezeichnet (siehe z. B. Abschnitt 2.2.6 in [NC00]).

Definition 1.31 (Orthogonale Messung) *Eine orthogonale Messung ist ein POVM, dessen Operatoren* $\Pi_j^2 = \Pi_j$ *und* $\Pi_j\Pi_k = 0$ *für* $j \neq k$ *erfüllen.*

Die Zustandsentwicklung bei einer orthogonalen Messung mit Resultat j wird durch die Projektionsformel

$$\rho \mapsto \frac{1}{\mathrm{tr}(\rho\Pi_j)}\Pi_j\rho\Pi_j$$

festgelegt (siehe z. B. Abschnitte 4.1.2 in [Aud05]). Hierbei wird also dem Resultat j der Operator $A_{j,0} = \sqrt{\Pi_j} = \Pi_j$ zugeordnet.

Eine orthogonale Messung kann nicht nur durch die Menge der orthogonalen Projektoren, sondern auch mit einer Observablen beschrieben werden (siehe Abschnitt 2.1.2 in [Aud05]). Hierbei werden die Π_j aus Def. 1.31 als Projektoren der Spektralzerlegung nach Satz 1.3 eines hermiteschen Operators erhalten, der Observable genannt wird; die möglichen Resultate der Messung sind die Eigenwerte dieses Operators.

Die Operatoren Π_j einer orthogonalen Messung sind Projektoren auf zueinander orthogonale Teilräume. Daher entspricht jeder Operator nach Lemma 1.4 einer bestimmten Menge von Vektoren einer ONB des gesamten Raums. Projiziert jeder Operator auf einen eindimensionalen Raum, so kann die Messung allein durch die zugehörige ONB beschrieben werden:

Definition 1.32 (Messung in einer ONB) *Die Messung in einer ONB mit den Vektoren $|\Psi_j\rangle$ umfaßt die Operatoren $\Pi_j := |\Psi_j\rangle\langle\Psi_j|$.*

Ein Spezialfall einer Messung in einer ONB ist die Messung in der Standardbasis $\{|0\rangle, \ldots |d-1\rangle\}$. Jede Messung bezüglich einer ONB kann durch die entsprechende Basiswechselmatrix auf die Messung in der Standardbasis zurückgeführt werden. In der Quanteninformatik wird in vielen Fällen angenommen, daß Messungen nur in der Standardbasis durchgeführt werden können.

Kapitel 2

Matrizen, Ensembles und POVMs mit Symmetrie

Hauptgegenstand der vorliegenden Arbeit sind *symmetrische* Ensembles und POVMs; im allgemeinen wird ein Objekt als symmetrisch bezeichnet, falls es unter der Operation einer Symmetriegruppe invariant ist. Da bei Ensembles und POVMs Darstellungen endlicher Gruppen diese Operationen vermitteln, werden in diesem Kapitel zunächst einige grundlegenden Definitionen und Hilfssätze der Darstellungstheorie bereitgestellt. Neben der Symmetrie von Ensembles und POVMs wird auch ein Symmetriebegriff für Matrizen definiert, denn es stellt sich bei den folgenden Untersuchungen heraus, daß sich mit diesem viele Problemstellungen sehr kompakt formulieren lassen. Der Symmetriebegriff für Matrizen führt darüber hinaus auch zu dem in Kap. 3 und 4 diskutierten Kernproblem, bei dem Matrizen konstruiert werden müssen, die eine bestimmte Symmetrie haben. Ist diese Konstruktion möglich, so können symmetriebasierte Zerlegungsverfahren genutzt werden, um diese Matrizen in Produkte einfacher Matrizen zu zerlegen. Diese Zerlegungen können als Ausgangspunkt für effiziente Durchführungen von Messungen dienen. In diesem Kapitel wird mit Hilfe des Schurschen Lemmas gezeigt, daß diese Konstruktion immer möglich ist und daher die symmetriebasierten Zerlegungsmethoden bei beliebigen Messungen als Hilfsmittel zur Verfügung stehen.

2.1 Darstellungen endlicher Gruppen

Eine Matrixdarstellung, im folgenden zur Vereinfachung auch Darstellung genannt, ordnet jedem Element einer Gruppe eine Matrix zu (siehe z. B. Abschnitt 1.1 in [Ser77]). Die wichtigste Eigenschaft ist hierbei, daß diese Zuordnung die Gruppenstruktur erhält.

Definition 2.1 (Darstellung, Grad) *Es sei G eine endliche Gruppe. Eine Darstellung von G ist ein Gruppen-Homomorphismus $\sigma : G \to \mathrm{GL}(\mathbb{C}, d)$, wobei $\mathrm{GL}(\mathbb{C}, d)$ die Gruppe der invertierbaren Matrizen in $\mathbb{C}^{d\times d}$ bezeichnet. Der Grad $\deg(\sigma)$ von σ ist d.*

Werden Zustandsvektoren oder die Vektoren $|\Psi\rangle$ von POVM-Operatoren $|\Psi\rangle\langle\Psi|$ vom Rang eins betrachtet, so soll bei der Multiplikation mit den Matrizen $\sigma(g)$ die Länge der Vektoren erhalten bleiben. Deshalb werden in der Quanteninformatik hauptsächlich unitäre Darstellungen untersucht (siehe z. B. Abschnitt 1.11.1 in [FS92]).

Definition 2.2 (Unitäre Darstellung) *Eine Darstellung σ der Gruppe G ist unitär, falls alle $\sigma(g)$, $g \in G$, unitäre Matrizen sind.*

Die wichtigsten Darstellungen einer Gruppe sind die irreduziblen Darstellungen (siehe z. B. Abschnitt 1.4 in [Ser77]):

Definition 2.3 (Irreduzible Darstellung) *Eine Darstellung $\sigma : G \to \mathcal{U}(d)$ ist irreduzibel, falls für jeden Vektorraum $\mathcal{H} \leq \mathbb{C}^d$ mit $\sigma(g)\mathcal{H} \subseteq \mathcal{H}$, $g \in G$, entweder $\mathcal{H} = \{0\}$ oder $\mathcal{H} = \mathbb{C}^d$ gilt.*

Die Bedeutung der irreduziblen Darstellungen folgt aus der Tatsache, daß alle Darstellungen einer Gruppe durch die direkte Summe irreduzibler Darstellungen aufgebaut werden können. Damit wird die Untersuchung aller Darstellungen einer Gruppe im wesentlichen auf die Identifizierung der irreduziblen Darstellungen reduziert.

Lemma 2.4 (Zerlegung in irreduzible Darstellungen) *Es sei $\sigma : G \to \mathcal{U}(d)$ eine Darstellung. Dann existiert eine Matrix $U \in \mathcal{U}(d)$ mit*

$$U\sigma U^\dagger = \kappa_0 \oplus \ldots \oplus \kappa_{n-1}\,, \tag{2.1}$$

wobei die κ_j irreduzibel und unitär sind.

Beweis: Gemäß dem Beweis von Prop. 2, Kap. 15 in [Ter99] sei W ein invarianter Unterraum von σ und $W^\perp$ das dazu orthogonale Komplement. Dieses ist auch unter σ invariant. Wird für W und $W^\perp$ jeweils eine orthonormale Basis gewählt, ist die Basiswechselmatrix, welche σ in die Komponenten bezüglich beider Räume zerlegt, unitär. Durch rekursives Vorgehen wird eine Zerlegung in die irreduziblen κ_j erhalten. Die Darstellungen κ_j sind unitär, da das Produkt unitärer Matrizen unitär ist. □

Neben den irreduziblen Darstellungen ist auch die reguläre Darstellung einer Gruppe (siehe z. B. §9, Kap. 2 in [CR62]) von Bedeutung.

Definition 2.5 (Reguläre Darstellung) *Es sei G eine Gruppe mit der festgelegten Reihenfolge $g_0, \ldots, g_{n-1}$ der Elemente. Jedes Element $h \in G$ permutiert durch Linksmultiplikation die Elemente von G, d. h. es existiert $\pi(h) \in S_n$ mit $hg_j = g_{\pi(h)(j)}$ und $\pi(g)\pi(h) = \pi(gh)$. Dann ist die Darstellung $\sigma_{\text{reg}} : G \to \mathcal{U}(n)$ mit*

$$\sigma_{\text{reg}}(g) := \sum_{j=0}^{n-1} |\pi(g)(j)\rangle\langle j|$$

die reguläre Darstellung von G.

Eine Änderung der Reihenfolge der Elemente von G entspricht einer Konjugation der Matrizen $\sigma_{\text{reg}}(g)$ mit einer Permutationsmatrix, welche die Basis des Vektorraums, auf dem σ_{reg} operiert, passend umordnet. Deshalb führt die Umordnung der Gruppenelemente nicht zu einer wesentlichen Änderung der regulären Darstellung. Allgemein können Darstellungen, die bis auf einen Basiswechsel gleich sind, miteinander identifiziert werden (siehe z. B. Abschnitt 1.1 in [Ser77]). Bei unitären Darstellungen kann die Äquivalenz auch mit unitären Basiswechsel definiert werden:

Lemma 2.6 (Äquivalenz von unitären Darstellungen) *Zwei unitäre Darstellungen $\sigma, \tau : G \to \mathcal{U}(d)$ sind genau dann äquivalent, falls es eine Matrix $W \in \mathcal{U}(d)$ gibt, die $\sigma(g) = W\tau(g)W^\dagger$ für alle $g \in G$ erfüllt.*

Beweis: Es ist nur die Existenz von W zu zeigen. Nach Prop. 1, Kap. 15 in [Ter99] und Lemma 2.4 existieren $U, V \in \mathcal{U}(d)$ mit $U\sigma U^\dagger = \kappa_0 \oplus \ldots \oplus \kappa_{m-1}$ und $V\tau V^\dagger = \tilde{\kappa}_0 \oplus \ldots \oplus \tilde{\kappa}_{n-1}$, wobei alle κ_j und $\tilde{\kappa}_j$ irreduzibel und unitär sind. Nach Kor. 1, Abschnitt 2.3 in [Ser77] gilt $m = n$ und es kann durch Permutation der κ_j angenommen, daß κ_j zu $\tilde{\kappa}_j$ äquivalent ist. Nach Lemma 33.1 in [Dor71] gibt es unitäre U_j mit $\kappa_j = U_j \tilde{\kappa}_j U_j^\dagger$ für alle j. Damit gilt $\sigma(g) = W\tau(g)W^\dagger$ für die unitäre Matrix $W := U^\dagger(U_0 \oplus \ldots \oplus U_{n-1})V$. □

Eine endliche Gruppe hat nur endlich viele inäquivalente irreduzible Darstellungen (siehe z. B. §2.5 in [Ser77]), wobei die Äquivalenzklassen mit Vertretern identifiziert werden. Es kann hierbei zu jeder Darstellung einer Gruppe eine äquivalente, unitäre Darstellung gefunden werden (siehe z. B. Prop. 1, Kapitel 15 in [Ter99]).

Beispiel 2.7 (Irreduzible Darstellungen) *Die Gruppe $C_3 := \langle r : r^3 = 1 \rangle$ hat genau die drei irreduziblen Darstellungen $\kappa_0, \kappa_1, \kappa_2 : C_3 \to \mathbb{C}^{1\times 1}$, die durch*

$$\kappa_0(r^j) = (1),\ \kappa_1(r^j) = (\omega_3^j) \ \text{ und } \ \kappa_2(r^j) = (\omega_3^{2j})$$

für $j \in \{0, 1, 2\}$ definiert sind, wobei $\omega_3 := e^{2\pi i/3}$ eine dritte Einheitswurzel ist.

Die Zerlegung einer Darstellung nach Lemma 2.4 kann insbesondere auf die reguläre Darstellung einer Gruppe angewandt werden (siehe Def. 2.11 in [Röt01]):

Definition 2.8 (Allgemeine Fourier-Transformation einer Gruppe) *Eine Matrix, welche σ_{reg} für eine Gruppe G wie in Gl. (2.1) zerlegt, wobei äquivalente Komponenten κ_j in der Zerlegung gleich sind, wird allgemeine Fourier-Transformation von G genannt.*

Für zyklische Gruppen fallen die DFT und die allgemeine Fourier-Transformation zusammen (siehe z. B. Abschnitt II.5 in [Bet84]):

Beispiel 2.9 (DFT) *Ist $C_n := \langle r : r^n = 1 \rangle$ eine zyklische Gruppe mit n Elementen, so sind bei der Anordnung $r^0, r^1, \ldots, r^{n-1}$ der Gruppenelemente die allgemeine Fourier-Transformation und die DFT aus Def. 1.24 gleich.*

Die reguläre Darstellung einer Gruppe G wird durch die allgemeine Fourier-Transformation in eine direkte Summe der irreduziblen Darstellungen κ_j von G zerlegt, wobei κ_j in dieser Zerlegung $\deg(\kappa_j)$ mal auftritt (siehe z. B. Kor. 1, Abschnitt 2.4 in [Ser77]). Allgemeiner ist die Anzahl des Auftretens einer irreduziblen Komponente von der Zerlegung einer Darstellung unabhängig (siehe Kor. 1 in §2.3 in [Ser77]); dies führt zu dem Begriff der Multiplizität (*multiplicity*, siehe z. B. Abschnitt 2.3 in [FS92]):

Definition 2.10 (Multiplizität) *Es sei $\sigma : G \to \mathcal{U}(d)$ eine Darstellung der endlichen Gruppe G und $U \in \mathcal{U}(d)$ eine Matrix, welche σ in die direkte Summe*

$$U\sigma U^\dagger = \bigoplus_{j=0}^{z-1} (I_{m_j} \otimes \kappa_j) := (\kappa_0 \oplus \ldots \oplus \kappa_0) \oplus \ldots \oplus (\kappa_{z-1} \oplus \ldots \oplus \kappa_{z-1}) \tag{2.2}$$

der verschiedenen irreduziblen Darstellungen κ_j zerlegt, d. h. κ_j tritt m_j-mal in $U\sigma U^\dagger$ auf. Dann heißt m_j die Multiplizität von κ_j in σ.

2.2 Projektive Darstellungen

In der Modellierung der Zustände eines Quantensystems sind nach Abschnitt 1.2.1 die globalen Phasen $e^{i\alpha}$, $\alpha \in \mathbb{R}$, der Zustandsvektoren $e^{i\alpha}|\Phi\rangle$ irrelevant. Deshalb werden im Rahmen einiger Untersuchungen projektive Darstellungen betrachtet; so wird beispielsweise bei gleichzeitigen Messungen des Ortes und des Impulses eines Partikels durch eine projektive Darstellung die Heisenberg-Weyl-Gruppe erhalten, welche die Verschiebungen im Orts- und Impulsraum umfaßt (siehe Abschnitt 3.4 in [Dav76]). Projektive Darstellungen sind eine Verallgemeinerung von Darstellungen, wobei die Homomorphieforderung abgeschwächt wird (siehe z. B. §25 in [Dor71]):

Definition 2.11 (Unitäre projektive Darstellung) *Eine unitäre projektive Darstellung ist eine Abbildung $\sigma : G \to \mathcal{U}(d)$ mit*

$$\sigma(g)\sigma(h) = \gamma_{g,h}\sigma(gh)$$

für $\gamma_{g,h} \in \mathbb{C}$ und $|\gamma_{g,h}| = 1$. Die Abbildung $(g,h) \mapsto \gamma_{g,h}$ wird Faktorenmenge (factor set) genannt.

Einige Aussagen über Darstellungen können nicht unmittelbar auf projektive Darstellungen übertragen werden: Beispielsweise muß die direkte Summe von projektiven Darstellungen nicht wieder eine sein. Diese und andere Probleme (siehe z. B. Abschnitt 3.10 in [Ste94]) können umgangen werden, indem projektive Darstellungen in nicht-projektive überführt werden (siehe Th. 11.17 in [Isa76]):

Lemma 2.12 (Erweiterung projektiver Darstellungen) *Für jede endliche Gruppe G gibt es eine endliche Gruppe $\hat{G}$ mit einem surjektiven Homomorphismus $\pi : \hat{G} \to G$, so daß $\mathrm{Kern}(\pi) \subseteq \mathcal{Z}(\hat{G})$ für das Zentrum $\mathcal{Z}(\hat{G})$ von $\hat{G}$ gilt und für jede projektive Darstellung $\sigma : G \to \mathrm{GL}(\mathbb{C}, d)$ eine Darstellung $\hat{\sigma} : \hat{G} \to \mathrm{GL}(\mathbb{C}, d)$ zusammen mit einer Funktion $\phi : \hat{G} \to \mathbb{C}$ existiert, die $\hat{\sigma}(\hat{g}) = \phi(\hat{g})\sigma(\pi(\hat{g}))$ für $\hat{g} \in \hat{G}$ erfüllen.*

Die Gruppe $\hat{G}$ von Lemma 2.12 wird aufgrund $\mathrm{Kern}(\pi) \subseteq \mathcal{Z}(\hat{G})$ als zentrale Erweiterung von G bezeichnet (siehe Def. 11.8 in [Isa76]). Das Lemma besagt, daß die von dem Bild der projektiven Darstellung erzeugte Gruppe $\langle \phi_g \sigma(g) : g \in G \rangle$ endlich ist, falls die Faktoren $\phi_g \in \mathbb{C}$ geeignet gewählt werden. Die Matrizen dieser Gruppe unterscheiden sich von den ursprünglichen Matrizen $\sigma(g)$ nur um diese Phasenfaktoren. Deshalb kann bei vielen Untersuchungen ohne wesentliche Einschränkungen durch diese Konstruktion angenommen werden, daß eine nicht-projektive Darstellung vorliegt.

2.3 Symmetrische Ensembles und POVMs

Die Symmetrie von Ensembles oder POVMs wird durch die Operation einer Symmetriegruppe auf den zugehörigen Dichtematrizen bzw. POVM-Operatoren definiert: Sind diese Operatoren unter der Gruppenoperation invariant, so ist das Ensemble bzw. POVM symmetrisch.

Definition 2.13 (Symmetrie von Ensembles und POVMs) *Es sei $\sigma : G \to \mathcal{U}(d)$ eine unitäre Darstellung der endlichen Gruppe G. Ferner seien $X_0, \ldots, X_{n-1} \in \mathbb{C}^{d\times d}$ die*

Operatoren eines Ensembles bzw. POVMs. Dann ist für eine Permutationsdarstellung $\pi : G \to S_n$ auf den Indizes der X_j das Ensemble bzw. POVM (G, σ, π)-symmetrisch, falls die Gleichung

$$\sigma(g) X_j \sigma(g)^\dagger = X_{\pi(g)(j)}$$

für alle j und $g \in G$ gilt. Für Ensembles wird darüber hinaus angenommen, daß die Wahrscheinlichkeiten $p(j)$ der Zustände auf jeder Bahn von π konstant sind.

In manchen Fällen wird die Symmetrie eines Ensembles oder POVMs mit einer projektiven Darstellung anstatt einer nicht-projektiven Darstellung definiert. Der Vorteil ist hierbei, daß die zugehörige Symmetriegruppe weniger Elemente umfaßt. Da nach Lemma 2.12 eine mit einer projektiven Darstellungen definierte Symmetrie durch eine Symmetrie mit nicht-projektiver Darstellung ersetzt werden kann, umfaßt Def. 2.13 auch diese verallgemeinerte Symmetrie.

Beispiel 2.14 (Symmetrisches POVM) *Das POVM mit den Operatoren*

$$\Pi_0 := \frac{1}{3}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},\ \Pi_1 := \frac{1}{3}\begin{pmatrix} 1 & \omega_3^2 \\ \omega_3 & 1 \end{pmatrix} \quad \text{und} \quad \Pi_2 := \frac{1}{3}\begin{pmatrix} 1 & \omega_3 \\ \omega_3^2 & 1 \end{pmatrix}$$

ist symmetrisch bzgl. der Darstellung $\sigma : C_3 \to \mathcal{U}(2), r^j \mapsto \mathrm{diag}(1, \omega_3^j)$, der Symmetriegruppe $C_3 := \langle r : r^3 = 1 \rangle$, wobei $\omega_3 := e^{2\pi i/3}$ eine dritte Einheitswurzel bezeichnet. Die zugehörige Permutationsdarstellung $\pi : C_3 \to S_3$ ist durch $\pi(r)(0) = 1, \pi(r)(1) = 2$ und $\pi(r)(2) = 0$ festgelegt.

Eine besondere Eigenschaft des symmetrischen POVMs aus Bsp. 2.14 ist, daß ausgehend von Π_0 jeder Operator bei Anwendung der Gruppenelemente auftritt. Dies kann bei beliebigen Darstellungen durch Konstruktion erhalten werden:

Definition 2.15 (Gruppenerzeugtes POVM) *Es sei G eine endliche Gruppe mit der Anordnung $g_0, \ldots, g_{n-1}$ der Elemente und $\sigma : G \to \mathcal{U}(d)$ eine unitäre Darstellung vom Grad d. Bilden die n Operatoren*

$$\Pi_j := \sigma(g_j) \Pi \sigma(g_j)^\dagger \tag{2.3}$$

für einen geeigneten Operator Π ein POVM, so wird dieses als ein von G erzeugtes POVM mit dem initialen Operator Π bezeichnet.

Wird die Reihenfolge der Gruppenelemente bei der Betrachtung eines gruppenerzeugten POVMs nicht benötigt, so können die Operatoren als Π_g geschrieben werden. Ein gruppenerzeugtes POVM hat eine Symmetrie, die unmittelbar angegeben werden kann.

Lemma 2.16 (Symmetrie eines gruppenerzeugten POVMs) *Es sei P ein gruppenerzeugtes POVM mit dem initialen Operator Π und der Darstellung σ der Symmetriegruppe G. Die Anordnung der Gruppenelemente sei $g_0, \ldots, g_{n-1}$. Dann hat P die Symmetrie (G, σ, π) mit π aus Def. 2.5, d. h. π entspricht der regulären Darstellung von G.*

Beweis: Es folgt mit π wie in Def. 2.5 die Gleichung

$$\sigma(h) \Pi_j \sigma(h)^\dagger = \sigma(h)\sigma(g_j)\Pi\sigma(g_j)^\dagger\sigma(h)^\dagger = \sigma(g_{\pi(h)(j)})\Pi\sigma(g_{\pi(h)(j)})^\dagger = \Pi_{g_{\pi(h)(j)}}\,.$$

□

Für eine gegebene Darstellung muß nicht jeder initiale Operator zu einem POVM führen. Beispielsweise folgt für die Darstellung σ aus Bsp. 2.14 kein POVM für den Operator $\Pi = |0\rangle\langle 0|$. Ist die Darstellung σ jedoch irreduzibel, so kann für jeden semipositiven Operator Π, der geeignet normiert ist, ein POVM erhalten werden. Dies gilt aufgrund der Gleichung

$$\sigma(h)\left(\sum_{g\in G}\sigma(g)\Pi\sigma(g)^\dagger\right) = \left(\sum_{g\in G}\sigma(g)\Pi\sigma(g)^\dagger\right)\sigma(h),$$

die zusammen mit dem Schurschen Lemma (siehe Lemma 2.22 in Abschnitt 2.4) zeigt, daß $\sum_g \Pi_g = \alpha I_d$ mit einem $\alpha \in \mathbb{R}$ gilt. Mit der Spurnormierung $\mathrm{tr}(\Pi) = d/|G|$ wird aufgrund $\alpha = 1$ immer ein POVM erhalten. Eine ähnliche Konstruktion ist möglich, falls nicht von einem Operator, sondern von einem POVM ausgegangen wird:

Lemma 2.17 (Symmetrisierung eines POVMs) *Es sei P ein POVM auf einem d-dimensionalen System. Ferner sei $\sigma : G \to \mathcal{U}(d)$ eine unitäre Darstellung der endlichen Gruppe G. Dann bilden die Operatoren*

$$\Pi_{j,g} := \frac{1}{|G|}\sigma(g)\Pi_j\sigma(g)^\dagger \quad \textit{mit} \quad g \in G \quad \textit{und} \quad \Pi_j \in P \tag{2.4}$$

ein (G,σ,π)-symmetrisches POVM mit der durch $\pi(h)(j,g) := (j,hg)$ definierten Darstellung π. Dieses POVM wird als P^G geschrieben, falls die Darstellung σ festgelegt ist.

Beweis: Es gilt

$$\sum_{j,g}\Pi_{j,g} = \frac{1}{|G|}\sum_g \sigma(g)\left(\sum_j \Pi_j\right)\sigma(g)^\dagger = \frac{1}{|G|}\sum_g \sigma(g) I_d \sigma(g)^\dagger = I_d\,.$$

Die Darstellungseigenschaft von π folgt aus der Homomorphie von σ. □

Bei der Gruppenerzeugung und der Symmetrisierung eines POVMs ist es von Bedeutung, daß die Operatoren von Gl. (2.3) und (2.4) nicht in einer Menge zusammengefaßt werden, denn durch die Symmetrisierung können identische Operatoren entstehen. Die Summe der Operatoren ist aber nur dann die Identitätsmatrix, falls mehrfach auftretende Operatoren nicht entfernt werden.

2.4 Matrizen mit Symmetrie

Die Operationen auf einem Quantensystem entsprechen nach Lemma 1.17 unitären Transformationen, die in Ein-Qubit- und CNOT-Operationen zerlegt werden können (siehe Lemma 1.22). Hierbei werden jedoch bei Quantenregistern für die allgemeinen Zerlegungsverfahren nach Lemma 1.22 in der Anzahl der Qubits exponentiell viele dieser Operationen benötigt. Eine Möglichkeit, diesen exponentiellen Aufwand zu umgehen, bieten die symmetriebasierten Zerlegungsverfahren, denn mit diesen können für einige Matrizen deutlich bessere Zerlegungen gefunden werden. Die symmetriebasierten Verfahren können für Matrizen angewandt werden, die eine Symmetrie haben; diese wird durch zwei Darstellungen der Symmetriegruppe definiert (siehe Def. 2.1 in [Röt01]):

Definition 2.18 (Symmetrie einer Matrix) *Es seien sowohl $\sigma : G \to \mathcal{U}(m)$ als auch $\tau : G \to \mathcal{U}(n)$ Darstellungen der endlichen Gruppe G. Die Matrix $M \in \mathbb{C}^{m\times n}$ hat die Symmetrie (G, σ, τ), falls $\sigma(g)M = M\tau(g)$ für alle $g \in G$ gilt. Kurznotation: $\sigma M = M\tau$.*

Eine Matrix mit Symmetrie muß keine quadratische Matrix sein, womit die Darstellungen der Symmetrie verschiedene Grade haben können.

Beispiel 2.19 (Matrix mit Symmetrie) *Für $j \in \{0, 1, 2\}$ gilt die Gleichung*

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^j \begin{pmatrix} 1 & 1 \\ 1 & \omega_3^2 \\ 1 & \omega_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & \omega_3^2 \\ 1 & \omega_3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \omega_3 \end{pmatrix}^j,$$

wobei $\omega_3 := e^{2\pi i/3}$ eine dritte Einheitswurzel ist. Damit ist die (3×2)-Matrix in der Mitte (C_3, σ, τ)-symmetrisch, wobei $C_3 = \langle r : r^3 = 1\rangle$ die zyklische Gruppe der Ordnung drei ist. Die Darstellungen σ und τ sind festgelegt durch

$$\sigma(r) := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{und} \quad \tau(r) := \begin{pmatrix} 1 & 0 \\ 0 & \omega_3 \end{pmatrix}. \tag{2.5}$$

Die Symmetrie einer Matrix hat die Symmetrie der adjungierten Matrix zur Folge:

Lemma 2.20 (Symmetrie der adjungierten Matrix) *Es sei M eine (G, σ, τ)-symmetrische Matrix, wobei σ und τ unitäre Darstellungen seien. Dann hat $M^\dagger$ die Symmetrie (G, τ, σ).*

Beweis: Es gilt

$$\tau(g)M^\dagger = (M\tau(g)^\dagger)^\dagger = (M\tau(g^{-1}))^\dagger = (\sigma(g^{-1})M)^\dagger = (\sigma(g)^\dagger M)^\dagger = M^\dagger\sigma(g)$$

für alle $g \in G$. □

Die Matrizen mit einer vorgegebenen Symmetrie bilden einen Vektorraum, welcher als Raum der Verkettungsmatrizen oder einfacher als Verkettungsraum bezeichnet wird (*intertwining space*, siehe z. B. Def. 2.3 in [Röt01]).

Definition 2.21 (Verkettungsraum) *Es seien $\sigma : G \to \mathcal{U}(m)$ und $\tau : G \to \mathcal{U}(n)$ zwei Darstellungen der endlichen Gruppe G. Dann ist*

$$\mathrm{Int}(\sigma, \tau) := \{M \in \mathbb{C}^{m\times n} : \sigma M = M\tau\}$$

der Verkettungsraum von σ und τ.

Das wichtigste Hilfsmittel zur Untersuchung der Struktur von Matrizen in einem Verkettungsraum ist das Schursche Lemma (siehe Satz 27.3 in [CR62]):

Lemma 2.22 (Schursches Lemma) *Es seien $\sigma : G \to \mathcal{U}(m)$ und $\tau : G \to \mathcal{U}(n)$ irreduzible Darstellungen. Ferner sei $M \in \mathbb{C}^{m\times n}$ eine Matrix, die $\sigma M = M\tau$ erfüllt. Sind σ und τ inäquivalent, so gilt $M = 0$. Sind σ und τ gleich, so ist M ein $\mathbb{C}$-skalares Vielfaches der Einheitsmatrix.*

Das Schursche Lemma kann auf reduzible Darstellungen erweitert und damit auf $\mathrm{Int}(\sigma,\tau)$ für beliebige σ und τ angewandt werden, indem die Darstellungen nach Lemma 2.4 in ihre irreduziblen Komponenten zerlegt werden. Durch die Anwendung von Lemma 2.22 für jedes Paar von irreduziblen Komponenten kann die Struktur des Verkettungsraums ermittelt werden (siehe Satz 1.48 in [Püs98]):

Lemma 2.23 (Struktur des Verkettungsraums) *Es seien $\sigma : G \to \mathcal{U}(m)$ sowie $\tau : G \to \mathcal{U}(n)$ zwei Darstellungen mit den Zerlegungen*

$$\sigma = \bigoplus_{j=0}^{z-1} \left(I_{m_j} \otimes \kappa_j\right) \quad \textit{und} \quad \tau = \bigoplus_{j=0}^{z-1} \left(I_{n_j} \otimes \kappa_j\right) \tag{2.6}$$

in die irreduziblen Darstellungen κ_j, die paarweise inäquivalent sind. Dann gilt

$$\mathrm{Int}(\sigma,\tau) = \left(\mathbb{C}^{m_0\times n_0} \otimes I_{\deg(\kappa_0)}\right) \oplus \ldots \oplus \left(\mathbb{C}^{m_{z-1}\times n_{z-1}} \otimes I_{\deg(\kappa_{z-1})}\right).$$

Für $m_j = 0$ oder $n_j = 0$ werden in der direkten Summe $n_j\deg(\kappa_j)$ Nullspalten bzw. $m_j\deg(\kappa_j)$ Nullzeilen an der entsprechenden Stelle eingefügt.

Die Zerlegung des Verkettungsraums nach Lemma 2.23 zeigt, daß jede Matrix A von $\mathrm{Int}(\sigma,\tau)$ die Form

$$A = (A_0 \otimes I_{\deg(\kappa_0)}) \oplus \ldots \oplus (A_{z-1} \otimes I_{\deg(\kappa_{z-1})})$$

mit geeigneten Matrizen $A_j \in \mathbb{C}^{m_j\times n_j}$ hat. Durch geeignete Permutationsmatrizen P_j kann hierbei jeweils die Umordnung

$$P_j(A_j \otimes I_{\deg(\kappa_j)})P_j^\dagger = I_{\deg(\kappa_j)} \otimes A_j = A_j \oplus \ldots \oplus A_j$$

der Reihenfolge der Tensorkomponenten erhalten werden (siehe Lemma 1.22 in [Röt01]). Damit sind für Darstellungen mit geringen Multiplizitäten m_j und n_j die Matrizen in $\mathrm{Int}(\sigma,\tau)$ strukturiert und dünn besetzt.

Beispiel 2.24 (Verkettungsraum) *Für die beiden Darstellungen $\sigma = \kappa_0 \oplus \kappa_1 \oplus \kappa_2$ und $\tau = \kappa_0 \oplus \kappa_1$ mit den irreduziblen Darstellungen κ_j der Gruppe C_3 aus Bsp. 2.7 folgt der Verkettungsraum*

$$\mathrm{Int}(\sigma,\tau) = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \\ 0 & 0 \end{pmatrix} : \alpha,\beta \in \mathbb{C} \right\}.$$

Für $\sigma = \tau$ sind die Matrizen in $\mathrm{Int}(\sigma,\tau)$ quadratisch, womit $\mathrm{Int}(\sigma,\tau)$ auch hermitesche Matrizen enthält. Aufgrund der einfachen Struktur des Verkettungsraums kann die Dimension des enthaltenen Raums hermitescher Matrizen unmittelbar abgelesen werden.

Lemma 2.25 (Dimension des hermiteschen Verkettungsraums) *Es sei σ eine Darstellung, die wie in Def. 2.10 zerlegt sei. Dann ist die Dimension des $\mathbb{R}$-linearen Unterraums hermitescher Matrizen in $\mathrm{Int}(\sigma,\sigma)$ durch $\sum_{j=0}^{z-1} m_j^2$ gegeben.*

2.5 Symmetriebasierte Zerlegungsverfahren

Das Ziel symmetriebasierter Zerlegungsverfahren ist die Faktorisierung von Matrizen mit Symmetrie in ein Produkt strukturierter und dünn besetzter Matrizen. Diese Verfahren reduzieren hierbei die Matrixzerlegung im wesentlichen auf die Zerlegung von Darstellungen: Es sei hierzu M eine Matrix mit der Symmetrie (G, σ, τ) gegeben; zerlegen die Matrizen A und B die Darstellungen σ bzw. τ in die direkten Summen

$$A\sigma A^\dagger = \bigoplus_{j=0}^{z-1} \left(I_{m_j} \otimes \kappa_j\right) \quad \text{und} \quad B\tau B^\dagger = \bigoplus_{j=0}^{z-1} \left(I_{n_j} \otimes \kappa_j\right)$$

der irreduziblen Darstellungen κ_j, so folgt die Symmetrie

$$\left(\bigoplus_{j=0}^{z-1} (I_{m_j} \otimes \kappa_j)\right) (AMB^\dagger) = (AMB^\dagger) \left(\bigoplus_{j=0}^{z-1} (I_{n_j} \otimes \kappa_j)\right)$$

der Matrix $AMB^\dagger$. Nach Lemma 2.23 ist $AMB^\dagger$ eine strukturierte Matrix, die für Darstellungen mit geringen Multiplizitäten in σ und τ dünn besetzt ist. Können darüber hinaus die Matrizen A und B als Produkt strukturierter und dünn besetzter Matrizen geschrieben werden, so gilt dies ebenfalls für die Matrix

$$M = A^\dagger (AMB^\dagger) B\,,$$

womit die gewünschte Zerlegung von M gefunden ist. In der Quanteninformatik können für die weitere Zerlegung von M in Ein-Qubit- und CNOT-Gatter beispielsweise die Verfahren aus [BBC+95, Cyb01, VMS04] genutzt werden. Zusammen mit bekannten Implementierungsverfahren diskreter Fourier-Transformationen führen damit die symmetriebasierten Verfahren für einige unitäre Transformationen zu effizienten Quantenschaltkreisen (siehe z. B. Abschnitt 4.1.3 in [Röt01]).

Die zentralen Probleme bei den symmetriebasierten Verfahren sind das Auffinden einer Matrixsymmetrie sowie die Konstruktion der Matrizen A und B. Hat eine Matrix eine Symmetrie, so kann diese für einige Symmetrieklassen algorithmisch gefunden werden (siehe Kap. 3 bis 5 in [Egn97]). In den folgenden Untersuchungen werden diese Algorithmen nicht benötigt, denn die Symmetrie von POVMs und Zuständen führt unmittelbar zu einer Matrixsymmetrie. Die Zerlegungsmatrizen A und B können mit Algorithmus 4.1 aus [Püs02] für auflösbare Gruppen konstruiert werden. Dieser Algorithmus steht im Programmpaket *AREP* des Computeralgebrasystems *GAP 3* zur Verfügung (siehe [S+97]) und gibt die Zerlegungsmatrizen der Darstellungen in geeigneter Faktorisierung aus:

Beispiel 2.26 (Zerlegung einer Darstellung) *Für die durch*

$$\sigma_{\text{reg}}(r) := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

gegebene reguläre Darstellung der Gruppe $C_4 := \langle r : r^4 = 1 \rangle$ *findet der Algorithmus die Zerlegungsmatrix*

$$F_4^\dagger = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} (F_2 \otimes I_2) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} (I_2 \otimes F_2) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

die als Produkt strukturierter und dünn besetzter Matrizen ausgegeben wird.

Die Grundlage des Algorithmus bilden Induktionen von Darstellungen (siehe z. B. Abschnitt 1.1 in [Püs98]).

Definition 2.27 (Induktion einer Darstellung) *Es sei* H *eine Untergruppe der endlichen Gruppe* G *vom Index* m *mit der Transversalen* $T = (t_0, \ldots, t_{m-1})$*, die als geordnete Liste der Vertreter* $t_0, \ldots, t_{m-1}$ *der Rechtsnebenklassen* $H\backslash G$ *definiert wird. Dann ist für eine Darstellung* σ *von* H *durch*

$$(\sigma \uparrow_T G)(g) := \begin{pmatrix} \dot\sigma(t_0 g t_0^{-1}) & \cdots & \dot\sigma(t_0 g t_{m-1}^{-1}) \\ \vdots & \ddots & \vdots \\ \dot\sigma(t_{m-1} g t_0^{-1}) & \cdots & \dot\sigma(t_{m-1} g t_{m-1}^{-1}) \end{pmatrix} \text{ mit } \dot\sigma(g) := \begin{cases} \sigma(g) & : g \in H \\ 0_{\deg(\sigma)} & : g \notin H \end{cases}$$

die Induktion von σ *auf* G *bezüglich der Transversalen* T *definiert, wobei* $0_{\deg(\sigma)}$ *die quadratische Nullmatrix der Größe* $\deg(\sigma)$ *bezeichnet.*

Liegt eine monomiale Darstellung σ vor, d. h. die Matrizen haben in jeder Zeile und Spalte genau ein nicht verschwindendes Element (siehe z. B. §43, Kap. VII in [CR62]), so kann durch Permutation der Elemente der zugrunde liegenden Vektorraumbasis eine Zerlegung $\sigma_0 \oplus \ldots \oplus \sigma_{k-1}$ von σ erhalten werden, wobei alle σ_j transitiv sind. Jede dieser Darstellungen kann als Induktion geschrieben werden (siehe Th. 3.15 und 3.16 in [Püs02]):

Lemma 2.28 (Monomiale Darstellungen als Induktion) *Es sei* $\sigma : G \to \mathcal{U}(d)$ *eine transitive, monomiale Darstellung. Dann gibt es eine Untergruppe* H *mit einer Transversalen* T *und einer Darstellung* τ *vom Grad eins, so daß* σ *zu* $\tau \uparrow_T G$ *äquivalent ist.*

Die Formulierung einer monomialen Darstellungen als Induktion ist die Grundlage eines rekursiven Zerlegungsverfahrens, denn unter geeigneten Voraussetzungen ist es möglich, von der Zerlegungsmatrix einer Darstellung σ von H auf die Zerlegungsmatrix der Induktion $\sigma \uparrow_T G$ zu schließen. Einen Zusammenhang zwischen irreduziblen Darstellungen einer Gruppe und deren Untergruppen stellt hierbei eine Variante des Theorems von Clifford her (siehe z. B. Th. 3.31 in [Püs02]):

Satz 2.29 (Clifford-Theorem) *Es sei* N *ein Normalteiler von* G *mit Primzahlindex* p *und* T *eine Transversale mit den Elementen* $t^0, \ldots, t^{p-1}$*. Ferner sei* σ *eine irreduzible Darstellung von* N*. Dann gibt es zwei Fälle:*

1. *Die Darstellungen* $\sigma^j : g \mapsto \sigma(t^j g t^{-j})$ *sind für alle* j *zu* σ *äquivalent. Dann kann* σ *zu* $\overline{\sigma}$ *erweitert werden, d. h.* $\overline{\sigma}$ *ist eine Darstellung von* G*, die auf* N *mit* σ *übereinstimmt. Die* p *inäquivalenten und irreduziblen Darstellungen* $\overline{\sigma}^j := \lambda_j \overline{\sigma}$*, wobei* $\lambda_j(t^k) = \omega_p^{jk}$ *eine Darstellung von* G/N *ist, sind alle möglichen Erweiterungen von* σ*. Die Darstellungen* $\sigma \uparrow_T G$ *und* $\overline{\sigma}^0 \oplus \ldots \oplus \overline{\sigma}^{p-1}$ *sind äquivalent.*

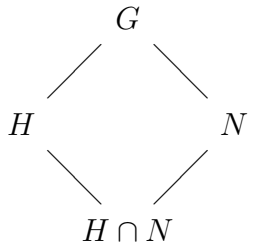

Abbildung 2.1: Die Gruppen und deren Anordnung in Lemma 2.30.

2. *Die Darstellungen σ^j sind für alle j nicht zu σ äquivalent. Dann ist $\sigma \uparrow_T G$ irreduzibel und die Einschränkung von $\sigma \uparrow_T G$ auf N ist zu $\sigma^0 \oplus \ldots \oplus \sigma^{p-1}$ äquivalent.*

Um dieses Theorem anzuwenden, wird ein Normalteiler von Primzahlindex benötigt, der bei auflösbaren Gruppen immer existiert (siehe Satz 6, Abschnitt 5.4 in [Bos96]). Werden der Normalteiler N und die Gruppe H aus Lemma 2.28 betrachtet, so gilt entweder $H \leq N$ oder $H \not\leq N$.

Im Fall $H \leq N \trianglelefteq G$ kann der Induktionsschritt $\sigma \uparrow_T G$ in die beiden Schritte

$$(\sigma \uparrow_{T_1} N) \uparrow_{T_2} G$$

zerlegt werden, wobei T_1 sowie $T_2 = (t^0, \ldots, t^{p-1})$ geeignete Transversalen sind (siehe Th. 3.2 in [Püs02]). Hierbei kann die Zerlegungsmatrix von $(\sigma \uparrow_{T_1} N) \uparrow_{T_2} G$ ausgehend von der Zerlegungsmatrix A von $\sigma \uparrow_{T_1} N$ konstruiert werden: Bei Konjugation mit $I_p \otimes A$ wird jede Komponente $\dot{\sigma}(t^j g t^{-k})$ der Induktion mit A konjugiert, also in irreduzible Komponenten zerlegt. Da ferner $(\tau_1 \oplus \tau_2) \uparrow_T G$ über eine Permutation zu $(\tau_1 \uparrow_T G) \oplus (\tau_2 \uparrow_T G)$ äquivalent ist (siehe Th. 3.3 in [Püs02]), kann durch diese Permutation die gesamte Induktion auch auf den einzelnen irreduziblen Komponenten betrachtet werden. Für die irreduziblen Darstellungen aus dem zweiten Fall des Clifford-Theorems führt die Induktion direkt zu irreduziblen Darstellungen, so daß hierfür keine weiteren Zerlegungsschritte notwendig sind. Die anderen Darstellungen können in einer Darstellung τ zusammengefaßt werden, welche die Erweiterung $\overline{\tau}$ hat. Durch die Konjugation der Induktion $\tau \uparrow_T G$ mit der Matrix $\overline{\tau}(t^0) \oplus \ldots \oplus \overline{\tau}(t^{p-1})$ werden die Komponenten der Induktion alle gleich (siehe Th. 3.11 in [Püs02]), womit die Darstellung $(1_N \uparrow_{T_2} G) \otimes \overline{\tau}$ folgt. Die Induktion $1_N \uparrow_{T_2} G$ kann durch die DFT-Matrix F_p zerlegt werden. Insgesamt folgt die Zerlegung von $(\sigma \uparrow_{T_1} N) \uparrow_{T_2} G$ in irreduzible Komponenten.

Im zweiten Fall $H \not\leq N \trianglelefteq G$ wird die Zerlegung der Induktion von H nach G durch die Zerlegung einer Induktion von $H \cap N$ nach N erhalten. Hierzu wird wie in Abb. 2.1 der obere Weg von H nach N über G durch den unteren Weg über $H \cap N$ ersetzt (siehe Kor. 3.10 in [Püs02]):

Lemma 2.30 (Wechsel der Untergruppe) *Es seien $H \leq G$ und $N \trianglelefteq G$ mit $HN = G$ gegeben. Ferner seien σ eine Darstellung von H und T eine Transversale von $(H \cap N) \backslash N$. Dann ist T auch eine Transversale von $H \backslash G$ und es gilt*

$$(\sigma \uparrow_T G) \downarrow N = (\sigma \downarrow (H \cap N)) \uparrow_T N\,,$$

wobei $\tau \downarrow K$ die Einschränkung einer Darstellung τ auf die Untergruppe K bezeichnet.

Das Lemma kann mit dem Mackey-Theorem (siehe Th. 3.8 in [Püs02]) bewiesen werden. Das Lemma zeigt, daß $\sigma \uparrow_T G$ eine Erweiterung von $(\sigma \downarrow (H \cap N)) \uparrow_T N$ ist. Damit kann bei dem rekursiven Verfahren die Gruppe G der untersuchten Darstellung auf N reduziert werden, falls die Zerlegungsmatrix der Erweiterung aus der Zerlegungsmatrix A von $(\sigma \downarrow (H \cap N)) \uparrow_T N$ gewonnen werden kann. Den Zusammenhang zwischen diesen Matrizen stellt hierbei aufgrund $N \trianglelefteq G$ wieder das Clifford-Theorem her: Durch A wird $\sigma \uparrow_T G$ in Komponenten τ_j zerlegt, die so angeordnet und konjugiert werden können, daß $\tau_j \downarrow N$ entweder in $\mu_j \oplus \ldots \oplus \mu_j$ für ein erweiterbares μ_j zerfällt oder in $\mu_j^0 \oplus \ldots \oplus \mu_j^{p-1}$ für ein nicht erweiterbares μ_j. Für die erweiterbaren μ_j folgt nach dem Clifford-Theorem, daß τ_j in die inäquivalenten und irreduziblen Darstellungen $\overline{\mu}_j^k$ zerfällt. Für die nicht erweiterbaren μ_j zerfällt τ_j in die direkte Summe mehrerer Kopien der Induktion $\mu_j \uparrow_T G$. In beiden Fällen können die zugehörigen Zerlegungsmatrizen der τ_j berechnet werden (siehe Th. 3.37 und 3.38 in [Püs02]).

Die wesentlichen Bestandteile des rekursiven Zerlegungsalgorithmus aus [Püs02] sind die Konstruktion der Zerlegungsmatrizen für die Fälle $H \leq N \trianglelefteq G$ und $H \not\leq N \trianglelefteq G$. Daneben treten noch weitere Fälle auf, beispielsweise Induktionen $\sigma \uparrow_T G$ mit abelschem G oder Darstellungen, die zu einem äußeren Tensorprodukt äquivalent sind (siehe den vierten und fünften Fall in Algorithmus 4.1 in [Püs02]). In allen Fällen können rekursiv Zerlegungsmatrizen konstruiert werden, die ein Produkt strukturierter und dünn besetzter Matrizen sind.

2.6 Unitäre Ergänzung von Matrizen mit Symmetrie

Das Hauptproblem in Kapitel 4 und 5 ist die Ergänzung einer Matrix mit orthonormalen Spalten und der Symmetrie (G, σ, τ) zu einer unitären Matrix $\tilde{M}$, indem der Matrix M geeignete Spalten hinzugefügt werden. Bei dieser Ergänzung soll die Symmetrie von M möglichst gut erhalten bleiben, damit symmetriebasierte Zerlegungsverfahren angewandt werden können. Im folgenden wird gezeigt, daß die Matrix $\tilde{M}$ immer so konstruiert werden kann, daß sie die Symmetrie $(G, \sigma, \tau \oplus \tilde{\tau})$ mit einer geeigneten Darstellung $\tilde{\tau}$ von G hat, womit die Symmetrie von M vollständig erhalten bleibt. Die dabei angewandte Ergänzungsmethode nutzt aus, daß die Darstellungen σ und τ der Symmetrie (G, σ, τ) nicht beliebig sein können. Die Einschränkungen an die beiden Darstellungen folgen unmittelbar aus dem Rang der Matrix (siehe Th. 5 in [DJR05]):

Satz 2.31 (Majorisierung der Multiplizitäten) *Es seien für $m \geq n$ die beiden Darstellungen $\sigma : G \to \mathcal{U}(m)$ und $\tau : G \to \mathcal{U}(n)$ der endlichen Gruppe G gegeben. Ferner sei $M \in \mathbb{C}^{m \times n}$ eine Matrix mit der Symmetrie (G, σ, τ). Gilt $\mathrm{Rang}(M) = n$, so folgt $m_j \geq n_j$ für die Multiplizitäten m_j und n_j der irreduziblen Darstellungen κ_j in σ bzw. τ.*

Beweis: Nach Lemma 2.4 existieren unitäre Matrizen A und B, welche σ und τ in die direkten Summen

$$A\sigma A^\dagger = \bigoplus_{j=0}^{z-1} (I_{m_j} \otimes \kappa_j) \quad \text{und} \quad B\tau B^\dagger = \bigoplus_{j=0}^{z-1} (I_{n_j} \otimes \kappa_j) \tag{2.7}$$

zerlegen. Es folgt die durch

$$\left(\bigoplus_{j=0}^{z-1}(I_{m_j}\otimes\kappa_j)\right)(AMB^\dagger)=(AMB^\dagger)\left(\bigoplus_{j=0}^{z-1}(I_{n_j}\otimes\kappa_j)\right) \tag{2.8}$$

definierte Symmetrie der Matrix $AMB^\dagger$. Mit Lemma 2.23 folgt

$$AMB^\dagger=\bigoplus_{j=0}^{z-1}(M_j\otimes I_{\deg(\kappa_j)})$$

für $M_j\in\mathbb{C}^{m_j\times n_j}$, wobei auch Matrizen der Größe $m_j\times 0$ betrachtet werden. Die Multiplikation von M mit den unitären Matrizen A und $B^\dagger$ ändert den Rang nicht. Es folgen daher die beiden Gleichungen

$$n=\mathrm{Rang}(AMB^\dagger)=\sum_{j=0}^{z-1}\deg(\kappa_j)\mathrm{Rang}(M_j)\quad\text{und}\quad n=\sum_{j=0}^{z-1}\deg(\kappa_j)n_j\,.$$

Da $\mathrm{Rang}(M_j)\leq n_j$ gilt, muß $\mathrm{Rang}(M_j)=n_j$ für alle j gelten. Da M_j eine Matrix der Größe $m_j\times n_j$ ist, muß die Ungleichung $m_j\geq n_j$ gelten, damit diese Rangbedingungen erfüllt werden können. □

Satz 2.31 kann insbesondere angewandt werden, wenn der Rang der Matrix durch die Orthonormalität der Spalten garantiert wird:

Korollar 2.32 (Majorisierung durch orthonormale Spalten) *Für $m\geq n$ seien σ, τ und M wie in Satz 2.31. Hat M orthonormale Spalten, so folgt $m_j\geq n_j$ für die Multiplizitäten m_j und n_j der irreduziblen Darstellungen κ_j in σ bzw. τ.*

Im Beweis von Satz 2.31 wird genutzt, daß sich der Rang einer Matrix bei der Multiplikation mit unitären Matrizen nicht ändert. Damit Kor. 2.32 gilt, muß bei diesen Multiplikationen auch die Orthonormalität der Spalten erhalten bleiben:

Lemma 2.33 (Erhaltung der Spaltenorthonormalität) *Es sei $M\in\mathbb{C}^{m\times n}$ eine Matrix mit orthonormalen Spalten. Dann hat auch AMB orthonormale Spalten für alle $A\in\mathcal{U}(m)$ und $B\in\mathcal{U}(n)$.*

Beweis: Da M orthonormale Spalten hat, gilt $M^\dagger M=I_n$ für die Gram-Matrix der Spalten (siehe z. B. §3.3 in [Koe85]). Es folgt

$$(AMB)^\dagger(AMB)=B^\dagger M^\dagger A^\dagger AMB=B^\dagger I_n B=I_n$$

für die Gram-Matrix der Spalten von AMB. Damit sind auch die Spalten von AMB orthonormal. □

Die Ergänzung der Matrix M mit orthonormalen Spalten zu einer unitären Matrix ist immer möglich, falls keine Symmetrie gefordert wird, indem geeignete orthonormale Spalten hinzugefügt werden. Werden diese Spalten zu der Matrix N zusammengefaßt, entspricht diese Ergänzung der Zusammensetzung von M und N:

Definition 2.34 (Zusammensetzung von Matrizen) *Es seien die beiden Matrizen* $M := (|\Phi_1\rangle \dots |\Phi_m\rangle) \in \mathbb{C}^{d\times m}$ *und* $N := (|\Psi_1\rangle \dots |\Psi_n\rangle) \in \mathbb{C}^{d\times n}$ *mit den Spalten* $|\Phi_j\rangle \in \mathbb{C}^d$ *bzw.* $|\Psi_j\rangle \in \mathbb{C}^d$ *gegeben. Dann bezeichnet*

$$(M|N) := (|\Phi_1\rangle \dots |\Phi_m\rangle|\Psi_1\rangle \dots |\Psi_n\rangle) \in \mathbb{C}^{d\times(m+n)}$$

die Zusammensetzung von M *und* N*.*

Soll bei der Ergänzung von M zu der unitären Matrix $\tilde{M}$ eine Symmetrie erhalten werden, so unterliegt diese Symmetrie aufgrund der Unitarität einer starken Einschränkung, die unmittelbar aus Lemma 2.6 folgt:

Lemma 2.35 (Unitäre Matrizen mit Symmetrie) *Es sei* $M \in \mathcal{U}(d)$ *eine unitäre Matrix mit der Symmetrie* $\sigma M = M\tau$*. Dann sind* σ *und* τ *äquivalent, d. h. jede irreduzible Darstellung hat in* σ *und* τ *dieselbe Multiplizität.*

Gemeinsam geben Kor. 2.32 und Lemma 2.35 den Weg vor, wie eine Matrix mit Symmetrie und orthonormalen Spalten zu einer unitären Matrix ergänzt werden kann, deren Symmetrie ebenfalls eine Ergänzung ist: Nach Kor. 2.32 folgt $m_j \geq n_j$ in den Zerlegungen von Gl. (2.6) für eine Matrix M mit $\sigma M = M\tau$ und orthonormalen Spalten. Soll diese Matrix zu einer unitären Matrix ergänzt werden, deren Symmetrie ebenfalls eine Erweiterung ist, so muß nach Lemma 2.35 die Gleichung $m_j = n_j$ gelten. Damit ist festgelegt, wie die Symmetrie erweitert werden muß, falls dies möglich ist: Jede Darstellung, für die $m_j > n_j$ gilt, muß bei dieser Erweiterung $m_j - n_j$ mal zusätzlich aufgenommen werden. Die gemeinsame Ergänzung von M und der Symmetrie läßt sich einfach durchführen, falls nacheinander die Multiplizitäten aller irreduziblen Darstellungen von σ und τ angeglichen werden, während die Matrix M entsprechend ergänzt wird:

Lemma 2.36 (Ergänzung einer irreduziblen Darstellung) *Es sei* M *eine Matrix mit orthonormalen Spalten und der Symmetrie*

$$(\sigma \oplus (I_m \otimes \kappa))M = M(\tau \oplus (I_n \otimes \kappa)), \tag{2.9}$$

wobei κ *irreduzibel ist und in* σ *sowie* τ *jeweils die Multiplizität null hat. Dann existiert eine Matrix* N*, so daß die Zusammensetzung* $\tilde{M} := (M|N)$ *orthonormale Spalten und die Symmetrie*

$$(\sigma \oplus (I_m \otimes \kappa))\tilde{M} = \tilde{M}(\tau \oplus (I_m \otimes \kappa)) \tag{2.10}$$

hat, wobei die Darstellung auf der rechten Seite im Vergleich zu Gl. (2.9) um $m - n$ *Komponenten* κ *ergänzt wird.*

Beweis: Da M orthonormale Spalten hat und die Multiplizität von κ in σ sowie τ null ist, folgt nach Kor. 2.32, daß $m \geq n$ gilt. Daher kann $I_n \otimes \kappa$ auf der rechten Seite von Gl. (2.9) durch Hinzufügen von $n - m$ Komponenten κ zu $I_m \otimes \kappa$ ergänzt werden. Die Matrix M hat nach Lemma 2.23 die Zerlegung $M = M_0 \oplus (A \otimes I_d)$ mit einer geeigneten Matrix M_0, wobei $d := \deg(\kappa)$ den Grad von κ bezeichnet und $A \in \mathbb{C}^{m\times n}$ gilt. Es kann hierbei auch der Fall $n = 0$ auftreten, womit $M_0 \oplus A$ durch Hinzufügen von md Nullzeilen aus M_0 erhalten wird. Die Matrix M soll zu einer Matrix $\tilde{M}$ im Verkettungsraum der Darstellungen von Gl. (2.10) ergänzt werden. So eine Ergänzung hat nach Lemma 2.23

eine Zerlegung $\tilde{M} = M_0 \oplus (B \otimes I_d)$, wobei $B \in \mathbb{C}^{m\times m}$ gilt. Da A orthonormale (oder im Fall $n = 0$ gar keine) Spalten hat und B eine quadratische Matrix ist, kann A durch Ergänzen $m - n$ orthonormaler Spalten zu B erweitert werden. Diese orthonormalen Spalten können in der Matrix $C \in \mathbb{C}^{m\times(m-n)}$ zusammengefaßt werden. Das Lemma folgt mit der Matrix $C \otimes I_d$, die um so viele Nullzeilen ergänzt wird, wie M_0 Zeilen hat. □

Die Ergänzung ist nicht eindeutig, denn die hinzugefügten Spalten können jeweils mit einem Phasenfaktor multipliziert werden, ohne daß die Orthogonalität verloren geht.

Beispiel 2.37 (Ergänzung einer Darstellung) *Nach Bsp. 2.24 hat die Matrix*

$$M := \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathbb{C}^{3\times 2} \tag{2.11}$$

die Symmetrie $(C_3, \kappa_0 \oplus \kappa_1 \oplus \kappa_2, \kappa_0 \oplus \kappa_1)$ *mit den* κ_j *aus Bsp. 2.7. Bei dieser Symmetrie kann die rechte Darstellung einmal um* κ_2 *ergänzt werden, womit die ergänzte Matrix* $\tilde{M}$ *die Form*

$$\tilde{M} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha \end{pmatrix} \in \mathcal{U}(3)$$

haben muß für ein $\alpha \in \mathbb{C}$ *mit* $|\alpha| = 1$.

Das Lemma kann mehrmals angewandt werden, um in den Zerlegungen (2.6) von σ und τ nacheinander alle Multiplizitäten n_j auf m_j zu erhöhen.

Korollar 2.38 (Ergänzung mehrerer irreduzibler Darstellungen) *Es sei* M *eine Matrix mit orthonormalen Spalten und der durch*

$$\left(\bigoplus_{j=0}^{z-1}(I_{m_j} \otimes \kappa_j)\right) M = M \left(\bigoplus_{j=0}^{z-1}(I_{n_j} \otimes \kappa_j)\right) \tag{2.12}$$

definierten Symmetrie. Dann existiert eine Matrix N*, so daß* $\tilde{M} := (M|N)$ *unitär ist und die Symmetrie*

$$\left(\bigoplus_{j=0}^{z-1}(I_{m_j} \otimes \kappa_j)\right) \tilde{M} = \tilde{M} \left(\bigoplus_{j=0}^{z-1}(I_{n_j} \otimes \kappa_j) \oplus \bigoplus_{j=0}^{z-1}(I_{m_j-n_j} \otimes \kappa_j)\right) \tag{2.13}$$

hat. Dies bedeutet, daß neben M *auch die Symmetrie auf der rechten Seite von Gl. (2.12) ergänzt werden kann.*

Beweis: Siehe Anhang B.1. □

Da nach Lemma 2.33 die Multiplikation einer Matrix mit unitären Matrizen nicht die Orthonormalität der Spalten beeinflußt, kann das Korollar auch für beliebige Darstellungen, welche die Symmetrie definieren, angewandt werden:

Satz 2.39 (Unitäre Ergänzung mit Symmetrie) *Es sei M eine Matrix mit orthonormalen Spalten und der Symmetrie (G, σ, τ). Ferner seien A und B Matrizen, welche wie in Gl. (2.7) die Darstellungen σ und τ in direkte Summen irreduzibler Komponenten zerlegen. Dann existiert eine Matrix N, so daß*

$$\tilde{M} := A^\dagger(AMB^\dagger|N)(B \oplus \tilde{B}) = (M|A^\dagger N\tilde{B})$$

für alle unitären $\tilde{B}$ passender Größe eine unitäre Matrix mit der Symmetrie $(G, \sigma, \tau \oplus \tilde{\tau})$ ist, wobei $\tilde{\tau}$ die durch

$$\tilde{\tau} := \tilde{B}^\dagger \left(\bigoplus_{j=0}^{z-1} (I_{m_j - n_j} \otimes \kappa_j) \right) \tilde{B} \tag{2.14}$$

definierte Darstellung ist.

Beweis: Es gilt Gl. (2.8) mit A und B aus dem Satz. Nach Kor. 2.38 existiert eine Matrix N, so daß

$$(A\sigma A^\dagger)(AMB^\dagger|N) = (AMB^\dagger|N) \left(B\tau B^\dagger \oplus \bigoplus_{j=0}^{z-1} (I_{m_j - n_j} \otimes \kappa_j) \right)$$

folgt. Mit der Darstellung $\tilde{\tau}$ aus Gl. (2.14) für eine beliebige unitäre Matrix $\tilde{B}$ kann diese Gleichung als

$$(A\sigma A^\dagger)(AMB^\dagger|N) = (AMB^\dagger|N)(B \oplus \tilde{B})(\tau \oplus \tilde{\tau})(B \oplus \tilde{B})^\dagger$$

geschrieben werden. Die Matrix $\tilde{M}$ wird durch die Umstellung der Matrizen dieser Gleichung erhalten. □

Die Matrix M, die nach Satz 2.39 konstruiert wird, ist nicht eindeutig bestimmt, denn die Matrix N kann beliebig gewählt werden, sofern die resultierende Matrix unitär ist und die Struktur des Verkettungsraums hat. Diese Wahl stellt bei der Konstruktion von $\tilde{M}$ einen Freiheitsgrad dar, der als Grundlage von Optimierungen gesehen werden kann. Ein weiterer Freiheitsgrad besteht in der Wahl der unitären Matrix $\tilde{B}$, die beliebig gewählt werden kann.

Beispiel 2.40 (Unitäre Ergänzung) *Die Einträge von M mit der Symmetrie (C_3, σ, τ) aus Bsp. 2.19 werden durch $\sqrt{3}$ dividiert, um orthonormale Spalten zu erhalten. Mit den Zerlegungsmatrizen $A := F_3$ sowie $B := I_2$ folgt die durch*

$$(\kappa_0 \oplus \kappa_1 \oplus \kappa_2)(F_3 M) = (F_3 M)(\kappa_0 \oplus \kappa_1)$$

festgelegte Symmetrie der Matrix $AMB^\dagger = F_3 M$, welche die Matrix aus Gl. (2.11) ist. Damit folgt dieselbe Ergänzung

$$N := \begin{pmatrix} 0 \\ 0 \\ \alpha \end{pmatrix} \in \mathbb{C}^{3\times 1}$$

wie in Bsp. 2.37 mit $|\alpha| = 1$. *Nach der Rücktransformation erhält man für die Matrix* $\tilde{B} := (1) \in \mathcal{U}(1)$ *die unitären Ergänzungen*

$$\tilde{M} := A^\dagger(F_3 M|N)(B \oplus \tilde{B}) = F_3^\dagger(F_3 M|N) = \sqrt{\frac{1}{3}} \begin{pmatrix} 1 & 1 & \alpha \\ 1 & \omega_3^2 & \alpha\omega_3 \\ 1 & \omega_3 & \alpha\omega_3^2 \end{pmatrix}$$

von M. *Diese Ergänzungen haben die Symmetrie* $(C_3, \sigma, \kappa_0 \oplus \kappa_1 \oplus \kappa_2)$ *mit* σ *aus Gl. (2.5).*

Kapitel 3

Optimale symmetrische POVMs

Bei den beiden bekanntesten Quantenalgorithmen, dem Shorschen Faktorisierungsalgorithmus und dem Suchalgorithmus von Grover (siehe Abschnitte 5.3 und 6.1 in [NC00]), werden am Ende die Ausgaben durch Zustände repräsentiert, die durch eine Messung in der Standardbasis voneinander unterschieden werden können. Dahingegen gibt es aber auch Probleme, bei denen bisher nur die schwächere Aussage bekannt ist, daß eine effiziente Lösung aus der Unterscheidung von Zuständen eines bestimmten, symmetrischen Ensembles folgt. Eine wichtige Klasse solcher Probleme bilden die Probleme der verborgenen Untergruppen (siehe Abschnitt 3.1.3). Zur Lösung dieser Probleme müssen daher noch Messungen gefunden werden, mit denen das Auslesen der Resultate möglich ist.

Die Zustandsunterscheidung ist nicht nur bei den algorithmischen Problemen von Bedeutung, sondern auch bei der Kommunikation, denn hierbei benötigt ein Empfänger Messungen, um die ihm zugesandte Information zu ermitteln. Die Unterscheidung nichtorthogonaler Zustände muß in Betracht gezogen werden, denn solche Zustände können während einer Übertragung durch Störungen entstehen. Darüber hinaus werden nichtorthogonale Zustände in der Quantenkryptographie eingesetzt, um Übertragungen gegen Abhören zu sichern. Eine Symmetrie kann hierbei als Ausgangspunkt dienen, um auf der Sender- und Empfängerseite sowie bei der Sicherheitsanalyse Vereinfachungen zu erhalten.

Werden zur Unterscheidung der Zustände eines gegebenen Ensembles optimale Messungen gesucht, so stehen verschiedene Kriterien zur Verfügung, um die Güte eines POVMs zu bewerten. Die Untersuchungen in diesem Kapitel konzentrieren sich auf die Bayes-Kosten und die Transinformation, da sich diese als wichtigste Kriterien herausstellen. Den Bayes-Kosten und der Transinformation ist gemein, daß für symmetrische Ensembles optimale POVMs existieren, die ebenfalls symmetrisch sind. Damit kann die Optimierung auf diese speziellen POVMs beschränkt werden, womit insbesondere die zu der Transinformation gehörenden nicht-linearen Optimierungsprobleme in manchen Fällen stark vereinfacht werden können.

3.1 Optimale Detektion

Bei der Übertragung nicht-quantenmechanischer Signale stehen einem Empfänger mehrere gut untersuchte Optimalitätskriterien wie z. B. das Bayes-, Maximum-a-posteriori- oder Neyman-Pearson-Kriterium zur Verfügung (siehe Abschnitt 4.1 in [Kro96]), um zu entscheiden, welches Signal eine Quelle gesendet hat. Diese Kriterien können auf die De-

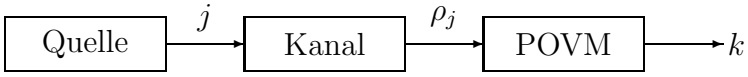

Abbildung 3.1: Übertragungsmodell zur Definition der Bayes-Kosten. Das Signal j wird gemäß der Verteilung $p(j)$ in den Kanal gegeben, ρ_j ist die zugehörige Ausgabe. Bei der Messung wird das Resultat k mit der Wahrscheinlichkeit $\mathrm{tr}(\rho_j \Pi_k)$ erhalten, womit die Bayes-Kosten nach Def. 3.1 festgelegt werden.

tektion von Quantenzuständen übertragen werden; hierbei sind hauptsächlich die Bayes-Kosten von Interesse, da diese der Suche nach Messungen, welche bei der Detektion die minimale Fehlerwahrscheinlichkeit erreichen, als Grundlage dienen.

3.1.1 Die Bayes-Kosten

Das Bayes-Verfahren der statistischen Entscheidungstheorie läßt sich einfach auf die Detektion von Quantenzuständen übertragen, falls es im Rahmen von Signalübertragungen formuliert wird (siehe Kapitel II in [Hel76]): Eine Quelle wählt wie in Abb. 3.1 eine Nachricht $j \in \{0, \ldots, m-1\}$ mit der Wahrscheinlichkeit $p(j)$ aus und übergibt diese an einen Kanal. Dieser gibt den Zustand ρ_j aus, der beim Empfänger durch ein POVM mit den Operatoren Π_k gemessen wird. Dem Meßresultat k wird die Hypothese zugeordnet, daß die Quelle das Signal k ausgegeben hat. Für diese Hypothese werden bei tatsächlich gesendeten Signal j die Kosten $C_{k,j}$ berechnet, womit sich durch Mittelung für ein Ensemble und ein POVM die Bayes-Kosten festlegen lassen (siehe Abschnitt IV.1 in [Hel76]).

Definition 3.1 (Bayes-Kosten) *Es seien ρ_j die Zustände eines Ensembles mit den Wahrscheinlichkeiten $p(j)$. Ferner seien Π_k die Operatoren eines POVMs. Dann sind die Bayes-Kosten des Ensembles und des POVMs gegeben durch*

$$\overline{C} := \sum_{j,k=0}^{m-1} p(j) C_{k,j} \mathrm{tr}(\rho_j \Pi_k) \,.$$

Bei der Definition der Bayes-Kosten wird angenommen, daß die Anzahl der Zustände und die der POVM-Operatoren gleich ist. Dies stellt keine Einschränkung dar, denn eine dem POVM folgende Entscheidungsstufe kann in das POVM aufgenommen werden. Die Bayes-Kosten können mit dem Risiko-Operator

$$W_k := \sum_{j=0}^{m-1} p(j) C_{k,j} \rho_j \quad \text{als} \quad \overline{C} = \mathrm{tr}\left(\sum_{k=0}^{m-1} W_k \Pi_k \right)$$

geschrieben werden (siehe Abschnitt IV.1 in [Hel76]). Das Ziel der Optimierung des POVMs ist die Minimierung der Bayes-Kosten für ein gegebenes Ensemble und eine gegebene Kostenmatrix $(C_{k,j})_{k,j}$. Ein Kriterium für die Optimalität eines POVMs kann mit Hilfe des Risiko-Operators kompakt dargestellt werden (siehe [YKL75, Hel76]):

Lemma 3.2 (Helstrom-Bedingungen) *Die Bayes-Kosten werden für ein POVM minimiert, falls*

$$(W_j - \Upsilon)\Pi_j = \Pi_j (W_j - \Upsilon) = 0 \;\; \textit{und} \;\; W_j - \Upsilon \geq 0 \tag{3.1}$$

für alle j gilt. Hierbei wird $\Upsilon := \sum_j \Pi_j W_j$ definiert, und die Ungleichung $W_j - \Upsilon \geq 0$ bedeutet, daß $W_j - \Upsilon$ semipositiv ist.

Mit Hilfe der Helstrom-Bedingungen läßt sich die Optimalität eines POVMs durch Einsetzen in Gl. (3.1) nachweisen. Die Bedingungen können durch Dualitätsargumente erhalten werden, da die Suche nach einem optimalen POVM ein lineares Optimierungsproblem ist (siehe [YKL75]). Die optimale Messung kann nur für einige einfache Probleme ohne explizite Lösung des Optimierungsproblems angegeben werden; es werden hierbei symmetrische Ensembles oder einfache Kostenmatrizen zu Grunde gelegt. Eine Lösung des Optimierungsproblems ist beispielsweise bei beliebigen Bayes-Kosten für Ensembles bekannt, die aus zwei Elementen bestehen (siehe Abschnitt IV.2 in [Hel76]). Weitere Aussagen über optimale POVMs sind bekannt, falls die Kostenmatrix so gewählt wird, daß die Bayes-Kosten der Detektionsfehlerwahrscheinlichkeit entsprechen.

3.1.2 Die Detektionsfehlerwahrscheinlichkeit

Die Detektionsfehlerwahrscheinlichkeit (DFW) bei dem Modell von Abb. 3.1 gibt an, mit welcher Wahrscheinlichkeit der Empfänger eine falsche Entscheidung trifft, d. h. das POVM des Empfängers ergibt nicht das Resultat j, falls bei der Quelle diese Nachricht ausgewählt wurde.

Definition 3.3 (DFW) *Die DFW eines POVMs mit den Operatoren Π_k für ein Ensemble mit den Zuständen ρ_j und Wahrscheinlichkeiten $p(j)$ ist durch*

$$\sum_{j,k=0}^{m-1}(1-\delta_{k,j})p(j)p(k|j) = 1 - \sum_{j=0}^{m-1} p(j)p(j|j)$$

festgelegt, wobei $p(k|j) := \mathrm{tr}(\rho_j\Pi_k)$ gilt und $\delta_{k,j}$ das Kronecker-Symbol bezeichnet.

Die DFW kann mit der Kostenmatrix $(1-\delta_{k,j})_{k,j}$ als Spezialfall der Bayes-Kosten aus Def. 3.1 erhalten werden. Zur Vereinfachung kann der Optimierung auch die Kostenmatrix $(-\delta_{k,j})_{k,j}$ zugrunde gelegt werden (siehe z. B. [BKMH97]), denn dies entspricht lediglich einer konstanten Verschiebung der Kosten für alle möglichen Messungen. Der Vorteil dieser Kostenmatrix ist, daß bei dieser alle Terme außerhalb der Diagonalen verschwinden und damit viele Rechnungen vereinfacht werden. Aufgrund der einfachen Struktur dieser Kostenmatrix können für einige symmetrische Ensembles optimale POVMs ohne explizite Lösung des Problems aus Lemma 3.2 angegeben werden. Grundlage ist hierbei das als PGM (*pretty good measurement*) bezeichnete POVM, das auch *square-root measurement* genannt wird (siehe z. B. [HW94, EF01]):

Definition 3.4 (PGM) *Es seien $\rho_j := |\Phi_j\rangle\langle\Phi_j|$ mit den Wahrscheinlichkeiten $p(j)$ die Zustände eines Ensembles mit der zugehörigen Dichtematrix $\rho := \sum_j p(j)\rho_j$. Dann ist die PGM das POVM mit den Operatoren $\Pi_j := |\Psi_j\rangle\langle\Psi_j|$, die durch*

$$|\Psi_j\rangle := \sqrt{p(j)}\rho^{-1/2}|\Phi_j\rangle$$

festgelegt sind und wobei die Inverse auf dem von den Vektoren $|\Phi_j\rangle$ aufgespannten Raum gebildet wird.

Erzeugen die Vektoren $|\Phi_j\rangle$ nicht den gesamten Raum, so definiert auch die PGM nur ein POVM auf diesem Teilraum. Durch die Ergänzung mit geeigneten Operatoren

auf dem orthogonalen Komplement kann ein POVM auf dem gesamten Raum erhalten werden. Da die ergänzten Operatoren orthogonal zu allen Zuständen sind und daher die zugehörigen Resultate nie auftreten, ist die Wahl dieser Operatoren für die Bayes-Kosten einer Messung unerheblich. Durch Nachrechnen der Helstrom-Bedingungen kann gezeigt werden, daß die PGM für einige Ensembles mit einer bestimmten Klasse von Symmetrie eine optimale Messung ist (siehe [EF01] und [BKMH97]).

Satz 3.5 (Optimalität der PGM) *Es seien $\sigma(g)|\Phi\rangle\langle\Phi|\sigma(g)^\dagger$, $g \in G$, gleichverteilte Zustände für eine Darstellung σ der endlichen Gruppe G. Dann umfaßt die PGM die Operatoren $\sigma(g)|\Psi\rangle\langle\Psi|\sigma(g)^\dagger$ für ein geeignetes $|\Psi\rangle$ und minimiert die DFW.*

Für gemischte Zustände, die eine allgemeinere Symmetrie haben, sind nur schwächere Aussagen bekannt (siehe [EMV04]):

Satz 3.6 (Optimale Messung) *Es sei ein Ensemble mit den gleichverteilten Zuständen $\sigma(g)\rho_j\sigma(g)^\dagger$, $g \in G$ und $j \in \{0, \ldots, m-1\}$, für eine Darstellung σ der Gruppe G gegeben. Dann gibt es ein POVM mit den Operatoren $\sigma(g)\Pi_j\sigma(g)^\dagger$, $g \in G$ und $j \in \{0, \ldots, m-1\}$, das die DFW minimiert.*

Die auf gemischte Zustände verallgemeinerte PGM (siehe [EMV04]) muß bei den symmetrischen Ensembles aus Satz 3.6 nicht optimal sein, d. h. die Aussage von Satz 3.5 kann nicht direkt verallgemeinert werden. Das Auffinden des optimalen POVMs kann aber dennoch durch Ausnutzung der Symmetrie vereinfacht werden (siehe [EMV04]).

3.1.3 Verborgene Untergruppen

Bei der Analyse vieler Quantenalgorithmen, z. B. dem Deutsch-Jozsa-Algorithmus (siehe Abschnitt 1.4.4 in [NC00]) oder dem Algorithmus von Shor, hat sich herausgestellt, daß sie im wesentlichen dasselbe Problem lösen. In einer gruppentheoretischen Formulierung entspricht dieses der Suche nach einer verborgenen Untergruppe (*hidden subgroup*, siehe z. B. Abschnitt 5.1 in [Röt01]):

Definition 3.7 (Verborgene Untergruppe) *Es sei $f : G \to M$ eine Funktion auf der endlichen Gruppe G in eine endliche Menge M. Gibt es eine Untergruppe H von G, so daß $f(x) = f(y)$ genau für $xH = yH$ gilt, so heißt H verborgene Untergruppe.*

Das Ziel ist das effiziente Auffinden der unbekannten Untergruppe H, falls nur Auswertungen von f zugelassen sind. Beispielsweise kann die Faktorisierung von Zahlen auf die Suche von verborgenen Untergruppen reduziert werden: Soll $N > 1$ faktorisiert werden, so wird versucht, eine Lösung von $x^2 \equiv 1 \bmod N$ zu bestimmen, denn diese Kongruenz hat zur Folge, daß N das Produkt $(x-1)(x+1)$ teilt. Damit wird für nicht-verschwindende $(x-1) \bmod N$ und $(x+1) \bmod N$ ein Faktor von N gefunden. Eine Lösung dieser Kongruenz kann in vielen Fällen durch die Bestimmung der Ordnung eines zufällig gewählten Elements erhalten werden: Hat x modulo N die Ordnung r, d. h. es gilt $x^r \equiv 1 \bmod N$ und r ist minimal mit dieser Eigenschaft, so ergeben für gerade r die Zahlen

$$\mathrm{ggT}(x^{r/2} - 1, N) \quad \text{und} \quad \mathrm{ggT}(x^{r/2} + 1, N)$$

in ausreichend vielen Fällen einen Faktor von N, um ein effizientes Faktorisierungsverfahren zu erhalten, falls die Ermittlung der Ordnung selbst effizient ist (siehe Abschnitt 5.3.2 in [NC00]). Diese Bestimmung kann mit der Funktion

$$f(a) := x^a \bmod N$$

als Suche nach einer verborgenen Untergruppe formuliert werden; die verborgene Untergruppe ist hierbei die von r erzeugte zyklische Gruppe.

Die verborgenen Untergruppen von *abelschen* Gruppen können mit Quantenalgorithmen effizient gefunden werden (siehe Abschnitt 3.5 in [Lom04] und Abschnitt 5.4.3 in [NC00]). Darüber hinaus sind nur für wenige nicht-abelsche Gruppen effiziente Verfahren bekannt, beispielsweise für bestimmte Kranzprodukte (siehe [RB98]). Prinzipiell besteht aber die Möglichkeit, daß sich verborgene Untergruppen beliebiger Gruppen effizient mit Quantenalgorithmen bestimmen lassen (siehe [EHK99]). Hierbei wird angenommen, daß sowohl die Elemente von G als auch die von M mit $O(\log|G|)$ vielen Qubits repräsentiert werden können. Ferner steht f als Quantengatter zur Verfügung, das eine unitäre Transformation U_f mit

$$U_f : |g\rangle \otimes |0\rangle \mapsto |g\rangle \otimes |f(g)\rangle$$

implementiert. Durch Überlagerung aller $|g\rangle$ wird der durch

$$\sqrt{\frac{1}{|G|}} \sum_{g\in G} |g\rangle \otimes |0\rangle \mapsto \sqrt{\frac{1}{|G|}} \sum_{g\in G} |g\rangle \otimes |f(g)\rangle$$

beschriebene Zustandsübergang erhalten (siehe [BCv05]). Durch anschließende Messung der zweiten Komponenten wird ein Nebenklassenzustand erhalten:

Definition 3.8 (Nebenklassenzustand) *Es seien $H \leq G$ und $g \in G$. Dann ist $|gH\rangle\langle gH|$ ein Nebenklassenzustand für*

$$|gH\rangle := \sqrt{\frac{1}{|H|}} \sum_{h\in H} |gh\rangle \,.$$

In [EHK99] wird nachgewiesen, daß im Prinzip polynomial viele Auswertungen von f genügen, um verborgene Untergruppen zu identifizieren. Grundlegende Beobachtung ist hierfür, daß Tensorprodukte von $O(\log(|G|))$ vielen Nebenklassenzuständen verschiedener Untergruppen einen exponentiell kleinen Skalarproduktbetrag haben, d. h. sie sind fast orthogonal. Damit ist es möglich, durch eine Unterscheidung dieser Zustände die verborgene Untergruppe zu identifizieren. Unbekannt ist dabei, wie die Unterscheidung der Zustände realisiert werden kann und wie die bei der Messung erhaltene Information effizient zur Lösung führt. Bei den Diedergruppen kann beispielsweise mit Hilfe der Helstrom-Bedingungen (siehe Lemma 3.2) über dieses Resultat hinaus gezeigt werden, daß die PGM aus Def. 3.4 die optimale Messung zur Unterscheidung der Zustände ist (siehe [BCv05]). Ungelöst ist hierbei jedoch die effiziente Durchführung dieses POVMs, denn das in [BCv05] vorgeschlagene Verfahren zur Messung beruht auf der Lösung spezieller Instanzen eines Problems, das NP-vollständig ist (*subset sum problem*, siehe Abschnitt A3.2 in [GJ79]). Damit führt dieser Vorschlag nicht unmittelbar zu einem effizienten Verfahren zur Bestimmung verborgener Untergruppen von Diedergruppen.

3.2 Die Transinformation eines POVMs

Bei dem Kommunikationsmodell von Abb. 3.1 gibt der Übertragungskanal die Zustände ρ_j aus, während die zugehörigen Eingaben j nicht quantenmechanisch beschrieben werden. Dieses Modell trifft beispielsweise zu, falls bei der Kommunikation kohärente Zustände (siehe Def. 4.30) genutzt werden und diese bei der Übertragung durch eine Faser so stark abgeschwächt werden, daß eine quantenmechanische Beschreibung notwendig wird (siehe z. B. [TFMS04]). In der Quantenkryptographie werden hingegen solche Kanäle mit der Absicht genutzt, daß Messungen eines Angreifers der Kommunikation die Zustände ρ_j stören und daher detektiert werden können. Um die Leistungsfähigkeit eines solchen Kanals für die Kommunikation zu bewerten, wird die Transinformation als grundlegendes Maß herangezogen (*mutual information*, siehe z. B. [CT91]).

Definition 3.9 (Transinformation) *Es sei P ein POVM mit den n Operatoren Π_j und S ein Ensemble mit den m Zuständen ρ_j, die jeweils mit der Wahrscheinlichkeit $p(j)$ auftreten. Ferner bezeichne*

$$p(j,k) := p(j)p(k|j) \quad mit \quad p(k|j) := \mathrm{tr}(\rho_j \Pi_k)$$

die gemeinsame Verteilung der Zustände und der Resultate. Dann ist

$$I(S,P) := \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} H(p(j,k)) - \sum_{k=0}^{n-1} H\left(\sum_{j=0}^{m-1} p(j,k) \right) - \sum_{j=0}^{m-1} H\left(p(j)\right) \tag{3.2}$$

mit $H(u) := u \log_2 u$ die Transinformation von S und P.

Die Transinformation gibt an, wieviel Information durch den Kanal übertragen werden kann, falls die Signale j gemäß der Verteilung $p(j)$ in den Kanal eingegeben werden und die Zustände ρ_j, die den Kanal verlassen, mit dem POVM P gemessen werden. Liegt das Ensemble der Kanalausgabe fest, so kann die maximal erhältliche Information durch die Holevo-Schranke (siehe Abschnitt 12.1.1 in [NC00]) abgeschätzt werden:

Lemma 3.10 (Holevo-Schranke) *Es sei P ein POVM und S ein Ensemble mit den Zuständen ρ_j, die jeweils mit Wahrscheinlichkeit $p(j)$ auftreten. Dann gilt*

$$I(S,P) \leq \chi \quad mit \quad \chi := \mathcal{S}\left(\sum_j p(j)\rho_j \right) - \sum_{j=0}^{m-1} p(j)\mathcal{S}(\rho_j)\,,$$

wobei $\mathcal{S}(\rho) := -\mathrm{tr}(\rho \log_2(\rho))$ die Von-Neumann-Entropie des Zustands ρ bezeichnet.

Die Gleichheit der Holevo-Schranke kann genau bei den Ensembles erhalten werden, deren Dichtematrizen kommutieren (siehe [Hol73]). Für alle anderen Ensembles muß die maximal erreichbare Information (*accessible information*, siehe [HJS$^+$96]) durch Optimierung der POVMs bestimmt werden:

Definition 3.11 (Erreichbare Information) *Für ein gegebenes Ensemble S ist die erreichbare Information das Maximum von $I(S,P)$ für alle POVMs P.*

Die erreichbare Information und die zugehörigen optimalen POVMs sind nur für einige einfache Ensembles bekannt (siehe [SBJ+99, Dav78, BYH97]). Beispielsweise kann für die Drillinge gezeigt werden, daß die erreichbare Information deutlich unterhalb von χ liegt:

Beispiel 3.12 (Drillinge) *Die Drillinge sind die Zustände $|\Phi_j\rangle\langle\Phi_j|$ für*

$$|\Phi_0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |\Phi_1\rangle := \frac{1}{2}\begin{pmatrix} -1 \\ -\sqrt{3} \end{pmatrix} \quad \textit{und} \quad |\Phi_2\rangle := \frac{1}{2}\begin{pmatrix} -1 \\ \sqrt{3} \end{pmatrix},$$

die jeweils mit der Wahrscheinlichkeit $1/3$ vorliegen.

Bei den Drillingen folgt $\log_2(3) - 1 \approx 0,585$ bit als erreichbare Information (siehe [SBJ+99]), wohingegen $\chi = 1$ bit gilt. Die Nutzung des Kanals kann verbessert werden, indem neben den POVMs auch die Verteilung $p(j)$ optimiert wird: Bei den Drillingen ist eine optimale Verteilung beispielsweise gegeben, wenn zwei der Drillinge jeweils mit Wahrscheinlichkeit $1/2$ auftreten und der dritte Zustand weggelassen wird, womit

$$I(S,P) = 1 + H\left(\frac{2-\sqrt{3}}{4}\right) + H\left(\frac{2+\sqrt{3}}{4}\right) \approx 0.645 \text{ bit}$$

erreicht werden mit einem geeignet konstruierten POVM (siehe [Sho04, BYH97]). Die erreichbare Information gibt die pro Kanalnutzung übertragbare Information nur dann an, falls die Kanalnutzungen voneinander unabhängig sind. Wird bei den Eingaben hingegen eine geeignete Codierung genutzt, so kann die pro Kanalnutzung übertragene Information erhöht werden (siehe [HJS+96]): Es werden hierzu n Nutzungen des Kanals zu Blöcken gebündelt, d. h. es wird der Kanal betrachtet, der bei Eingabe des Blocks $(j_0, \ldots, j_{n-1})$ den Zustand $\rho_0 \otimes \ldots \otimes \rho_{n-1}$ ausgibt. Durch Optimierung der POVMs und der Wahrscheinlichkeiten zum Senden der Blöcke wird die Kapazität des Kanals erreicht (siehe [Hol98]):

Definition 3.13 (Kanalkapazität) *Die C_n-Kapazität eines Kanals ist*

$$C_n := \sup_{p,P} I(S^p, P)\,,$$

wobei S^p das Ensemble bezeichnet, das durch die Verteilung p der Eingabeblöcke der Länge n festgelegt wird, und P die POVMs auf den Ausgabeblöcken. Die Kapazität eines Kanals ist $C := \lim_{n\to\infty} C_n/n$.

Bei der Optimierung von $I(S,P)$ werden alle POVMs für die Zustände $\rho_0 \otimes \ldots \otimes \rho_{n-1}$ untersucht, d. h. die POVM-Operatoren müssen nicht die Tensorzerlegung der Zustände haben. Dies ermöglicht, daß durch die Codierung die Information $C_n/n > C_1$ pro Nutzung des Kanals erreicht wird. Liegt dieser Fall vor, so ist der Kanal *superadditiv* (siehe [Hol98]).

Beispiel 3.14 (Superadditiver Kanal) *Es seien zwei Zustände $|a\rangle\langle a|$ und $|b\rangle\langle b|$ mit $\kappa := \langle a|b\rangle \in \mathbb{R}$ gegeben. Die Kapazität C_1 ist durch*

$$C_1 = 1 + H(p) + H(1-p) \quad \textit{mit} \quad p := \frac{1-\sqrt{1-\kappa^2}}{2}$$

gegeben (siehe [SKIH97]). Werden die vier durch

$$|a\rangle \otimes |a\rangle \otimes |a\rangle,\ |a\rangle \otimes |b\rangle \otimes |b\rangle,\ |b\rangle \otimes |b\rangle \otimes |a\rangle \text{ und } |b\rangle \otimes |a\rangle \otimes |b\rangle$$

gegebenen Zustände mit Gleichverteilung betrachtet, so kann im Bereich $0,74 < \kappa < 1$ mit der PGM die Superadditivität $C_3 > 3C_1$ nachgewiesen werden (siehe [SKIH97]).

Die Superadditivität zeigt, daß prinzipiell die Möglichkeit besteht, daß bei einer Kanalnutzung die Kapazität C_1 übertroffen wird. Durch eine Variante des Kanalcodierungstheorems (siehe [Sha48]) kann sogar gezeigt werden, daß die Holevo-Schranke erreicht werden kann (siehe [HJS$^+$96, Hol98]):

Satz 3.15 (Kanalcodierungstheorem) *Es gilt* $C = \max_p \chi$.

Der Beweis des Kanalcodierungstheorems beruht auf der Mittelung zufällig gewählter Codes (siehe [HJS$^+$96]) und bietet daher nur eine Existenzaussage, aber keine Konstruktionsverfahren für geeignete Codes. Ebenso wie Konstruktionen fehlerkorrigierender Codes gesucht werden (siehe z. B. [MS83]), müssen brauchbare Codierungsschemata konstruiert werden. Dabei stellt sich insbesondere die Frage, wie die übertragenen Codewörter gemessen werden. Die im Beweis des Kanalcodierungstheorems genutzte PGM ist nämlich nur asymptotisch optimal (siehe [HJS$^+$96]), d. h. mit dieser Messung wird die Holevo-Schranke im Grenzfall erreicht. Ist hingegen eine Codierung mit einer endlichen Länge gegeben, so muß die PGM nicht die erreichbare Information liefern. Dies ist beispielsweise bei den Drillingen der Fall, bei denen mit der PGM nur 1/3 bit erhalten wird, wohingegen die erreichbare Information ca. $0,585$ bit beträgt. Dies zeigt, daß es für die Kommunikation nach dem Modell von Abb. 3.1 ein grundlegendes Problem ist, POVMs zu bestimmen, die bezüglich der Transinformation optimal sind.

3.3 Eigenschaften der Transinformation

Ein optimales POVM kann durch Ausnutzung elementarer Eigenschaften der Transinformation in ein anderes umgewandelt werden, das ebenfalls optimal ist und zusätzliche Eigenschaften hat; beispielsweise können POVMs konstruiert werden, die aus einer beschränkten Anzahl von Operatoren bestehen. Diese Konstruktionen ermöglichen es, bei der Suche nach optimalen POVMs den Suchraum erheblich einzuschränken.

Die wichtigste Eigenschaft der Transinformation, die für diese Konstruktionen genutzt wird, ist ihre Konvexität: Mit der Notation von Def. 3.9 ist bei gegebener Verteilung $p(j)$ die Transinformation in der bedingten Wahrscheinlichkeit $p(k|j)$ eine konvexe Funktion (siehe Th. 2.7.4 in [CT91]). Werden also mit den bedingten Wahrscheinlichkeiten $p_0(k|j)$ und $p_1(k|j)$ die gemeinsamen Verteilungen

$$p_0(j,k) := p(j)p_0(k|j) \quad \text{und} \quad p_1(j,k) := p(j)p_1(k|j)$$

gebildet, so ist für $\lambda \in [0,1]$ die nach Gl. (3.2) definierte Transinformation für die gemeinsame Wahrscheinlichkeitsverteilung

$$\lambda p_0(j,k) + (1-\lambda)p_1(j,k)$$

höchstens so groß wie die Konvexkombination $\lambda I_0 + (1-\lambda)I_1$ der jeweils zu $p_0(j,k)$ und $p_1(j,k)$ gehörenden Transinformationen I_0 und I_1. Diese Konvexität überträgt sich auf POVMs, wobei die Konvexkombination zweier POVMs der zufälligen Wahl zwischen zwei Meßgeräten mit denselben Resultatsmengen entspricht, wobei nicht gespeichert wird, welches Meßgerät genutzt wurde.

Lemma 3.16 (Konvexität der Transinformation) *Es seien S ein Ensemble und P sowie $\tilde{P}$ POVMs mit den Operatoren Π_j bzw. $\tilde{\Pi}_j$ für $j \in \{0, \ldots, n-1\}$. Für das POVM Q mit den Operatoren $\lambda\Pi_j + (1-\lambda)\tilde{\Pi}_j$ für $\lambda \in [0,1]$ gilt die Ungleichung*

$$I(S,Q) \leq \lambda I(S,P) + (1-\lambda) I(S,\tilde{P}).$$

Die Gleichheit gilt genau dann, wenn

$$p(j,k) \sum_{\ell=0}^{m-1} \tilde{p}(\ell,k) = \tilde{p}(j,k) \sum_{\ell=0}^{m-1} p(\ell,k) \tag{3.3}$$

für alle j und k ist, wobei $\tilde{p}(k|\ell) := \mathrm{tr}(\rho_\ell \tilde{\Pi}_k)$ und $\tilde{p}(\ell,k) := p(\ell)\tilde{p}(k|\ell)$ gelten.

Die Gleichheitsbedingung in Lemma 3.16 ist genau für die POVMs erfüllt, bei denen die beiden Vektoren

$$(p(0,k), \ldots, p(m-1,k)) \text{ und } (\tilde{p}(0,k), \ldots, \tilde{p}(m-1,k)), \tag{3.4}$$

die durch Π_k bzw. $\tilde{\Pi}_k$ für das gegebene Ensemble definiert werden, bis auf einen konstanten Faktor gleich sind:

$$c_k(p(0,k), \ldots, p(m-1,k)) = d_k(\tilde{p}(0,k), \ldots, \tilde{p}(m-1,k)) \tag{3.5}$$

mit $c_k, d_k \geq 0$ und $c_k + d_k > 0$ für jedes k. Dies entspricht bei der Konvexkombination $\lambda\Pi_k + (1-\lambda)\tilde{\Pi}_k$ zwei Operatoren Π_k und $\tilde{\Pi}_k$, die für alle Zustände des Ensembles bis auf einen konstanten Faktor dieselben Wahrscheinlichkeiten liefern, d. h. beide POVMs sind für das gegebene Ensemble bis auf einen skalaren Faktor gleich.

Die Konvexkombination von POVMs in Lemma 3.16 weicht von der Definition von $\lambda P + (1-\lambda)\tilde{P}$ nach Def. 1.30 ab, denn die Operatoren beider POVMs werden nicht vereinigt, sondern elementweise addiert. Die Konvexkombination $\lambda P + (1-\lambda)\tilde{P}$ kann mit dieser elementweisen Addition durch folgende Konstruktion erhalten werden: Die POVMs P und $\tilde{P}$ werden von links bzw. rechts her mit Nulloperatoren ergänzt, so daß $\lambda\Pi_k + (1-\lambda)\tilde{\Pi}_k$ immer den Nulloperator $\Pi_k = 0$ bzw. $\tilde{\Pi}_k = 0$ umfaßt. Dies entspricht der Auswahl zwischen POVMs, die disjunkte Mengen von Resultaten haben. Bei solchen POVMs folgt

$$\sum_{\ell=0}^{m-1} p(\ell,k) = 0 \quad \text{oder} \quad \sum_{\ell=0}^{m-1} \tilde{p}(\ell,k) = 0$$

für alle k, d. h. es gilt $c_k = 0$ oder $d_k = 0$ in Gl. (3.5). Dies bedeutet, daß die Information, die durch die Konvexkombination zweier POVMs erhalten wird, die Konvexkombination der entsprechenden Informationen ist:

Lemma 3.17 (Konvexität der Transinformation) *Es sei S ein Ensemble. Ferner seien P und $\tilde{P}$ zwei POVMs. Dann gilt für alle $\lambda \in [0,1]$ die Gleichung*

$$I(S, \lambda P + (1-\lambda)\tilde{P}) = \lambda I(S,P) + (1-\lambda) I(S,\tilde{P}).$$

In Lemma 3.16 folgt bei der Konvexkombination $\lambda\Pi_k + (1-\lambda)\tilde{\Pi}_k$ von Operatoren die Gleichheit insbesondere dann, falls sich Π_k und $\tilde{\Pi}_k$ nur um skalare Vielfache unterscheiden: Die Wahrscheinlichkeitsvektoren (3.4) sind für *alle* Ensembles bis auf einen konstanten Faktor gleich und nicht nur für das gegebene Ensemble. Diese Gleichheit wird auch erhalten, falls Operatoren eines POVMs, die bis auf skalare Faktoren gleich sind, zusammengefaßt werden (siehe Lemma 2 [Dav78]):

Lemma 3.18 (Aufspaltung von Operatoren) *Es bezeichne S ein Ensemble und P ein POVM mit den Operatoren Π_j. Ferner sei $\tilde{P}$ das POVM, das entsteht, wenn ein Π_j aus P entfernt wird und durch $\lambda\Pi_j$ sowie $(1-\lambda)\Pi_j$ ersetzt wird für $\lambda \in [0,1]$. Dann gilt $I(S,P) = I(S,\tilde{P})$.*

Neben der Konvexkombination von POVMs und der Zusammenfassung von POVM-Operatoren kann eine weitere Vereinfachung der Suche nach optimalen POVMs durch das Umformen von $\sum_{j=0}^{n-1} \Pi_j = I_d$ erhalten werden: Diese Summe geht durch Umnormieren der Π_j in eine konvexe Zerlegung der Matrix I_d über (siehe [Dav78]). Damit können für POVMs Argumente für konvexe Mengen, beispielsweise Carathéodorys Theorem (siehe [Grü67] und [Alf71]), angewandt werden.

Definition 3.19 (POVM als Konvexkombination) *Es sei P ein POVM mit den Operatoren Π_j, wobei kein Π_j dem Nulloperator gleiche. Dann kann $\Pi_j = \lambda_j \Pi'_j$ mit*

$$\lambda_j := \frac{\mathrm{tr}(\Pi_j)}{d} \quad \textit{und} \quad \Pi'_j := \frac{d}{\mathrm{tr}(\Pi_j)}\Pi_j$$

geschrieben werden. Die Identität ist damit die Konvexkombination $\sum_{j=0}^{n-1} \lambda_j \Pi'_j = I_d$.

Das letzte Lemma, das für die Untersuchungen in Abschnitt 3.4 benötigt wird, ist eine Erweiterung von Def. 2.17 für symmetrische Ensembles: Liegt bei einem symmetrischen Ensemble ein optimales POVM vor, so kann dieses nach Def. 2.17 zu einem symmetrischen POVM erweitert werden. Hierbei bleibt die Transinformation und damit auch die Optimalität erhalten (siehe [Dav78]).

Lemma 3.20 (Symmetrisierung eines POVMs) *Es sei S ein symmetrisches Ensemble mit der Symmetriegruppe G und P ein POVM. Dann gilt $I(S,P) = I(S,P^G)$.*

Beweis: Werden alle Operatoren von P jeweils mit $\sigma(g)$ konjugiert, so wird das POVM $\sigma(g)P\sigma(g)^\dagger$ mit den Operatoren $\sigma(g)\Pi_k\sigma(g)^\dagger$ erhalten, bei dem die Wahrscheinlichkeiten

$$\mathrm{tr}(\rho_j(\sigma(g)\Pi_k\sigma(g)^\dagger)) = \mathrm{tr}((\sigma(g)^\dagger\rho_j\sigma(g))\Pi_k) = \mathrm{tr}(\rho_{\pi(g^{-1})(j)}\Pi_k)$$

auftreten. Da dies nur einer Umordnung der Zustände ρ_j entspricht, gilt die Gleichung $I(S,P) = I(S,\sigma(g)P\sigma(g)^\dagger)$. Da das POVM P^G die konvexe Kombination

$$P^G = \sum_{g\in G} \lambda_g \sigma(g)\Pi\sigma(g)^\dagger \quad \text{mit} \quad \lambda_g := \frac{1}{|G|}$$

ist, folgt die Aussage mit Lemma 3.17. □

Das Lemma besagt, daß für ein symmetrisches Ensemble immer ein optimales symmetrisches POVM existiert. Da hierbei für jeden Operator von P die gesamte Bahn unter der Gruppe gebildet wird, kann P^G sehr viele Operatoren umfassen. Durch die Ausnutzung der Konvexität der Menge der POVMs kann eine Schranke für die Anzahl dieser Bahnen abgeleitet werden.

3.4 Konvexität und optimale Messungen

Die bedeutendsten Hilfsmittel zur Optimierung von POVMs bzgl. der Transinformation für ein gegebenes Ensemble sind die beiden Theoreme von Davies (siehe [Dav78]): Das erste Theorem ermöglicht eine Beschränkung der Anzahl der Operatoren, die in Abhängigkeit von der Dimension des Hilbert-Raums für ein optimales POVM benötigt werden. Das zweite Theorem kann für symmetrische Ensembles mit irreduzibler Darstellung der Symmetriegruppe angewandt werden und garantiert die Existenz eines optimalen POVMs, das bzgl. der Symmetrie genau eine Bahn umfaßt. Mit diesen beiden Theoremen kann die Suche nach optimalen POVMs in einigen Fällen sehr stark vereinfacht werden (siehe z.B. [SBJ$^+$99]). In diesem Abschnitt werden die Beweise beider Theoreme zusammenfassend dargestellt, wobei gleichzeitig das zweite Theorem auf reduzible Darstellungen verallgemeinert wird.

Die Beweise der Davies-Theoreme beruhen im wesentlichen auf dem folgenden Lemma (siehe [Dav78]), das eine Zerlegung von Konvexkombinationen der Einheitsmatrix in andere Konvexkombinationen ermöglicht. Die Menge dieser Konvexkombinationen ist selbst konvex und das Lemma gibt eine obere Schranke für die Anzahl der Operatoren eines Randpunktes dieser Menge. Ein Beweis des Lemmas, der auf Carathéodorys Theorem beruht, kann im Anhang von [Dec05] gefunden werden.

Lemma 3.21 (Zerlegung in Konvexkombinationen) *Es sei $\sum_{j=0}^{n-1} \lambda_j \Pi'_j = I_d$ eine Konvexkombination mit $\mathrm{tr}(\Pi'_j) = d$. Ferner seien alle Π'_j Elemente des affinen Raums $I_d + K$, wobei K ein $\mathbb{R}$-linearer Teilraum des Raums der hermiteschen Matrizen sei, der die Dimension r habe. Dann kann die Konvexkombination umgeschrieben werden in*

$$\sum_{j=0}^{n-1} \lambda_j \Pi'_j = \sum_j \mu_j \left(\sum_{k=0}^{n-1} \nu_{j,k} \Pi'_k \right) \quad \textit{mit} \quad \sum_{k=0}^{n-1} \nu_{j,k} \Pi'_k = I_d \,,$$

wobei $\mu_j, \nu_{j,k} \geq 0$ und

$$\sum_j \mu_j = \sum_{k=0}^{n-1} \nu_{j,k} = 1 \quad \textit{sowie} \quad \sum_j \mu_j \nu_{j,k} = \lambda_k$$

für alle j gelten. Ferner sind für alle j höchstens $r+1$ Elemente $\nu_{j,k}$ ungleich null.

Aus diesem Lemma folgen unmittelbar beide Theoreme von Davies:

Satz 3.22 (Erstes Theorem von Davies) *Es sei S ein Ensemble mit Zuständen eines d-dimensionalen Raums. Dann existiert ein optimales POVM mit n Operatoren vom Rang eins, wobei $d \leq n \leq d^2$ gilt.*

Beweis (siehe [Dav78]): Es seien $\Pi_0, \ldots, \Pi_{n-1}$ die Operatoren eines optimalen POVMs. Es kann angenommen werden, daß alle Operatoren vom Rang eins sind (siehe [Dav78]). Mit der Normierung von Def. 3.19 folgt die Konvexkombination $\sum_{j=0}^{n-1} \lambda_j \Pi'_j = I_d$. Mit Lemma 3.21 ist das POVM eine Konvexkombination von POVMs mit jeweils höchstens d^2 Operatoren, da K die Dimension[1] $d^2 - 1$ hat. Lemma 3.17 und 3.18 zeigen zusammen, daß mindestens eines dieser POVMs ebenfalls optimal ist. □

[1] Der Raum K ist der gesamte Raum der hermiteschen Matrizen bis auf die Spurnormierung. Diese Normierung verringert die Dimension d^2 um eins, d. h. es gilt $r = d^2 - 1$ in Lemma 3.21.

Auch das zweite Theorem von Davies (Th. 4 in [Dav78]) folgt aus Lemma 3.21:

Satz 3.23 (Zweites Theorem von Davies) *Es sei S ein symmetrisches Ensemble mit irreduzibler Darstellung σ der Symmetriegruppe G. Dann existiert ein optimales POVM mit Operatoren vom Rang eins, das eine einzelne Bahn unter der Operation von G ist.*

Beweis (siehe [Dav78]): Es sei P ein optimales POVM mit den Operatoren Π_j vom Rang eins. Ferner bezeichne O_j die Bahn mit den Operatoren

$$\frac{d}{|G|\mathrm{tr}(\Pi_j)}\sigma(g)\Pi_j\sigma(g)^\dagger$$

für $g \in G$. Es folgt nach Def. 1.30 die Konvexkombination

$$P^G = \sum_j \lambda_j O_j \quad \text{mit} \quad \lambda_j := \frac{\mathrm{tr}(\Pi_j)}{d}$$

wie in Def. 3.19 für das symmetrisierte POVM P^G, das nach Lemma 3.20 ebenfalls optimal ist. Es bezeichne

$$D_j := \sum_{g\in G} \frac{d}{|G|\mathrm{tr}(\Pi_j)}\sigma(g)\Pi_j\sigma(g)^\dagger$$

die Summe der Operatoren der Bahn von Π_j. Da P^G ein POVM ist, gilt die Gleichung $\sum_j \lambda_j D_j = I_d$, d. h. die Identitätsmatrix ist eine Konvexkombination der Matrizen D_j. Mit der Irreduzibilität von σ und mit der Symmetrie $\sigma D_j = D_j\sigma$ folgt $D_j = \alpha_j I_d$ für alle j, denn die Matrizen D_j sind nach Lemma 2.22 Elemente des Verkettungsraums $\mathrm{Int}(\sigma,\sigma) = \mathbb{C}I_d$. Da die Matrizen D_j darüber hinaus die Spur d haben, liegen sie im Teilraum $I_d + \{0\}$ von $\mathrm{Int}(\sigma,\sigma)$, d. h. es gilt $D_j = I_d$. Nach Lemma 3.21 gibt es eine Konvexkombination von I_d mit einem einzigen D_j. Mit Lemma 3.17 und 3.18 folgt, daß eine einzelne Bahn für eine optimale Messung genügt. □

Der Beweis des zweiten Satzes kann auf reduzible Darstellungen σ verallgemeinert werden: Die Matrizen D_j sind Elemente des Verkettungsraums $\mathrm{Int}(\sigma,\sigma)$, der nach Lemma 2.25 die Dimension $r := \sum_{j=0}^{z-1} m_j^2$ hat. Die Spurnormierung $\mathrm{tr}(D_j) = d$ reduziert diese Dimension um eins. Dann folgt mit Lemma 3.21, daß höchstens r Bahnen benötigt werden, um die Identität zu kombinieren:

Satz 3.24 (Anzahl der Bahnen bei optimalen POVMs) *Es sei S ein symmetrisches Ensemble mit σ wie in Gl. (2.6). Dann gibt es ein optimales POVM mit Operatoren vom Rang eins, das die Vereinigung von höchstens $\sum_{j=0}^{z-1} m_j^2$ Bahnen ist.*

Die Anwendung von Satz 3.24 ist auch möglich, falls die Symmetrie auf eine Untergruppe eingeschränkt wird, denn die Symmetriegruppe muß nicht transitiv auf dem Ensemble und dem POVM operieren. Durch diese Einschränkung wird die Schranke jedoch schwächer: Die Anzahl der verschiedenen irreduziblen Darstellungen einer Untergruppe kann nicht größer als die der ganzen Gruppe sein und damit werden die Multiplizitäten beim Übergang auf die Untergruppe nicht kleiner. Als Grenzfall[2] kann der Satz auf eine

[2]Da jede Bahn unter dieser Symmetrie jeweils nur ein Element umfaßt, können die Wahrscheinlichkeiten der Zustände wie in Satz 3.22 beliebig sein.

Darstellung der trivialen Gruppe $G := \{e\}$ angewandt werden: Dabei wird die Multiplizität d der einzigen irreduziblen Darstellung $e \mapsto (1) \in \mathcal{U}(1)$ erhalten, womit Satz 3.24 die obere Schranke d^2 ergibt. Demnach wird das erste Theorem von Davies als Spezialfall von Satz 3.24 erhalten. Eine weitere Möglichkeit, die Schranke von Satz 3.24 zu erhalten, besteht in der Charakterisierung der Randpunkte der konvexen Menge der POVMs, die eine gegebene Symmetrie haben (siehe [CD06]).

3.5 Optimale Messungen reeller Zustandsmengen

Sind alle Einträge der Dichtematrizen eines Ensembles reell, so kann beim ersten Theorem von Davies eine kleinere obere Schranke für die Anzahl der Operatoren erhalten werden, die ein optimales POVM benötigt (siehe [SBJ$^+$99]). Sind darüber hinaus bei einem symmetrischen Ensemble auch die Matrizen der zugehörigen Darstellung reell, so kann die Forderung der Irreduzibilität im zweiten Theorem von Davies abgeschwächt werden. Sowohl die Verkleinerung der Schranke als auch die Abschwächung der Irreduzibilität können auf Satz 3.24 übertragen werden. Dafür werden zunächst die in den Abschnitten 2.1 und 2.4 zusammengefaßten Definitionen und Eigenschaften von Darstellungen und Matrizen auf den reellen Fall übertragen. Bei den folgenden Untersuchungen kann der Eigenschaft eines Zustands, nur reelle Einträge zu haben, nicht unmittelbar eine physikalische Systemeigenschaft zugeordnet werden, denn die Einträge der Dichtematrizen sind von der gewählten Basis des Hilbert-Raums abhängig. Dahingegen könnte es durchaus eine physikalische Bedeutung haben, falls für einen Zustand eine Basis existiert, bezüglich deren die Dichtematrix nur reelle Einträge umfaßt.

3.5.1 Verkettungsraum reeller Darstellungen

Reelle Darstellungen sind Darstellungen, bei denen einer Gruppe nur Matrizen zugeordnet werden, deren Einträge alle reell sind. Es werden im folgenden nur unitäre reelle Darstellungen betrachtet, d. h. es gilt $\sigma(g) \in \mathcal{O}(d)$ für alle $g \in G$, wobei $\mathcal{O}(d)$ die Gruppe der orthogonalen Matrizen der Größe $d \times d$ bezeichnet (siehe §3.5 in Kap. I von [Hei90]). Für die Definition der Äquivalenz von reellen Darstellungen werden ebenfalls nur reelle Matrizen für die Konjugation einer Darstellung zugelassen:

Lemma 3.25 (Reelle Äquivalenz) *Zwei reelle Darstellungen σ und τ vom Grad d sind reell äquivalent, falls eine Matrix $A \in \mathbb{R}^{d\times d}$ mit $A\sigma(g)A^{-1} = \tau(g)$ für alle $g \in G$ existiert.*

Die Irreduzibilität einer reellen Darstellung wird nur über reellen Räumen definiert (siehe Def. 10.2 in [CR62]), womit die Forderungen bei reeller Irreduzibilität schwächer sind als diejenigen bei komplexer Irreduzibilität, d. h. eine reell irreduzible Darstellung muß nicht über den komplexen Zahlen irreduzibel sein.

Definition 3.26 (Reelle Irreduzibilität) *Eine Darstellung $\sigma : G \to \mathcal{O}(d)$ ist reell irreduzibel, falls für $\mathcal{H} \leq \mathbb{R}^d$ mit $\sigma(g)\mathcal{H} \subseteq \mathcal{H}$, $g \in G$, entweder die Gleichung $\mathcal{H} = \{0\}$ oder $\mathcal{H} = \mathbb{R}^d$ folgt.*

Wie im komplexen Fall kann jede Darstellung durch einen Basiswechsel in irreduzible Komponenten zerlegt werden.

Lemma 3.27 (Zerlegung in irreduzible Komponenten) *Es sei $\sigma : G \to \mathcal{O}(d)$ eine Darstellung. Dann existiert ein $A \in \mathcal{O}(d)$ mit*

$$A\sigma A^\dagger = \kappa_0 \oplus \ldots \oplus \kappa_{n-1}\,,$$

wobei alle κ_j orthogonal und reell irreduzibel sind.

Beweis: Der Satz von Maschke (siehe Th. 10.8 in [CR62]) garantiert, daß σ in irreduzible Komponenten zerlegt werden kann. Die Zerlegung kann wie im Beweis von Lemma 2.4 gefunden werden. Die orthonormalen Basen führen hierbei zu orthogonalen Matrizen, da alle Vektoren reell sind. □

Bei komplexen Darstellungen kann gemäß Lemma 2.6 die Äquivalenz von Darstellungen nicht nur über invertierbare, sondern auch über unitäre Matrizen definiert werden. Eine ähnliche Aussage folgt auch mit orthogonalen Matrizen bei reellen Darstellungen:

Lemma 3.28 (Äquivalenz mit orthogonalem Basiswechsel) *Es seien σ und τ zwei unitäre reelle Darstellungen vom Grad d derselben Gruppe. Die Darstellungen σ und τ sind genau dann reell äquivalent, falls ein $A \in \mathcal{O}(d)$ mit $A\sigma A^\dagger = \tau$ existiert.*

Beweis: Es seien σ und τ reell äquivalent. Dann können σ und τ nach Lemma 3.27 in gleich lange direkte Summen reell irreduzibler Darstellungen κ_j bzw. $\tilde{\kappa}_j$ zerlegt werden, wobei $\kappa_j \cong \tilde{\kappa}_j$ gilt. Dies folgt, da reell irreduzible Darstellungen, die reell inäquivalent sind, über den komplexen Zahlen auch in nicht äquivalente Darstellungen zerfallen (siehe §13.2 in [Ser77]). Durch Lemma 33.1 in [Dor71] folgt, daß die Äquivalenz durch orthogonale Matrizen erreicht werden kann. □

Das Schursche Lemma kann auch für reelle Darstellungen betrachtet werden (siehe Beweis von Prop. 4 von §2.2 in [Ser77]).

Lemma 3.29 (Reelles Schur-Lemma) *Es seien $\sigma : G \to \mathcal{O}(m)$ und $\tau : G \to \mathcal{O}(n)$ zwei reell irreduzible Darstellungen und $M \in \mathbb{R}^{m\times n}$ mit $\sigma M = M\tau$. Dann gilt $M = 0$, falls σ und τ nicht reell äquivalent sind. Sind σ und τ gleich und hat M einen reellen Eigenwert λ, so ist M ein reelles Vielfaches der Identität.*

Beweis: Der Fall inäquivalenter Darstellungen kann wie bei komplexen Darstellungen gezeigt werden (siehe z. B. Prop. 4 in §2.2 in [Ser77]). Bei gleichen Darstellungen muß im Gegensatz zum komplexen Fall die Existenz eines reellen Eigenwerts von M gefordert werden, denn diese Existenz wird im reellen Fall nicht durch den Fundamentalsatz der Algebra gesichert. Es wird die Matrix $M' := M - \lambda I_m$ gebildet, für die $\sigma M' = M'\sigma$ gilt. Der Kern $\ker(M')$ von M' ist aufgrund

$$M'(\sigma\ker(M')) = (M'\sigma)\ker(M') = (\sigma M')\ker(M') = \sigma(M'\ker(M')) = 0$$

ein reeller und invarianter Raum unter der Operation von σ. Da σ reell irreduzibel ist und da $\ker(M) \neq 0$ wegen dem zu λ gehörenden Eigenvektor gilt, folgt $M = \lambda I_m$. □

Die Forderung nach einem reellen Eigenwert kann beim reellen Schurschen Lemma nicht weggelassen werden, wie das folgende Beispiel zeigt:

Beispiel 3.30 (Reelles Schursches Lemma) *Die durch*

$$\kappa(r) := \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix} \in \mathcal{O}(2)$$

definierte Darstellung der Gruppe $C_3 := \langle r : r^3 = 1 \rangle$ *ist reell irreduzibel. Für alle* $a, b \in \mathbb{R}$ *haben die Matrizen*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{R}^{2\times 2} \tag{3.6}$$

die Symmetrie (C_3, κ, κ)*. Die Eigenwerte dieser Matrizen sind* $a \pm bi$*, so daß genau bei reellen Eigenwerten die Vielfachen der Einheitsmatrix erhalten werden.*

Für die Untersuchung symmetrischer Ensembles und POVMs sind reelle, hermitesche Matrizen von Interesse. Die Hermitezität garantiert durch den Spektralsatz (siehe Satz 1 in §1, Kap. III von [Lor96]) die Existenz des reellen Eigenwerts, der für die Anwendung des Schurschen Lemmas benötigt wird.

Korollar 3.31 (Schursches Lemma für reelle, hermitesche Matrizen) *Es seien die beiden irreduziblen Darstellungen* $\sigma, \tau : G \to \mathcal{O}(m)$ *von* G *gegeben. Ferner sei* $M \in \mathbb{R}^{m\times m}$ *hermitesch mit der Symmetrie* (G, σ, τ)*. Dann gilt* $M = 0$ *für reell inäquivalente* σ *und* τ *sowie* $M = \lambda I_m$ *mit* $\lambda \in \mathbb{R}$ *für gleiche Darstellungen* σ *und* τ*.*

Mit dem Schurschen Lemma für reelle Darstellungen kann wie im komplexen Fall die Struktur des reellen Verkettungsraums zweier Darstellungen bestimmt werden. Hierbei kann für Matrizen mit einer Symmetrie, die durch zwei inäquivalente Darstellungen σ und τ festgelegt ist, ebenfalls gefolgert werden, daß die Matrix die Nullmatrix ist. Im Fall gleicher Darstellungen werden jedoch nur viel schwächere Aussagen erhalten, da reelle quadratische Matrizen keine reellen Eigenwerte haben müssen und daher das reelle Schursche Lemma nicht immer angewandt werden kann.

Lemma 3.32 (Strukur des reellen Verkettungsraums) *Es seien* $\sigma : G \to \mathcal{O}(m)$ *und* $\tau : G \to \mathcal{O}(n)$ *zwei reelle Darstellungen mit den Zerlegungen*

$$\sigma = \bigoplus_{j=0}^{z-1} \left(I_{m_j} \otimes \kappa_j\right) \quad \textit{und} \quad \tau = \bigoplus_{j=0}^{z-1} \left(I_{n_j} \otimes \kappa_j\right) \tag{3.7}$$

in reell inäquivalente und reell irreduzible Komponenten κ*. Dann bilden die reellen Matrizen mit der Symmetrie* $\sigma M = M\tau$ *einen* $\mathbb{R}$*-linearen Raum, der in*

$$\mathbb{R}^{\tilde{m}_0\times\tilde{n}_0} \oplus \ldots \oplus \mathbb{R}^{\tilde{m}_{z-1}\times\tilde{n}_{z-1}}$$

liegt, wobei $\tilde{m}_j := d_j m_j$ *und* $\tilde{n}_j := d_j n_j$ *mit* $d_j := \deg(\kappa_j)$ *definiert werden. Für* $m_j = 0$ *und* $n_j = 0$ *werden* $n_j d_j$ *Nullspalten bzw.* $m_j d_j$ *Nullzeilen eingefügt.*

Eine Schranke für die Dimension der hermiteschen Matrizen in dem Verkettungsraum $\mathrm{Int}(\sigma, \sigma)$ kann einfach angegeben werden, falls als Basis aller hermiteschen Matrizen die verallgemeinerten Pauli-Matrizen genutzt werden:

Lemma 3.33 (Verallgemeinerte Pauli-Matrizen) *Die d^2 Matrizen*

$$E_{k,k} := |k\rangle\langle k|, \quad X_{k,\ell} := |k\rangle\langle \ell| + |\ell\rangle\langle k| \quad \textit{und} \quad Y_{k,\ell} := i|k\rangle\langle \ell| - i|\ell\rangle\langle k|,$$

$k > \ell$, der Größe $d \times d$ sind eine Basis des $\mathbb{R}$-linearen Raums der hermiteschen Matrizen. Bezüglich des Spurskalarprodukts $\langle A|B\rangle := \mathrm{tr}(A^\dagger B)$ sind diese Matrizen orthogonal.

Durch die Einschränkung des Verkettungsraums auf reelle Matrizen und reell irreduzible Darstellungen sinken im Vergleich zum komplexen Fall sowohl die Multiplizitäten m_j als auch die reelle Dimension des Verkettungsraums, denn die reellen, hermiteschen Matrizen liegen in einem Teilraum aller hermiteschen Matrizen, der ohne Linearkombinationen mit den Matrizen $Y_{k,\ell}$ aus Lemma 3.33 gebildet wird:

Lemma 3.34 (Dimension des reellen Verkettungsraums) *Es sei $\sigma : G \to \mathcal{O}(n)$ eine reelle Darstellung von G, die wie in Gl. (3.7) zerlegt sei und wobei die κ_j reell irreduzibel und reell inäquivalent seien. Dann bilden die reellen und hermiteschen Matrizen im Verkettungsraum $\mathrm{Int}(\sigma, \sigma)$ einen reellen Vektorraum der höchstens die Dimension*

$$\sum_{j=0}^{z-1} m_j + d_j^2 \, \frac{m_j(m_j-1)}{2}$$

mit $d_j := \deg(\kappa_j)$ hat.

Beweis: Eine hermitesche Matrix $M \in \mathrm{Int}(\sigma, \sigma)$ kann nach Lemma 3.32 als

$$M = \bigoplus_{j=0}^{z-1} M_j \quad \text{mit} \quad M_j \in \mathrm{Int}(I_{m_j} \otimes \kappa_j, I_{m_j} \otimes \kappa_j) \leq \mathbb{C}^{d_j m_j \times d_j m_j}$$

geschrieben werden, wobei alle M_j hermitesch sind und $d_j := \deg(\kappa_j)$ gilt. Damit genügt es, eine hermitesche Matrix $M \in \mathrm{Int}(I_m \otimes \kappa, I_m \otimes \kappa)$ für eine irreduzible Darstellung κ des Grades $d := \deg(\kappa)$ zu betrachten. Die Matrix M kann in m^2 Teilmatrizen $M_{j,k}$ der Größe $d \times d$ zerlegt werden, d.h. es gilt

$$M = \begin{pmatrix} M_{0,0} & \dots & M_{0,d-1} \\ \vdots & \ddots & \vdots \\ M_{d-1,0} & \dots & M_{d-1,d-1} \end{pmatrix}.$$

Die Matrizen $M_{j,j}$ sind hermitesch, womit nach Kor. 3.31 die Gleichungen $M_{j,j} = \alpha_j I_d$ für $\alpha_j \in \mathbb{R}$ folgen. Da $M_{j,k} = M_{k,j}^\dagger$ gilt, verbleiben $m(m-1)/2$ Matrizen $M_{j,k}$ oberhalb der Diagonalen, die frei gewählt werden können. Für jede dieser Matrizen kann eine $\mathbb{R}$-lineare Basis mit den Matrizen $X_{k,\ell}$ aus Def. 3.33 gefunden werden, die d^2 Elemente umfaßt. □

Wie Bsp. 3.30 zeigt, kann die Schranke von Lemma 3.34 in einigen Fällen verbessert werden, denn bei diesem Beispiel können von allen möglichen (2×2)-Matrizen nur die Matrizen (3.6) die entsprechende Symmetrie haben. Dies zeigt, daß die Symmetrie einer Matrix mit reell irreduziblen Darstellungen auch dann die Menge der Matrizen einschränken kann, falls diese keine reellen Eigenwerte haben. Die Struktur der möglichen

Matrizen kann in einigen Fällen durch den Übergang zu den komplexen Darstellungen gefunden werden: Die Darstellung κ von Bsp. 3.30 wird durch

$$A := \sqrt{\frac{1}{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \quad \text{in} \quad A\kappa A^\dagger = \kappa_2 \oplus \kappa_1$$

mit den κ_j von Bsp. 2.7 zerlegt. Damit folgt für eine Matrix M mit der Symmetrie (C_3, κ, κ) nach Lemma 2.23 die Zerlegung $AMA^\dagger = \mathrm{diag}(\alpha, \beta)$ mit $\alpha, \beta \in \mathbb{C}$; durch Rücktransformation wird

$$M = A^\dagger \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} A = \frac{1}{2} \begin{pmatrix} \alpha + \beta & (\alpha - \beta)i \\ -(\alpha - \beta)i & \alpha + \beta \end{pmatrix}$$

erhalten. Diese Gleichung zeigt, daß M die in Gl. (3.6) gegebene Form haben muß. Diese über das reelle Schursche Lemma hinausgehende Struktur kann zur Verbesserung der Schranke aus Lemma 3.34 genutzt werden.

Beispiel 3.35 (Matrix mit reeller Symmetrie) *Es sei κ die irreduzible Darstellung von Bsp. 3.30. Eine reelle hermitesche Matrix M von* $\mathrm{Int}(\kappa \oplus \kappa, \kappa \oplus \kappa)$ *hat die Form*

$$\begin{pmatrix} \alpha & 0 & \beta & \gamma \\ 0 & \alpha & -\gamma & \beta \\ \beta & -\gamma & \delta & 0 \\ \gamma & \beta & 0 & \delta \end{pmatrix}$$

mit $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Der $\mathbb{R}$-lineare Raum aller reellen hermiteschen Matrizen M mit der Symmetrie $(\kappa \oplus \kappa)M = M(\kappa \oplus \kappa)$ hat demnach vier Dimensionen.

3.5.2 Optimale Messungen für reelle Ensembles

Grundlage der Anpassung von Satz 3.24 und beider Davies-Theoreme auf reelle Ensembles ist eine Konstruktion, mit der aus einem POVM ein reelles POVMs konstruiert werden kann, so daß die Transinformation erhalten bleibt:

Lemma 3.36 (Realteil eines POVMs) *Es sei S ein reelles Ensemble und P ein POVM mit den Operatoren Π_j. Ferner bezeichne $\Re(P)$ die Familie der Operatoren $\Re(\Pi_j)$, die durch eintragsweise Bildung des Realteils aus Π_j hervorgehen. Dann ist auch $\Re(P)$ ein POVM, und es gilt $I(S, P) = I(S, \Re(P))$.*

Beweis: Siehe Beweis von Th. 1 in [SBJ+99]. □

Bei der Konstruktion der Operatoren $\Re(\Pi_j)$ bleibt der Rang der Operatoren nicht notwendigerweise erhalten; insbesondere müssen die $\Re(\Pi_j)$ nicht vom Rang eins sein, auch wenn es die Π_j sind. Dies kann mit dem Spektralsatz und Lemma 2 in [Dav78] behoben werden, denn diese lassen es zu, daß jeder Operator $\Re(\Pi)$ in Operatoren des Ranges eins zerlegt wird.

Lemma 3.37 (Optimale reelle POVMs) *Es sei S ein reelles Ensemble. Dann existiert ein optimales POVM, das nur reelle Operatoren vom Rang eins umfaßt.*

Beweis: Siehe Beweis von Th. 1 in [SBJ+99]. □

Mit einem optimalen POVM P, das reelle Operatoren vom Rang eins hat, kann dieselbe Konstruktion wie beim erstem Davies-Theorem durchgeführt werden, um eine obere Schranke für die Anzahl der POVM-Operatoren zu erhalten. Hierbei wird aber eine niedrigere obere Schranke erreicht, denn die Operatoren von P liegen in dem Teilraum der hermiteschen Matrizen, der ohne lineare Kombinationen mit den imaginären Matrizen $Y_{k,\ell}$ aus Lemma 3.33 gebildet wird. Damit kann die Schranke von Satz 3.22 um die Anzahl dieser Basismatrizen verringert werden (siehe [SBJ+99]).

Satz 3.38 (Erstes reelles Davies-Theorem) *Es sei S ein reelles Ensemble. Dann existiert ein optimales POVM mit n reellen Operatoren vom Rang eins, wobei*

$$d \leq n \leq \frac{d(d+1)}{2}\,.$$

Neben dieser Anpassung des ersten Theorems von Davies läßt sich auch das zweite Davies-Theorem anpassen, wobei die Irreduzibilität der Darstellung zu einer *reellen* Irreduzibilität abgeschwächt werden kann (siehe [SBJ+99]).

Satz 3.39 (Zweites reelles Davies-Theorem) *Es sei S ein reelles Ensemble mit einer reell irreduziblen Darstellung der Symmetriegruppe G. Dann gibt es ein optimales POVM mit reellen Operatoren vom Rang eins, das eine einzelne Bahn unter G ist.*

Ist die Darstellung der Symmetriegruppe auch nicht reell irreduzibel, so kann eine reelle Version des allgemeineren Satzes 3.24 genutzt werden:

Satz 3.40 (Anzahl Bahnen bei reellen Ensembles) *Es sei S ein reelles Ensemble, das bzgl. der reellen Darstellung σ symmetrisch sei. Hierbei sei σ wie in Gl. (3.7) zerlegt, wobei die Darstellungen κ_j reell irreduzibel und reell inäquivalent seien. Dann existiert ein optimales POVM mit Operatoren vom Rang eins, das höchstens*

$$\sum_{j=0}^{z-1} m_j + d_j^2 \, \frac{m_j(m_j-1)}{2}$$

Bahnen unter der Operation von G umfaßt, wobei $d_j := \deg(\kappa_j)$ gilt.

Beweis: Es sei P ein optimales POVM. Mit Lemma 3.37 kann angenommen werden, daß P nur reelle Operatoren vom Rang eins hat. Im Vergleich zum Beweis zu Satz 3.24 sind alle D_j reell. Damit können die reellen Verkettungsräume betrachtet werden. Deren Dimension ist in Lemma 3.34 festgelegt. □

Kann Satz 3.40 statt Satz 3.24 für ein Ensemble angewandt werden, folgen für die Optimierung von POVMs zwei Vereinfachungen: Einerseits kann die Suche auf POVMs mit weniger Bahnen beschränkt werden und andererseits können die Bahnen aufgrund der Einschränkung auf reelle Werte einfacher parametrisiert werden. Die Ursache der reduzierten Anzahl von Bahnen ist, daß eine reell irreduzible Darstellung über den komplexen Zahlen nicht irreduzibel sein muß, sondern in bis zu zwei Komponenten zerfallen kann (siehe §13.2 in [Ser77]).

3.6 Beispiele für optimale POVMs

Einfache Beispiele symmetrischer Zustände, bei denen Satz 3.40 genutzt werden kann, um die Suche nach optimalen Messungen zu vereinfachen, stellen die angehobenen Drillinge (*lifted trines*, siehe [Sho01, Sho04]) und auch die Doppeldrillinge (*double trines*, siehe [PW91, Woo05]) dar. Für diese Ensembles können mit Satz 3.40 ähnlich wie bei der Analyse von [Sho01, Sho04] durch numerische Untersuchungen optimale symmetrische POVMs bestimmt werden. Es stellt sich dabei heraus, daß bei den angehobenen Drillingen eine einzelne Bahn von Operatoren nicht genügen muß, um die erreichbare Information zu erhalten. Bei den Doppeldrillingen kann hingegen numerisch gezeigt werden, daß die nur eine Bahn umfassende PGM aus Def. 3.4 optimal ist.

3.6.1 Angehobene Drillinge

Die angehobenen Drillinge werden ausgehend von den Drillingen aus Bsp. 3.12 erhalten, indem diese entlang einer dritten Dimension angehoben werden (siehe [Sho01, Sho04]):

Definition 3.41 (Angehobene Drillinge) *Für $\alpha \in [0,1]$ legen die Zustandsvektoren*

$$\begin{pmatrix} \sqrt{\alpha} \\ \sqrt{1-\alpha} \\ 0 \end{pmatrix}, \begin{pmatrix} \sqrt{\alpha} \\ -\frac{1}{2}\sqrt{1-\alpha} \\ \frac{\sqrt{3}}{2}\sqrt{1-\alpha} \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} \sqrt{\alpha} \\ -\frac{1}{2}\sqrt{1-\alpha} \\ -\frac{\sqrt{3}}{2}\sqrt{1-\alpha} \end{pmatrix}$$

ein Ensemble angehobener Drillinge fest. Jeder Zustand tritt hierbei mit der Wahrscheinlichkeit $1/3$ auf.

Die Symmetriegruppe der angehobenen Drillinge wird von der 120°-Drehung

$$R := \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & \sqrt{3} \\ 0 & -\sqrt{3} & -1 \end{pmatrix} \in \mathcal{O}(3)$$

erzeugt, womit diese Gruppe zu $C_3 := \langle r : r^3 = 1 \rangle$ isomorph ist. Die zugehörige Darstellung $\sigma(r^j) := R^j$ von C_3 enthält die beiden reell irreduziblen Darstellungen κ_0 und κ_1, welche durch

$$\kappa_0(r) := (1) \quad \text{und} \quad \kappa_1(r) := \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}$$

festgelegt sind, jeweils einmal. Da diese nicht zueinander reell äquivalent sind, werden nach Satz 3.40 höchstens zwei Bahnen O_0 und O_1 mit den Operatoren

$$\Pi_0, R\Pi_0R^{-1}, R^2\Pi_0R^{-2} \quad \text{bzw.} \quad \Pi_1, R\Pi_1R^{-1}, R^2\Pi_1R^{-2}$$

vom Rang eins benötigt, um ein optimales POVM zu erreichen. Mit der Normierung $\mathrm{tr}(\Pi_0) = \mathrm{tr}(\Pi_1) = 1$ kann das POVM als Konvexkombination $P = \lambda O_0 + (1-\lambda)O_1$ geschrieben werden; umgekehrt ist aber solch eine Konvexkombination nur für geeignete λ, Π_0 und Π_1 ein POVM. Mit der Anwendung von Lemma 3.17 auf die einzelnen Bahnen wird die Transinformation

$$I(S,P) = \lambda I(S,O_0) + (1-\lambda)I(S,O_1)$$

erhalten, womit folgt, daß die Transinformation der Konvexkombination zweier Bahnen die Konvexkombination der entsprechenden Informationen ist. Dabei können $I(S, O_0)$ und $I(S, O_1)$, die hier für einzelne Bahnen und nicht für POVMs definiert sind, negative Werte annehmen und sind daher nur *formale* Transinformationen; die Konvexkombination der formalen Transinformationen zweier Bahnen ist hingegen immer positiv und entspricht der Transinformation des POVMs.

Zur Suche optimaler POVMs werden die Operatoren der Bahnen parametrisiert: Für einen Operator $\Pi := |\Psi(a,b)\rangle\langle\Psi(a,b)|$ wird die Parametrisierung

$$|\Psi(a,b)\rangle := \begin{pmatrix} \cos(a) \\ \sin(a)\cos(b) \\ \sin(a)\sin(b) \end{pmatrix} \tag{3.8}$$

genutzt, womit die Bahnsumme

$$\Pi + R\Pi R^{-1} + R^2\Pi R^{-2} = \begin{pmatrix} 3\cos^2(a) & 0 & 0 \\ 0 & \frac{3}{2} - \frac{3}{2}\cos^2(a) & 0 \\ 0 & 0 & \frac{3}{2} - \frac{3}{2}\cos^2(a) \end{pmatrix}$$

folgt. Für zwei Bahnen O_0 und O_1 mit den Parametern (a,b) und (c,d) ist deshalb die Konvexkombination $\lambda O_0 + (1-\lambda)O_1$ genau dann ein POVM, d. h. die Summe aller Operatoren ist I_3, wenn

$$\lambda\cos^2(a) + (1-\lambda)\cos^2(c) = \frac{1}{3} \tag{3.9}$$

gilt. Falls ohne Beschränkung der Allgemeinheit die Ungleichung $\cos^2(a) \leq \cos^2(c)$ angenommen wird, bedeutet diese Forderung, daß $1/3 \in [\cos^2(a), \cos^2(c)]$ gilt, womit durch

$$\cos^2(a) \in [0, 1/3] \quad \text{und} \quad \cos^2(c) \in [1/3, 1]$$

alle möglichen Werte von a und c festgelegt sind. Zur Vereinfachung der Optimierung kann die Transinformation $I(a,b)$ auch nur für Bahnen mit $a = \arccos\sqrt{x}$ für $x \in [0,1]$ und $b \in [0, 2\pi/3]$ betrachtet werden[3]. Dies genügt für das Auffinden optimaler POVMs, denn für gegebenes $\cos(a)$ mit $\cos^2(a) = x$ und gegebenes b gibt es nur vier mögliche Vektoren $|\Psi(a,b)\rangle$ aus Gl. (3.8), die denselben Wert x haben: Diese Vektoren sind durch

$$\cos(a) = \pm\sqrt{x} \quad \text{und} \quad \sin(a) = \pm\sqrt{1-x}$$

festgelegt. Zur Vereinfachung werden diese vier möglichen Kombinationen mit $++$, $+-$, $-+$ und $--$ bezeichnet. Der Fall $--$ führt zu derselben Information wie $++$, denn der entsprechende Vektor $|\Psi(a,b)\rangle$ unterscheidet sich nur durch die globale Phase -1 vom Vektor des Falls $++$. Die Wahrscheinlichkeiten der beiden Messungen und die Informationen sind deshalb für beide Fälle gleich. Analog folgt, daß die Fälle $+-$ und $-+$ dieselbe Information zur Folge haben. Für $+-$ trägt der Vektor (3.8) im Vergleich zum Fall $++$ in den letzten beiden Komponenten ein Minuszeichen. Dieselben Wahrscheinlichkeiten und damit auch dieselbe Information wie für den Fall $++$ können erhalten werden, falls b durch $b + \pi$ ersetzt wird, denn dabei erhalten $\sin(a)\cos(b)$ und $\sin(a)\sin(b)$ jeweils den

[3]Der Wert von b kann durch die Drehsymmetrie eingeschränkt werden.

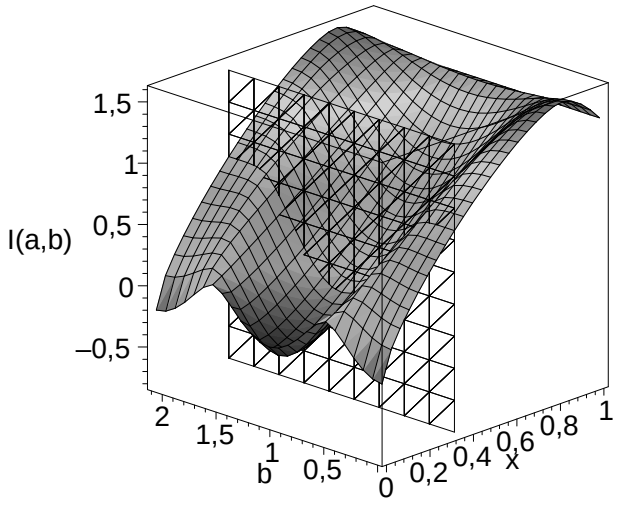

Abbildung 3.2: Die Transinformation $I(a,b)$ mit $a = \arccos\sqrt{x}$ für die angehobenen Drillinge mit $\alpha = 1/20$. Die Information einer Bahn kann negativ sein. Wie Abb. 3.3 aber zeigt, führt die Konvexkombination der Information zweier Punkte auf verschiedenen Seiten von $x = 1/3$ immer zu einer nichtnegativen Information. (Abbildung aus [Dec05] übernommen.)

Phasenfaktor -1. Dies zeigt, daß die Suche nach optimalen Messungen auf die Parameter $(\arccos\sqrt{x}, b)$ mit $x \in [0,1]$ und $b \in [0, 2\pi/3]$ eingeschränkt werden kann, ohne die Optimalität der so durchsuchten POVMs zu verlieren.

Für leicht angehobene Drillinge, d. h. α ist nahe null, kann numerisch gezeigt werden, daß mindestens zwei Bahnen von POVM-Operatoren für eine optimale Messung notwendig sind (siehe [Sho01, Sho04]). Damit ist eine direkte Verallgemeinerung des zweiten Davies-Theorems auf reduzible Darstellungen nicht möglich: Es gibt Ensembles, für die kein POVM optimal ist, das nur aus einer einzigen Bahn besteht. Darüber hinaus wird durch dieses Beispiel gezeigt, daß die obere Schranke von Satz 3.40 erreicht werden kann. Für die folgende, zu [Sho01, Sho04] ähnliche Analyse dieser Eigenschaften für das Beispiel mit $\alpha := 1/20$ ist in Abb. 3.2 und 3.3 die von x und b abhängige Information $I(\arccos\sqrt{x}, b)$ dargestellt. Die Bedingung von Gl. (3.9) zum Erhalten eines POVMs bedeutet hierbei, daß die zu den Parametern (a,b) und (c,d) der beiden Bahnen gehörenden Punkte auf verschiedenen Seiten der Ebene $x = 1/3$ liegen. Aus den Abbildungen folgt, daß eine einzelne Bahn nicht ausreicht, um ein optimales POVM zu erhalten: Ein POVM, das nur aus einer Bahn besteht, entspricht einem Punkt auf der Ebene $x = 1/3$, und die Information, die für einen Punkt auf dieser Ebene erhalten werden kann, ist nach Abb. 3.4 maximal $0,8456$ bit. Diese Information wird für ein POVM erhalten, dessen Parameter $(a,b) = (\nu, b)$ durch

$$\nu := \arccos\sqrt{1/3} \quad \text{und} \quad b \approx 0,1377$$

festgelegt sind. Mit Abb. 3.3 folgt wie in [Sho01, Sho04], daß mit zwei Bahnen mehr Information erhalten werden kann: Eine Bahn entspricht einem Punkt mit $x = 0$ und die andere einem Punkt mit $b = 0$ auf der anderen Seite der Ebene $x = 1/3$. Numerische Berechnungen zeigen, daß ein möglicher optimaler Punkt für $x = 0$ mit den Parametern $(a,b) = (\pi/2, \pi/2)$ gefunden wird; die zugehörige Bahn führt zu der Transinformation $0,15996$ bit. Der andere optimale Punkt kann mit den Parametern $(\arccos\sqrt{0,3831}, 0)$

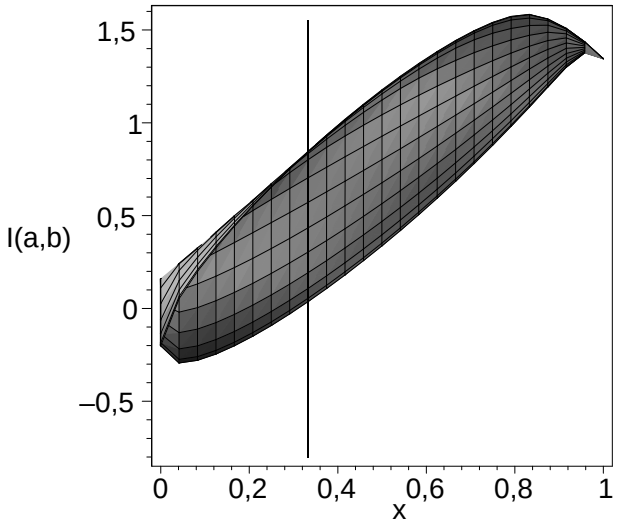

Abbildung 3.3: Draufsicht von Abb. 3.2 auf die x-I-Ebene. Diese Darstellung zeigt für jedes x das Maximum von $I(a, b)$, wobei $a = \arccos\sqrt{x}$ gilt und b die Variable ist, für die das Maximum gesucht wird. Nach [Sho01, Sho04] ist dieses Maximum als Funktion von x im Bereich $[0,\ 0,3831]$ konvex. (Abbildung aus [Dec05] übernommen.)

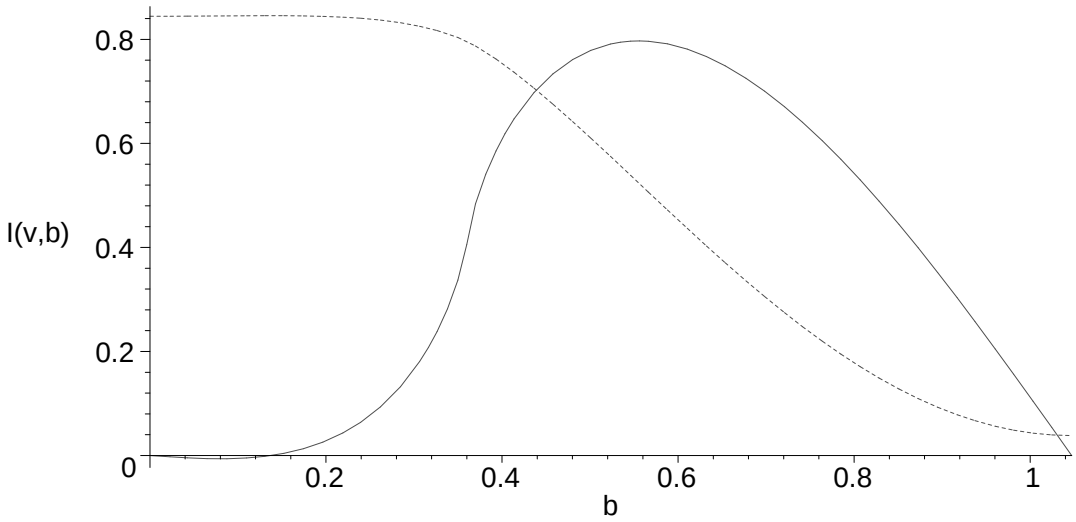

Abbildung 3.4: Die gestrichelte Funktion ist $I(\nu, b)$ für den Wert $\nu := \arccos\sqrt{1/3}$. Diese Funktion hat an der Stelle $b \approx 0,1377$ ein globales Maximum, denn die andere Funktion ist die Ableitung $-(d/db)I(\nu, b)/2$ und verschwindet an dieser Stelle. Alle übrigen Werte von $I(\nu, b)$ können durch die Symmetrie ermittelt werden. (Abbildung aus [Dec05] übernommen.)

erreicht werden; die zugehörige Bahn ergibt $0,9499$ bit. Die Konvexkombination beider Informationen ist $0,8472$ bit. Dies ist mehr Transinformation als die $0,8456$ bit, die durch ein POVM, das nur eine Bahn umfaßt, erhalten werden kann. Damit müssen optimale symmetrische POVMs für die angehobenen Drillinge mit $\alpha = 1/20$ mindestens zwei Bahnen umfassen.

3.6.2 Doppeldrillinge

Die Doppeldrillinge gehen aus den Drillingen von Bsp. 3.12 hervor, indem durch das Tensorprodukt die Zustände auf vier Dimensionen erweitert werden (siehe [PW91, Woo05]):

Definition 3.42 (Doppeldrillinge) *Die Doppeldrillinge sind die Zustände* $|\Phi'_j\rangle\langle\Phi'_j|$ *für* $|\Phi'_j\rangle := |\Phi_j\rangle \otimes |\Phi_j\rangle$ *mit den Drillingen* $|\Phi_j\rangle\langle\Phi_j|$ *aus Bsp. 3.12. Jeder Zustand tritt mit der Wahrscheinlichkeit* $1/3$ *auf.*

Die Doppeldrillinge entsprechen den Zustandsvektoren

$$|\Phi'_0\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |\Phi'_1\rangle := \frac{1}{4}\begin{pmatrix} 1 \\ \sqrt{3} \\ \sqrt{3} \\ 3 \end{pmatrix} \quad \text{und} \quad |\Phi'_2\rangle := \frac{1}{4}\begin{pmatrix} 1 \\ -\sqrt{3} \\ -\sqrt{3} \\ 3 \end{pmatrix}$$

zweier Qubits[4]. Die Anwendung des unitären Basiswechsels

$$V := \sqrt{\frac{1}{2}}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

führt zu den Zustandsvektoren

$$\sqrt{\frac{1}{2}}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \sqrt{\frac{1}{2}}\begin{pmatrix} 1 \\ -1/2 \\ \sqrt{3}/2 \\ 0 \end{pmatrix} \quad \text{und} \quad \sqrt{\frac{1}{2}}\begin{pmatrix} 1 \\ -1/2 \\ -\sqrt{3}/2 \\ 0 \end{pmatrix}.$$

Wird die letzte Komponente weggelassen[5], so ergeben sich die angehobenen Drillinge aus Def. 3.41 mit dem Parameter $\alpha := 1/2$; im Unterschied zu den Drillingen aus Abschnitt 3.6.1 sind diese stark angehoben. Wie in [Sho01, Sho04] angedeutet wird, führt dieser Unterschied dazu, daß für die Doppeldrillinge ein optimales POVM existiert, das nur eine Bahn umfaßt. Durch eine Anpassung der Analyse aus Abschnitt 3.6.1 kann darüber hinaus auch numerisch gezeigt werden, daß die in [PW91] untersuchte PGM für die Doppeldrillinge sogar eine optimale Messung ist.

Die Analyse aus Abschnitt 3.6.1 für die schwach angehobenen Drillinge kann auf die

[4] Im Vergleich zur Symmetrie der angehobenen Drillinge aus Abschnitt 3.6.1 haben die Doppeldrillinge die zusätzliche Symmetrieoperation, die beide Qubits vertauscht. Da durch diese zusätzliche Symmetrie keine Vereinfachungen folgen, wird sie bei der Untersuchung der Doppeldrillinge nicht betrachtet.

[5] Ein optimales POVM auf den vier Dimensionen kann auf ein POVM, das auf den ersten drei Komponenten operiert, projiziert werden. Diese Projektion ändert nicht die Transinformation.

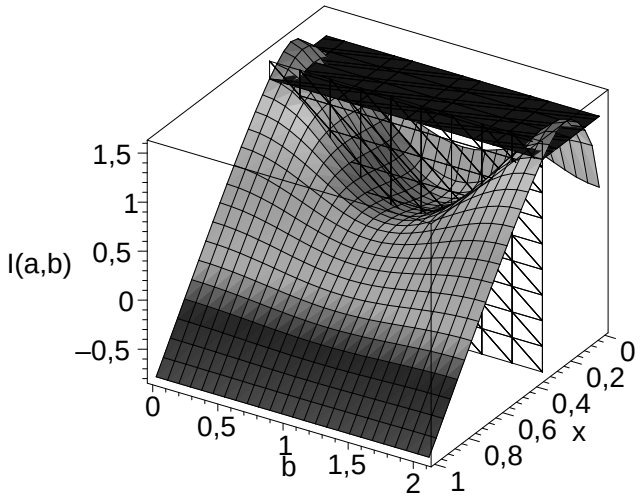

Abbildung 3.5: Die Transinformation $I(a, b)$ mit $a = \arccos\sqrt{x}$ für die Doppeldrillinge; die horizontale Ebene entspricht der Information $1,369$ bit. Es wird vermutet, daß diese Information die erreichbare Information ist (siehe [PW91, Woo05]). (Abbildung aus [Dec05] entnommen.)

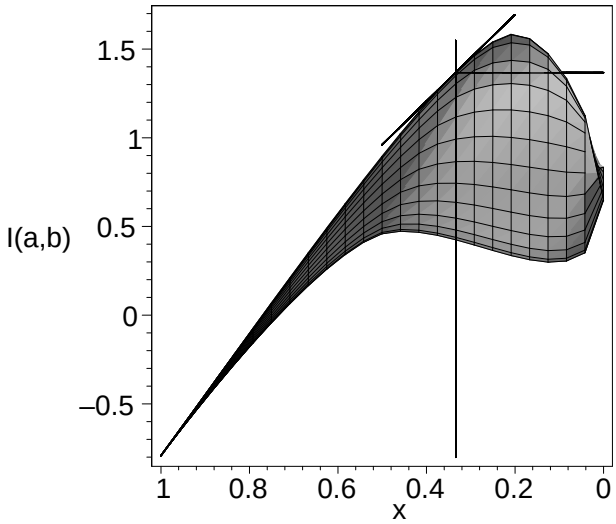

Abbildung 3.6: Draufsicht von Abb. 3.5 auf die x-I-Ebene mit zusätzlicher Tangente bei $x = 1/3$. Diese Darstellung zeigt das Maximum von $I(a, b)$ mit $a = \arccos\sqrt{x}$ für jedes x, wobei das Maximum über b gebildet wird. (Abbildung aus [Dec05] entnommen.)

Doppeldrillinge übertragen werden, indem bei den Rechnungen der Wert $\alpha = 1/20$ durch $\alpha = 1/2$ ersetzt wird. Damit folgen Abb. 3.5 und 3.6, in denen die Transinformation $I(\arccos\sqrt{x}, b)$ in Abhängigkeit von x und b dargestellt wird. Ein optimales POVM kann wie bei den leicht angehobenen Drillingen nach Satz 3.40 durch die Konvexkombination von höchstens zwei Bahnen erhalten werden. Aus Abb. 3.5 und 3.6 folgt, daß eine einzelne Bahn, die einem Punkt mit $x = 1/3$ entspricht, optimal ist. Der Grund hierfür ist, daß in Abb. 3.6 jede Verbindungsgerade zweier Bildpunkte der Funktion auf verschiedenen Seiten von $x = 1/3$ an dieser Stelle nicht über dem Maximum für $x = 1/3$ liegt. Dies kann darüber hinaus durch die negativ definite Hesse-Matrix

$$\begin{pmatrix} \frac{81-27\sqrt{2}\gamma}{16\ln(2)} & 0 \\ 0 & \frac{6-(2+\sqrt{2})\gamma}{3\ln(2)} \end{pmatrix} \approx \begin{pmatrix} -7,221 & 0 \\ 0 & -4,041 \end{pmatrix} \quad \text{mit} \quad \gamma := \ln\left(2(3+2\sqrt{2})^2\right)$$

von $I(\arccos\sqrt{x}, b)$ an der Stelle $(x, b) = (1/3, 0)$ gezeigt werden, denn diese hat zur Folge, daß die Information an diesem Punkt lokal konkav ist. Eine optimale Messung kann gefunden werden, indem die von der Variablen b abhängige Funktion $I(\nu, b)$ an der Stelle $\nu := \arccos\sqrt{1/3}$ betrachtet wird: Diese Funktion hat bei $b := 0$ ein Extremum, weshalb durch $(a, b) = (\nu, 0)$ ein optimales POVM mit drei Operatoren festgelegt wird. Dieses führt zur erreichbaren Information

$$I(\nu, 0) = \frac{2\sqrt{2}\gamma - 9\ln(2)}{6\ln(2)} \approx 1,369 \text{ bit}\,.$$

Derselbe Wert wurde auch in [PW91] für die PGM der Doppeldrillinge gefunden, wobei die Optimalität nur vermutet wurde (siehe auch [Woo05]). Durch die Ausnutzung von Satz 3.40 konnte damit die Gültigkeit dieser Vermutung unterstützt werden.

Kapitel 4

Durchführung symmetrischer POVMs

Bei vielen Quantensystemen stellen die orthogonalen Messungen die Klasse der am besten untersuchten Messungen dar. In der Quanteninformationstheorie und bei Quantenalgorithmen können aber auch die allgemeineren POVMs von Interesse sein: Beispielsweise sind nach den Untersuchungen von Kap. 3 optimale Messungen nur in wenigen, speziellen Fällen orthogonal. Dies führt unmittelbar zu der Frage, wie ein POVM mit möglichst geringem Aufwand auf eine orthogonale Messung reduziert werden kann. Dabei soll angenommen werden, daß diese Reduktion auf einem Quantenrechner durchgeführt wird. Dieses Vorgehen bietet zwei große Vorteile: Einerseits sind die zur Verfügung stehenden Grundoperationen und direkt durchführbaren Messungen klar spezifiziert und von Eigenschaften spezieller physikalischer Systeme unabhängig. Andererseits bietet der Quantenrechner mit dem Quantenschaltkreismodell einen möglichen Ausgangspunkt für eine Komplexitätstheorie von Messungen.

Es kann nicht erwartet werden, daß für alle POVMs effiziente Reduktionsverfahren existieren, denn schon eine effiziente Durchführung aller orthogonalen Messungen würde effiziente Algorithmen für PSPACE-vollständige Probleme zur Folge haben (siehe z. B. [WJDB03]). Es ist daher sinnvoll, die Untersuchungen auf Messungen zu beschränken, die eine zusätzliche Struktur haben, welche als Grundlage der Konstruktion effizienter Reduktionsalgorithmen dienen kann. Die Untersuchungen in Kap. 3 zeigen, daß die symmetrischen POVMs eine interessante Klasse solcher Messungen sind. In diesem Kapitel wird daher der Frage nachgegangen, wie die Symmetrie von POVMs genutzt werden kann, um diese effizient auf einem Quantenrechner durchzuführen. Es zeigt sich hierbei, daß die Symmetrie zu einem allgemeinen Entwurfsprinzip führt, das für einige symmetrische POVMs effiziente Reduktionsalgorithmen liefert. Die Untersuchungen beschränken sich hierbei zunächst auf die Wahrscheinlichkeiten der Messungen, d. h. durch die orthogonalen Messungen werden dieselben Wahrscheinlichkeiten wie bei der POVM-Messung erhalten. Die Reduktion auf orthogonale Messungen unter Berücksichtigung der Zustandsänderung wird im fünften Kapitel diskutiert.

4.1 Durchführung eines POVMs

Sollen bei der Reduktion eines POVMs auf orthogonale Messungen nur die Wahrscheinlichkeiten der Resultate reproduziert werden, so genügt es, wenn Operatoren vom Rang eins betrachtet werden. Liegt nämlich bei der Messung des POVMs P mit den Operatoren $\Pi_j = \sum_k \Pi_{j,k}$ der Zustand ρ vor, so gilt für die Wahrscheinlichkeit des Resultats j die Gleichung

$$\mathrm{tr}(\rho\Pi_j) = \sum_k \mathrm{tr}(\rho\Pi_{j,k})\,.$$

Demnach können die Wahrscheinlichkeiten auch dann erhalten werden, wenn das POVM, das die Operatoren $\Pi_{j,k}$ umfaßt, gemessen wird und die Resultate (j,k) zu j zusammengefaßt werden. Dasselbe Linearitätsargument zeigt, daß die Wahrscheinlichkeiten für alle Zustände korrekt reproduziert werden, falls dies für alle reinen Zustände der Fall ist. Bei der Suche nach einer Reduktion des POVMs mit $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ genügt daher der Nachweis, daß bei den Zuständen $\rho = |\Phi\rangle\langle\Phi|$ die Wahrscheinlichkeiten

$$\mathrm{tr}(\rho\Pi_j) = |\langle\Psi_j|\Phi\rangle|^2 \tag{4.1}$$

für die Resultate j erhalten werden. Diese folgen beispielsweise bei der Messung in der Standardbasis, falls der Zustand $|\Phi\rangle\langle\Phi|$ in den durch

$$\sum_{j=0}^{n-1}\langle\Psi_j|\Phi\rangle|j\rangle \tag{4.2}$$

beschriebenen Zustand transformiert wird. Dieser Zustand kann aber nur erhalten werden, wenn angenommen wird, daß das zu messende d-dimensionale System Teil eines n-dimensionalen Systems ist. Dies bedeutet, daß alle Zustände und POVM-Operatoren außerhalb der ersten d Dimensionen verschwinden und diese Zusatzdimensionen bei $|\Phi\rangle$ und $|\Psi\rangle$ daher weggelassen werden. Für die Bildung des in Gl. (4.2) beschriebenen Zustands ist es notwendig, diesen Unterraum zu verlassen, indem eine geeignete unitäre Transformation auf dem gesamten Raum durchgeführt wird. Werden die $n-d$ Dimensionen außerhalb des Raums bei der Beschreibung wieder hinzugenommen, so wird der Zustand durch $\rho \oplus 0_{n-d}$ beschrieben, wobei 0_{n-d} die quadratische Nullmatrix der Größe $n-d$ bezeichnet. Entsprechend wird der Zustandsvektor $|\Phi\rangle$ um $n-d$ Nullen erweitert. In dem erweiterten Raum können die Forderungen an die notwendige Transformation beschrieben werden:

Definition 4.1 (Durchführung eines POVMs) *Es sei auf einem d-dimensionalen System ein POVM mit den n Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ gegeben. Das POVM wird mit der Matrix $\tilde{M} \in \mathcal{U}(n)$ durchgeführt, falls*

$$\tilde{M}^\dagger \begin{pmatrix} |\Phi\rangle \\ 0_{n-d} \end{pmatrix} = \sum_{j=0}^{n-1}\langle\Psi_j|\Phi\rangle|j\rangle \tag{4.3}$$

für alle $|\Phi\rangle$ gilt. Hierbei bezeichnet $|\Phi\rangle \in \mathbb{C}^d$ den Zustandsvektor des zu messenden Systems und 0_{n-d} den Nullvektor der Länge $n-d$.

Durch Gl. (4.3) wird die Matrix $\tilde{M}^\dagger$ nicht vollständig festgelegt, denn durch die Nullkomponenten des Vektors sind nur die ersten d Spalten von $\tilde{M}^\dagger$ relevant. Diese Freiheit bei der Wahl von $\tilde{M}$ kann genutzt werden, um den Aufwand der Durchführung zu verringern. Durch das Naimark-Theorem wird hierbei garantiert, daß eine geeignete Matrix $\tilde{M}$ immer existiert (siehe Abschnitt 9-6 in [Per93]):

Lemma 4.2 (Naimark-Theorem) *Für jedes POVM P existiert eine unitäre Matrix $\tilde{M}$, die P nach Def. 4.1 durchführt.*

Für das Naimark-Theorem gibt es einen konstruktiven Beweis: Es werden hierzu die Vektoren $|\Psi_j\rangle$ des POVMs in der Matrix

$$M := \sum_{j=0}^{n-1} |\Psi_j\rangle\langle j| = (|\Psi_0\rangle \dots |\Psi_{n-1}\rangle) \in \mathbb{C}^{d\times n} \tag{4.4}$$

zusammengefaßt. Die Vektoren $|\Psi_j\rangle$ sind nicht eindeutig, denn jeder dieser Vektoren kann mit einer beliebigen Phase multipliziert werden. Nach Gl. (4.1) haben aber diese Phasen keinen Einfluß auf die Wahrscheinlichkeiten der Messung und können daher beliebig gewählt werden. Die Zeilen von M sind aufgrund der zugehörenden Gram-Matrix $MM^\dagger = \sum_{j=0}^{n-1} |\Psi_j\rangle\langle\Psi_j| = I_d$ orthonormal. Damit kann M zu einer unitären Matrix

$$\tilde{M} = \sum_{j=0}^{n-1} \begin{pmatrix} |\Psi_j\rangle \\ |\Theta_j\rangle \end{pmatrix} \langle j| \in \mathcal{U}(n) \tag{4.5}$$

ergänzt werden, indem passende orthonormale Zeilen angehängt werden. Diese Zeilen werden in Gl. (4.5) zur Vereinfachung der Notation als Spaltenvektoren $|\Theta_j\rangle \in \mathbb{C}^{n-d}$ geschrieben. Alternativ ist auch die Erweiterung von $M^\dagger$ um orthonormale Spalten möglich; werden diese zu der Matrix N zusammengefaßt, so folgt mit der Notation aus Def. 2.34 die Zusammensetzung $\tilde{M}^\dagger = (M^\dagger|N)$. Die so konstruierte Matrix $\tilde{M}$ erfüllt die Forderung von Def. 4.1 und führt deshalb das POVM durch.

Beispiel 4.3 (Durchführung eines POVM) *Für das POVM mit den zu*

$$|\Psi_0\rangle := \sqrt{\frac{1}{3}} \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ |\Psi_1\rangle := \sqrt{\frac{1}{3}} \begin{pmatrix} 1 \\ \omega_3 \end{pmatrix} \text{ und } |\Psi_2\rangle := \sqrt{\frac{1}{3}} \begin{pmatrix} 1 \\ \omega_3^2 \end{pmatrix}$$

gehörenden Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ folgt nach Gl. (4.4) die Matrix

$$M := \sqrt{\frac{1}{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \end{pmatrix} \in \mathbb{C}^{2\times 3},$$

wobei $\omega_3 := e^{2\pi i/3}$ eine dritte Einheitswurzel ist. Eine mögliche unitäre Ergänzung dieser Matrix ist die DFT-Matrix

$$\tilde{M} := \sqrt{\frac{1}{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3 \end{pmatrix} \in \mathcal{U}(3),$$

wobei nach Gl. (4.5) die drei Vektoren

$$|\Theta_0\rangle := \sqrt{\frac{1}{3}}\,(1)\,,\quad |\Theta_1\rangle := \sqrt{\frac{1}{3}}\,(\omega_3^2)\quad \text{und}\quad |\Theta_2\rangle := \sqrt{\frac{1}{3}}\,(\omega_3)$$

mit jeweils einer Komponente betrachtet werden. Das POVM kann demnach durch $F_3^\dagger$ aus Def. 1.24 auf die Messung in der Standardbasis reduziert werden.

Das zu messende System kann durch Hinzunahme eines Hilfssystems der Dimension k in ein n-dimensionales eingebettet werden, falls $dk = n$ gilt, d. h. die Dimension des Systems teilt die Anzahl der POVM-Operatoren. Ist das Hilfssystem mit $|0\rangle$ initialisiert, so folgt die nach Def. 4.1 notwendige Initialisierung

$$|0\rangle \otimes |\Phi\rangle = \begin{pmatrix} |\Phi\rangle \\ 0_{d(k-1)} \end{pmatrix}$$

des Systems, wobei $0_{d(k-1)}$ den Nullvektor der Länge $d(k-1) = n-d$ bezeichnet. Diese Ankopplung eines Hilfssystems kann für beliebige POVMs genutzt werden, denn ein POVM kann immer durch Nulloperatoren erweitert werden, womit das POVM nicht wesentlich verändert wird. Eine andere Möglichkeit, die zusätzlichen Dimensionen zu erhalten, wird in Abschnitt 4.5.2 für quantenoptische Systeme diskutiert.

4.2 Ausnutzung der Symmetrie

Für die Operatoren eines POVMs mit der Symmetrie (G, σ, π) gilt nach Def. 2.13 die Gleichung $\sigma(g)\Pi_j\sigma(g)^\dagger = \Pi_{\pi(g)(j)}$. Bei der Zerlegung von Operatoren Π_j höheren Ranges in mehrere vom Rang eins bleibt diese Symmetrie im wesentlichen erhalten, falls π keine Operatoren auf sich selbst abbildet:

Lemma 4.4 (Zerlegung und Symmetrie eines POVMs) *Es sei P ein POVM mit den Operatoren Π_j und der Symmetrie (G, σ, π), wobei $\pi(g)(j) \neq j$ für alle j gilt. Dann gibt es ein POVM mit den Operatoren $\Pi_{j,k} := |\Psi_{j,k}\rangle\langle\Psi_{j,k}|$, die sich zu*

$$\Pi_j = \sum_{k=0}^{n_j-1} |\Psi_{j,k}\rangle\langle\Psi_{j,k}|$$

aufsummieren, und der Symmetrie $(G, \sigma, \tilde{\pi})$ mit $\tilde{\pi}(g)(j,k) := (\pi(g)(j), k)$.

Beweis: Unter der Operation von π zerfallen die Operatoren von P in Bahnen. Für jede Bahn wird ein Vertreter Π_j gewählt und gemäß Satz 1.3 in

$$\Pi_j = \sum_k \Pi_{j,k} \quad \text{mit} \quad \Pi_{j,k} := |\Psi_{j,k}\rangle\langle\Psi_{j,k}|$$

zerlegt. Durch die Symmetrie werden die anderen Operatoren $\Pi_{\pi(g)(j)} := \sigma(g)\Pi_{j,k}\sigma(g)^\dagger$ der Bahnen erhalten. Da $\pi(g)(j) \neq \pi(h)(j)$ für $g \neq h$ gilt, sind diese Operatoren wohldefiniert. Die Gleichung des Lemmas folgt mit

$$\Pi_{\pi(g)(j),k} := \sigma(g)\Pi_{j,k}\sigma(g)^\dagger\,.$$

□

Durch Lemma 4.4 kann auch bei vielen symmetrischen POVMs angenommen werden, daß alle Operatoren vom Rang eins sind und daher die Form $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ haben. Wird die Operation von σ auf den zugehörigen $|\Psi_j\rangle$ betrachtet, so folgt

$$\sigma(g)|\Psi_j\rangle = \phi(g,j)|\Psi_{\pi(g)(j)}\rangle \tag{4.6}$$

mit passenden Phasenfaktoren $\phi(g,j)$, die beim Übergang von $|\Psi_j\rangle$ zu Π_j wieder wegfallen. Die Phasenfaktoren werden mit Gl. (4.6) durch beidseitige Bildung des Skalarprodukts mit dem Vektor $|\Psi_{\pi(g)(j)}\rangle$ bestimmt:

Definition 4.5 (Phasenfaktoren bei POVMs) *Es sei P ein POVM mit den Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ und der Symmetrie (G,σ,π). Dann gilt*

$$\sigma(g)|\Psi_j\rangle = \phi(g,j)|\Psi_{\pi(g)(j)}\rangle \;\; \textit{mit} \;\; \phi(g,j) := \frac{\langle\Psi_{\pi(g)(j)}|\sigma(g)\Psi_j\rangle}{\langle\Psi_{\pi(g)(j)}|\Psi_{\pi(g)(j)}\rangle}.$$

Für Nullvektoren wird $\phi(g,j) := 1$ gesetzt.

Da σ eine Darstellung ist, können für die $\phi(g,j)$ Rechenregeln abgeleitet werden:

Lemma 4.6 (Verknüpfung der Phasenfaktoren) *Für die Phasenfaktoren $\phi(g,j)$ aus Def. 4.5 gilt die Gleichung*

$$\phi(g,\pi(h)(j))\phi(h,j) = \phi(gh,j)\,.$$

Beweis: Ist einer der betreffenden Vektoren null, so müssen aufgrund der Unitarität von σ alle Vektoren null sein, womit alle Phasenfaktoren eins sind. Sind alle Vektoren ungleich null, so sind es auch alle betrachteten Skalarprodukte. Für eine komplexe Zahl $\alpha = \beta/\gamma$ vom Betrag eins gilt $\alpha = \overline{\gamma}/\overline{\beta}$. Damit kann $\phi(h,j)$ als

$$\phi(h,j) = \frac{\langle\Psi_{\pi(h)(j)}|\Psi_{\pi(h)(j)}\rangle}{\langle\sigma(h)\Psi_j|\Psi_{\pi(h)(j)}\rangle} = \frac{\langle\Psi_{\pi(gh)(j)}|\Psi_{\pi(gh)(j)}\rangle}{\langle\sigma(h)\Psi_j|\Psi_{\pi(h)(j)}\rangle}$$

geschrieben werden, denn $|\Psi_{\pi(h)(j)}\rangle$ und $|\Psi_{\pi(gh)(j)}\rangle$ haben dieselbe Länge. Es folgt

$$\phi(g,\pi(h)(j))\phi(h,j) = \frac{\langle\Psi_{\pi(gh)(j)}|\sigma(g)\Psi_{\pi(h)(j)}\rangle}{\langle\sigma(gh)\Psi_j|\sigma(g)\Psi_{\pi(h)(j)}\rangle} = \frac{\langle\Psi_{\pi(gh)(j)}|\Psi_{\pi(gh)(j)}\rangle}{\langle\sigma(gh)\Psi_j|\Psi_{\pi(gh)(j)}\rangle}\,.$$

Durch Anwendung von $\beta/\gamma = \overline{\gamma}/\overline{\beta}$ für $|\beta| = |\gamma|$ folgt die Gleichung des Lemmas. □

Bei der Bildung des Produkts

$$\sigma(g)M = \sum_j \sigma(g)|\Psi_j\rangle\langle j| = (\sigma(g)|\Psi_0\rangle \;\ldots\; \sigma(g)|\Psi_{n-1}\rangle)$$

wird nach Def. 4.5 die Spalte $|\Psi_j\rangle$ auf $\phi(g,j)|\Psi_{\pi(g)(j)}\rangle$ abgebildet, d. h. die Spalten von M werden permutiert und gleichzeitig mit einer Phase multipliziert. Diese Abbildung kann für $g \in G$ auch durch das Produkt $M\sigma_{\mathrm{mon}}(g)$ mit einer Matrix $\sigma_{\mathrm{mon}}(g)$ beschrieben werden, die bis auf Multiplikation der Einträge mit Phasenfaktoren eine Permutationsmatrix ist. Diese Matrix hat also in jeder Spalte und Zeile genau ein nicht verschwindendes Element, womit $\sigma_{\mathrm{mon}}(g)$ eine monomiale Matrix ist (siehe z. B. §43, Kap. VII in [CR62]). Mit σ und σ_{mon} kann eine Symmetrie von M definiert werden:

Lemma 4.7 (Monomiale Darstellung und Symmetrie) *Es sei P ein POVM mit den Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ und der Symmetrie (G, σ, π). Dann hat M die Symmetrie $(G, \sigma, \sigma_{\text{mon}})$ mit der durch*

$$\sigma_{\text{mon}}(g) := \sum_{j=0}^{n-1} \phi(g, j)|\pi(g)(j)\rangle\langle j|$$

definierten unitären Darstellung σ_{mon}. Diese Darstellung ist monomial, d. h. alle $\sigma_{\text{mon}}(g)$ sind monomiale Matrizen.

Beweis: Die Unitarität von σ_{mon} kann durch direktes Nachrechnen gezeigt werden. Die Homomorphie von σ_{mon} folgt mit der Verknüpfungsregel aus Lemma 4.6. Die Symmetrie $(G, \sigma, \sigma_{\text{mon}})$ von M wird durch die Gleichung

$$\begin{aligned} \sigma(g)M\sigma_{\text{mon}}(g)^\dagger &= \sigma(g)\left(\sum_{j=0}^{n-1} |\Psi_j\rangle\langle j|\right)\left(\sum_{j=0}^{n-1} \phi(g, j)|\pi(g)(j)\rangle\langle j|\right)^\dagger \\ &= \sum_{j=0}^{n-1} |\Psi_{\pi(g)(j)}\rangle\langle\pi(g)(j)| \end{aligned}$$

gezeigt, denn die Summe in der letzten Zeile entspricht Gl. (4.4) bis auf eine Permutation der Summationsreihenfolge. □

Die Matrix M und deren Symmetrie werden durch die POVM-Operatoren nicht eindeutig festgelegt, denn jede Spalte von M kann mit einem beliebigen Phasenfaktor multipliziert werden. Diese Multiplikationen entsprechen der Bildung des Produkts $M\Delta$, wobei Δ eine diagonale Phasenmatrix ist. Durch den Übergang von M zu $M\Delta$ wird die Äquivalenzklasse von σ_{mon} nicht verlassen:

Lemma 4.8 (Wechsel der Phasenfaktoren) *Es sei $M \in \mathbb{C}^{d\times n}$ eine Matrix mit der Symmetrie (G, σ, τ). Dann hat für $\Delta \in \mathcal{U}(n)$ die Matrix $M\Delta$ die Symmetrie $(G, \sigma, \Delta^\dagger\tau\Delta)$.*

Beweis: Die Gleichung $\sigma M = M\tau$ kann zu $\sigma M = M\Delta\Delta^\dagger\tau$ umgeformt werden, womit die Aussage des Lemmas durch Multiplikation mit Δ folgt. □

Die Freiheit bei der Wahl der Phasenfaktoren kann genutzt werden, um die Darstellung σ_{mon} so zu wählen, daß sie möglichst einfach in irreduzible Komponenten zerlegt werden kann. Dies ist von Nutzen, falls die Konstruktion von $\tilde{M}$ wie in Abschnitt 2.6 symmetriebasiert durchgeführt werden soll. Grundlage ist hierfür die durch Lemma 2.20 gegebene Symmetrie $\sigma_{\text{mon}}M^\dagger = M^\dagger\sigma$ von $M^\dagger$. Da $M^\dagger$ orthonormale Spalten hat, kann Satz 2.39 angewandt werden, um ein $\tilde{M}$ zu konstruieren, das ebenfalls eine Symmetrie hat:

Satz 4.9 (Durchführung symmetrischer POVMs) *Es sei P ein POVM mit den Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$ und der Symmetrie (G, σ, π). Ferner seien $A \in \mathcal{U}(d)$ und $B \in \mathcal{U}(n)$ Zerlegungsmatrizen der Darstellungen σ bzw. σ_{mon}, d. h. es gilt*

$$A\sigma A^\dagger = \bigoplus_{j=0}^{z-1}(I_{m_k} \otimes \kappa_j) \quad \textit{und} \quad B\sigma_{\text{mon}}B^\dagger = \bigoplus_{j=0}^{z-1}(I_{n_k} \otimes \kappa_j)\,.$$

Dann existiert eine Darstellung $\tilde{\sigma}$, so daß $A\sigma A^\dagger \oplus \tilde{\sigma}$ und $B\sigma_{\text{mon}}B^\dagger$ bis auf die Reihenfolge der irreduziblen Komponenten gleich sind. Ferner existiert eine Matrix $N \in \mathbb{C}^{n\times(n-d)}$, so daß

$$\tilde{M}^\dagger := B^\dagger(BM^\dagger A^\dagger|N)(A \oplus \tilde{A}) = (M^\dagger|B^\dagger N\tilde{A})$$

das POVM für alle $\tilde{A} \in \mathcal{U}(n-d)$ auf die Messung in der Standardbasis reduziert und die Symmetrie $\sigma_{\text{mon}}\tilde{M}^\dagger = \tilde{M}^\dagger(\sigma \oplus \tilde{A}\tilde{\sigma}\tilde{A}^\dagger)$ hat.

Aus dem in Abschnitt 2.6 diskutierten Beweis von Satz 2.39 folgt unmittelbar ein symmetriebasiertes Konstruktionsverfahren für $\tilde{M}$:

- Bestimme eine Symmetrie (G, σ, π) von P
- Finde Zerlegungsmatrizen A und B für σ bzw. σ_{mon}
- Konstruiere $\tilde{\sigma}$ so, daß $A\sigma A^\dagger \oplus \tilde{\sigma}$ und $B\sigma_{\text{mon}}B^\dagger$ bis auf die Reihenfolge der irreduziblen Komponenten gleich sind
- Finde eine Matrix N so, daß $(BM^\dagger A^\dagger|N)$ eine unitäre Ergänzung von $BM^\dagger A^\dagger$ mit der Symmetrie $(G, B\sigma_{\text{mon}}B^\dagger, A\sigma A^\dagger \oplus \tilde{\sigma})$ ist
- Bilde $\tilde{M}^\dagger := B^\dagger(BM^\dagger A^\dagger|N)(A \oplus \tilde{A}) = (M^\dagger|B^\dagger N\tilde{A})$ mit einem unitären $\tilde{A}$

Dieses Verfahren entspricht weitgehend dem in Abschnitt 2.5 diskutierten Zerlegungsverfahren für Matrizen mit Symmetrie; ist das POVM eine orthogonale Messung, so sind beide Verfahren gleich. Der Hauptunterschied für nicht-orthogonale Messungen ist, daß die Matrix im Verkettungsraum der zerlegten Darstellungen nicht direkt in einen Schaltkreis übersetzt werden kann, sondern zuerst unitär ergänzt werden muß. Der Vorteil des Verfahrens im Vergleich zur direkten Ergänzung von M ist, daß sowohl B als auch $A \oplus \tilde{A}$ für einige Darstellungen als Produkt dünn besetzter und strukturierter Matrizen erhalten werden können (siehe Abschnitt 2.5). Darüber hinaus kann in manchen Fällen die Matrix $(BM^\dagger A^\dagger|N)$ aufgrund ihrer Struktur so konstruiert werden, daß diese in einen einfachen Schaltkreis übersetzt werden kann.

4.3 Gruppenerzeugte POVMs

Bei gruppenerzeugten POVMs werden nach Def. 2.15 alle Operatoren ausgehend vom initialen Operator $\Pi = |\Psi\rangle\langle\Psi|$ durch die Operation der Gruppe erhalten. Hierbei können die Vektoren $|\Psi_g\rangle$ der Operatoren $\Pi_g = |\Psi_g\rangle\langle\Psi_g|$ gemäß

$$|\Psi_g\rangle := \sigma(g)|\Psi\rangle \tag{4.7}$$

definiert werden. Mit dieser Wahl ist die monomiale Darstellung aus Lemma 4.7 festgelegt:

Lemma 4.10 (Gruppenerzeugtes POVM) *Es sei P ein gruppenerzeugtes POVM mit dem initialen Operator Π und der Darstellung σ der Gruppe G, wobei $g_0, \ldots, g_{n-1}$ die Anordnung der Gruppenelemente sei. Werden den Operatoren die Vektoren $|\Psi_g\rangle$ aus Gl. (4.7) zugeordnet, so hat M aus Gl. (4.4) die Symmetrie $(G, \sigma, \sigma_{\text{mon}})$, wobei σ_{mon} der regulären Darstellung von G entspricht.*

Beweis: Es seien $g_0, \ldots, g_{n-1}$ die Elemente von G in einer festen Reihenfolge. Zur Vereinfachung der Notation sei ferner $|\Psi_j\rangle := |\Psi_{g_j}\rangle$. Es gilt damit

$$\sigma(h)|\Psi_j\rangle = \sigma(h)\sigma(g_j)|\Psi\rangle = \sigma(g_{\pi(h)(j)})|\Psi\rangle = |\Psi_{\pi(h)(j)}\rangle$$

mit der Darstellung π von Def. 2.5. Nach Def. 4.5 folgen die Phasenfaktoren

$$\phi(h,j) = \frac{\langle\Psi_{\pi(h)(j)}|\sigma(h)\Psi_j\rangle}{\langle\Psi_{\pi(h)(j)}|\Psi_{\pi(h)(j)}\rangle} = \frac{\langle\Psi_{\pi(h)(j)}|\sigma(hg_j)\Psi\rangle}{\langle\Psi_{\pi(h)(j)}|\Psi_{\pi(h)(j)}\rangle} = 1.$$

Damit ist $\sigma_{\text{mon}}(g) = \sum_j |\pi(h)(j)\rangle\langle j|$ nach Def. 2.5 die reguläre Darstellung von G. □

Die reguläre Darstellung einer Gruppe wird nach Def. 2.8 durch die allgemeine Fourier-Transformation in ihre irreduziblen Bestandteile zerlegt. Mit der Notation von Satz 4.9 entspricht diese daher der Matrix B. Da bei einigen Gruppen effiziente Schaltkreise für die Fourier-Transformation bekannt sind (siehe z. B. [Bea97, MRR04] oder Kap. 3 in [Röt01]), ist in diesen Fällen bei der Zerlegung

$$\tilde{M}^\dagger = B^\dagger(BM^\dagger A^\dagger|N)(A \oplus \tilde{A})$$

das Teilproblem, wie $B^\dagger$ effizient implementiert werden kann, gelöst.

4.4 Beispiele

In diesem Abschnitt werden mit dem durch Satz 4.9 bereitgestellten Verfahren unitäre Transformationen für einige Beispiele symmetrischer POVMs konstruiert: Für Qubits werden zwei POVMs untersucht, die Platonischen Körpern in der Bloch-Kugel entsprechen. Für ein dreidimensionales System wird das Computeralgebrasystem GAP genutzt, um die Durchführung eines POVMs zu vereinfachen. Darüber hinaus werden für höherdimensionale Systeme zwei Familien von POVMs betrachtet: Die erste Familie hat eine zyklische Symmetrie, die zweite die Heisenberg-Weyl-Symmetrie. Bei beiden Familien werden effiziente Schaltkreise zur Durchführung der Messungen erhalten. Zur Vereinfachung der Notation bei den Untersuchungen beider Familien werden zunächst die Schiebe- und Phasenmatrizen definiert:

Definition 4.11 (Schiebe- und Phasenmatrix) *Die Matrizen X_d und Z_d sind für d-dimensionale Systeme durch*

$$X_d := \sum_{j=0}^{d-1} |(j+1) \bmod d\rangle\langle j| \quad \textit{und} \quad Z_d := \sum_{j=0}^{d-1} \omega_d^j |j\rangle\langle j|$$

definiert, wobei $\omega_d := e^{2\pi i/d}$ eine d-te Einheitswurzel ist. Die Matrix X_d ist die zyklische Schiebematrix, und die Matrix Z_d ist die Phasenmatrix.

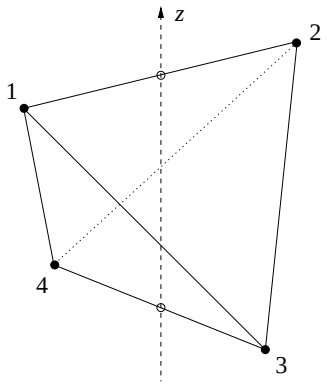

Abbildung 4.1: Das Tetraeder mit zwei Kanten, die zur z-Achse orthogonal sind. Durch diese Anordnung entsprechen die Ecken den Zustandsvektoren (4.8). (Abbildung aus [DJB04] übernommen.)

4.4.1 Platonische Körper

Der Zustand eines Qubits entspricht in der Bloch-Kugel einem Punkt, der eine Richtung im Raum festlegt. Werden geeignete Richtungen präpariert, übertragen und gemessen, so ist es möglich, daß zwischen Sender und Empfänger ein gemeinsames räumliches Bezugssystem hergestellt wird (siehe z. B. [PS02b, PS02a]). Da für den Empfänger das Problem symmetrisch ist, d. h. vor der Übertragung der Zustände gibt es für ihn keine ausgezeichneten Richtungen, ist es sinnvoll, daß er Messungen nutzt, die bezüglich aller Drehungen im dreidimensionalen Raum der Bloch-Kugel symmetrisch sind. Steht dem Empfänger zur Messung ein Quantenrechner zur Verfügung, so sind nur Messungen mit endlich vielen verschiedenen Resultaten möglich, womit eine Approximation der drehsymmetrischen Messung erreicht werden kann. Zur Vereinfachung der Meßverfahren kann auch bei diesen Messungen eine Symmetrie gefordert werden; hierbei stehen neben den zyklischen Gruppen und den Diedergruppen die Symmetriegruppen der Platonischen Körper (siehe Abschnitt 1.8 in [Ste94]) zur Verfügung. Es gibt fünf Platonische Körper: das Tetraeder, den Würfel, das Okta-, Dodeka- und Ikosaeder. Allen ist gemein, daß sie eine Drehsymmetrie haben, bezüglich derer sie in Bahnen zerfallen, wobei alle Bahnen eines Körpers gleich viele Elemente umfassen. Das Tetraeder, der Würfel und das Oktaeder zerfallen hierbei in zwei Bahnen, das Dodeka- und Ikosaeder hingegen in vier. Unter Nutzung dieser Symmetrie wird für jeweils einen Vertreter dieser Fälle, das Tetra- und das Dodekaeder, ein Schaltkreis zur Durchführung des POVMs konstruiert, dessen Operatoren den Ecken des Platonischen Körpers in der Bloch-Kugel entsprechen. Die Schaltkreise zur Durchführung der POVMs, die zu den anderen Platonischen Körpern gehören, können in [DJB04] gefunden werden.

Das Tetraeder

Das Tetraeder ist der Platonische Körper mit vier Ecken, vier Flächen sowie sechs Kanten. Es kann so skaliert und gedreht werden, daß die Ecken auf der Oberfläche der Bloch-Kugel

liegen und zu den Zustandsvektoren

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix},\ \begin{pmatrix} \tilde{\alpha} \\ -\tilde{\beta} \end{pmatrix},\ \begin{pmatrix} \tilde{\beta} \\ \tilde{\alpha} i \end{pmatrix}\ \text{sowie}\ \begin{pmatrix} \tilde{\beta} \\ -\tilde{\alpha} i \end{pmatrix} \tag{4.8}$$

mit den beiden Werten

$$\tilde{\alpha} := \sqrt{\frac{3+\sqrt{3}}{6}} \quad \text{und} \quad \tilde{\beta} := \sqrt{\frac{3-\sqrt{3}}{6}}$$

gehören. In Abb. 4.1 entsprechen dem ersten und zweiten Vektorenpaar aus Zeile (4.8) die Ecken 1 und 2 bzw. 3 und 4. Werden zu den vier Zustandsvektoren die Operatoren gebildet, so folgt deren Summe

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} (\tilde{\alpha}, \tilde{\beta}) + \begin{pmatrix} \tilde{\alpha} \\ -\tilde{\beta} \end{pmatrix} (\tilde{\alpha}, -\tilde{\beta}) + \begin{pmatrix} \tilde{\beta} \\ \tilde{\alpha} i \end{pmatrix} (\tilde{\beta}, -\tilde{\alpha} i) + \begin{pmatrix} \tilde{\beta} \\ -\tilde{\alpha} i \end{pmatrix} (\tilde{\beta}, \tilde{\alpha} i) = 2\, I_2\,,$$

die zeigt, daß die Vektoren $|\Psi_j\rangle$ bis auf einen skalaren Faktor ein POVM definieren:

Definition 4.12 (Tetraeder-POVM) *Das Tetraeder-POVM auf einem Qubit umfaßt die vier durch*

$$|\Psi_0\rangle := \begin{pmatrix} \alpha \\ \beta \end{pmatrix},\ |\Psi_1\rangle := \begin{pmatrix} \alpha \\ -\beta \end{pmatrix},\ |\Psi_2\rangle := \begin{pmatrix} \beta \\ \alpha i \end{pmatrix}\ \textit{und}\ |\Psi_3\rangle := \begin{pmatrix} \beta \\ -\alpha i \end{pmatrix}$$

festgelegten Operatoren $\Pi_j := |\Psi_j\rangle\langle\Psi_j|$ *für*

$$\alpha := \sqrt{\frac{3+\sqrt{3}}{12}} \quad \textit{und} \quad \beta := \sqrt{\frac{3-\sqrt{3}}{12}}\,.$$

Eine unitäre Transformation, die das POVM durchführt, wird nach Abschnitt 4.1 durch die Ergänzung der Matrix

$$M = \sum_{j=0}^{3} |\Psi_j\rangle\langle j| = \begin{pmatrix} \alpha & \alpha & \beta & \beta \\ \beta & -\beta & \alpha i & -\alpha i \end{pmatrix} \in \mathbb{C}^{2\times 4}$$

aus Gl. (4.4) gefunden, die beim Tetraeder-POVM eine Symmetrie hat, da das Tetraeder von Abb. 4.1 unter der 180°-Drehung um die z-Achse invariant ist. Bei dieser Drehung wird jeder Vektor $|\Psi_j\rangle$ mit $\mathrm{diag}(1,-1)$ multipliziert, womit die Symmetrie $\sigma M = M\sigma_{\mathrm{mon}}$ mit den beiden durch

$$\sigma(r) := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{und} \quad \sigma_{\mathrm{mon}}(r) := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

definierten Darstellungen der Gruppe $C_2 := \langle r : r^2 = 1\rangle$ folgt. Zur Konstruktion der Ergänzung von M werden nach dem Verfahren von Abschnitt 4.2 sowohl σ als auch σ_{mon} in irreduzible Komponenten zerlegt. Da dies bei σ schon der Fall ist, kann mit der

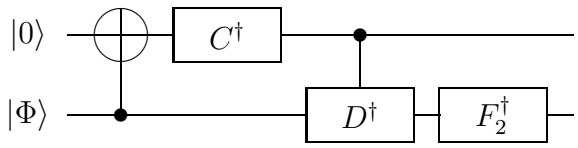

Abbildung 4.2: Ein Schaltkreis für das Tetraeder-POVM. Die beiden Gatter C und D werden in Gl. (4.10) definiert. (Schaltkreis aus [DJB04] übernommen.)

Notation von Satz 4.9 die Zerlegungsmatrix $A := I_2$ gewählt werden. Die Darstellung σ_{mon} wird hingegen durch $B := I_2 \otimes F_2$ zerlegt, da hierbei die Fourier-Transformation F_2 auf die durch $r \mapsto \sigma_x$ gegebene reguläre Darstellung von C_2 angewandt wird (siehe Bsp. 2.9). Es folgt

$$AMB^\dagger = \sqrt{2} \begin{pmatrix} \alpha & 0 & \beta & 0 \\ 0 & \beta & 0 & \alpha i \end{pmatrix} \in \text{Int}(\sigma, \sigma \oplus \sigma)\,,$$

da $B\sigma_{\text{mon}}B^\dagger = \sigma \oplus \sigma$ gilt. Wird die Darstellung σ durch die Darstellung $\tilde{\sigma} := \sigma$ zu $\sigma \oplus \sigma$ ergänzt, so kann gleichzeitig $AMB^\dagger$ um zwei orthogonale Zeilen zu

$$\tilde{W} := \sqrt{2} \begin{pmatrix} \alpha & 0 & \beta & 0 \\ 0 & \beta & 0 & \alpha i \\ \beta & 0 & -\alpha & 0 \\ 0 & \alpha & 0 & -\beta i \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} (C \otimes I_2)(I_2 \oplus D) \tag{4.9}$$

mit der Symmetrie $(\sigma \oplus \sigma)\tilde{W} = \tilde{W}(\sigma \oplus \sigma)$ erweitert werden, wobei

$$C := \begin{pmatrix} \tilde{\alpha} & \tilde{\beta} \\ \tilde{\beta} & -\tilde{\alpha} \end{pmatrix} \quad \text{und} \quad D := \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \tag{4.10}$$

genutzt werden. Für $\tilde{A} := I_2$ folgt nach Abschnitt 4.2 die Ergänzung

$$\tilde{M} := (A^\dagger \oplus \tilde{A})\tilde{W}B = \begin{pmatrix} \alpha & \alpha & \beta & \beta \\ \beta & -\beta & \alpha i & -\alpha i \\ \beta & \beta & -\alpha & -\alpha \\ \alpha & -\alpha & -\beta i & \beta i \end{pmatrix} \tag{4.11}$$

von M, womit die Matrix $\tilde{A}$ so gewählt wird, daß $A \oplus \tilde{A} = I_4$ gilt. Die Zerlegungen von Gl. (4.9) und (4.11) können unmittelbar in einen Schaltkreis übersetzt werden: Die (4×4)-Permutationsmatrix aus Gl. (4.9) entspricht einem CNOT-Gatter auf dem ersten Qubit, das durch das zweite Qubit gesteuert wird; die Diagonalmatrix $I_2 \oplus D$ wird durch eine vom ersten Qubit gesteuerte Operation erhalten.

Satz 4.13 (Aufwand des Tetraeder-POVMs) *Das Tetraeder-POVM wird mit dem Schaltkreis von Abb. 4.2 durchgeführt. Dieser kann in fünf Ein-Qubit- und drei CNOT-Gatter zerlegt werden.*

Beweis: Die gesteuerte Operation D in Abb. 4.2 kann durch drei Ein-Qubit- und zwei CNOT-Gatter ersetzt werden (siehe Lemmata 5.2 und 5.4 in [BBC$^+$95]). □

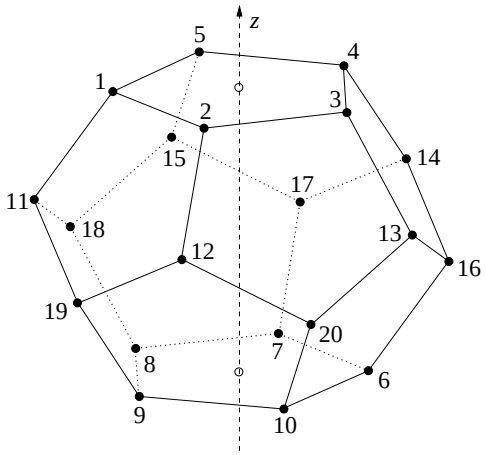

Abbildung 4.3: Das Dodekaeder mit zwei zu der z-Achse orthogonalen Flächen. Durch diese Anordnung entsprechen die Ecken den Zustandsvektoren (4.12). (Abbildung aus [DJB04] übernommen.)

Die Konstruktion, die zu dem Schaltkreis in Abb. 4.2 führt, nutzt nur die zyklische Symmetriegruppe C_2, wohingegen die Gruppe aller Drehungen des Tetraeders zur alternierenden Gruppe

$$A_4 := \langle (0\,1\,2), (0\,1\,3) \rangle$$

isomorph ist, welche die zwölf Permutationen von vier Elementen mit positivem Signum umfaßt (siehe Abschnitt 5.4.1 in [FS92]). Der Vorteil der Einschränkung auf die Untergruppe C_2 ist, daß hierbei die Darstellung σ_{mon} allein durch $I_2 \otimes F_2$ zerlegt werden kann, während $\text{Int}(\sigma \oplus \sigma, \sigma \oplus \sigma)$ schon ein einfach implementierbares $\tilde{W}$ enthält.

Das Dodekaeder

Das Dodekaeder hat 20 Ecken, zwölf Flächen und 30 Kanten. Liegt es in der Bloch-Kugel mit einer geeigneten Größe und Anordnung, entsprechen die Ecken den Zustandsvektoren

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta}\omega_5^j \end{pmatrix}, \begin{pmatrix} \tilde{\beta} \\ -\tilde{\alpha}\omega_5^j \end{pmatrix}, \begin{pmatrix} \tilde{\gamma} \\ \tilde{\delta}\omega_5^j \end{pmatrix} \text{ und } \begin{pmatrix} \tilde{\delta} \\ -\tilde{\gamma}\omega_5^j \end{pmatrix} \quad \text{für} \quad j \in \{0, \ldots, 4\}, \tag{4.12}$$

wobei $\omega_5 := e^{2\pi i/5}$ eine fünfte Einheitswurzel ist und die Werte

$$\tilde{\alpha} := \sqrt{\frac{1}{2} + \frac{1}{30}\sqrt{75 + 30\sqrt{5}}}, \quad \tilde{\beta} := \sqrt{\frac{1}{2} - \frac{1}{30}\sqrt{75 + 30\sqrt{5}}}$$

sowie

$$\tilde{\gamma} := \sqrt{\frac{1}{2} + \frac{1}{30}\sqrt{75 - 30\sqrt{5}}}, \quad \tilde{\delta} := \sqrt{\frac{1}{2} - \frac{1}{30}\sqrt{75 - 30\sqrt{5}}}$$

genutzt werden (siehe Abschnitt 9 in [DJB04]). In Abb. 4.3 entsprechen dem ersten Typ von Vektoren (4.12) die Punkte 1–5, den anderen jeweils die Punkte 6–10, 11–15 und 16-20. Werden zu den Zustandsvektoren die Operatoren gebildet, so zeigt deren Summe

$$\sum_{j=0}^{4} \begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta}\omega_5^j \end{pmatrix} (\tilde{\alpha}, \tilde{\beta}\omega_5^{-j}) + \ldots + \sum_{j=0}^{4} \begin{pmatrix} \tilde{\delta} \\ \tilde{\gamma}\omega_5^j \end{pmatrix} (\tilde{\delta}, \tilde{\gamma}\omega_5^{-j}) = 10\, I_2\,,$$

daß die Vektoren durch Multiplikation mit dem Faktor $\sqrt{1/10}$ zu einem POVM führen:

Definition 4.14 (Dodekaeder-POVM) *Das Dodekaeder-POVM auf einem Qubit besteht aus den zwanzig Operatoren* $\Pi_{j,k} := |\Psi_{j,k}\rangle\langle\Psi_{j,k}|$*, die durch*

$$|\Psi_{j,0}\rangle := \begin{pmatrix} \alpha \\ \beta\omega_5^j \end{pmatrix}, |\Psi_{j,1}\rangle := \begin{pmatrix} \beta \\ -\alpha\omega_5^j \end{pmatrix}, |\Psi_{j,2}\rangle := \begin{pmatrix} \gamma \\ \delta\omega_5^j \end{pmatrix} \quad \textit{und} \quad |\Psi_{j,3}\rangle := \begin{pmatrix} \delta \\ -\gamma\omega_5^j \end{pmatrix}$$

definiert werden mit den Werten

$$\alpha := \frac{\tilde{\alpha}}{\sqrt{10}}, \quad \beta := \frac{\tilde{\beta}}{\sqrt{10}}, \gamma := \frac{\tilde{\gamma}}{\sqrt{10}} \quad \textit{sowie} \quad \delta := \frac{\tilde{\delta}}{\sqrt{10}}\,.$$

Nach Def. 4.1 wird das POVM durch eine unitäre Ergänzung $\tilde{M} \in \mathcal{U}(20)$ von

$$M = \left(\begin{array}{cccc|ccc|ccc|cccc} \alpha & \alpha & \dots & \alpha & \beta & \dots & \beta & \gamma & \dots & \gamma & \delta & \delta & \dots & \delta \\ \beta & \beta\omega_5 & \dots & \beta\omega_5^4 & -\alpha & \dots & -\alpha\omega_5^4 & \delta & \dots & \delta\omega_5^4 & -\gamma & -\gamma\omega_5 & \dots & -\gamma\omega_5^4 \end{array}\right)$$

aus Gl. (4.4) durchgeführt. Wie beim Tetraeder-POVM folgt aus der Symmetrie des Platonischen Körpers eine Symmetrie von M: Das Dodekaeder in Abb. 4.3 ist invariant unter der 72°-Drehung um die z-Achse; bei den Zustandsvektoren entspricht diese Drehung der Multiplikation mit $\mathrm{diag}(1, \omega_5) \in \mathcal{U}(2)$. Die dadurch entstehende Symmetrie $\sigma M = M\sigma_{\mathrm{mon}}$ von M wird hierbei mit den durch

$$\sigma(r) := \begin{pmatrix} 1 & 0 \\ 0 & \omega_5 \end{pmatrix} \quad \text{und} \quad \sigma_{\mathrm{mon}}(r) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

festgelegten Darstellungen der Gruppe $C_5 := \langle r : r^5 = 1\rangle$ beschrieben. Zur Konstruktion von $\tilde{M}$ werden gemäß Abschnitt 4.2 die Darstellungen σ und σ_{mon} zunächst in irreduzible Komponenten zerlegt. Da σ bereits zerlegt ist, kann mit der Notation von Satz 4.9 die Matrix $A := I_2$ gewählt werden. Für σ_{mon} folgt hingegen $B := I_4 \otimes F_5$, da σ_{mon} viermal die reguläre Darstellung von C_5 enthält und diese jeweils durch F_5 zerlegt werden (siehe Bsp. 2.9). Durch $I_4 \otimes F_5$ wird σ_{mon} in

$$I_4 \otimes \kappa = \kappa \oplus \kappa \oplus \kappa \oplus \kappa \quad \text{mit} \quad \kappa := \kappa_0 \oplus \kappa_1 \oplus \kappa_2 \oplus \kappa_3 \oplus \kappa_4 \tag{4.13}$$

transformiert, wobei die fünf irreduziblen Darstellungen κ_j von C_5 durch $\kappa_j(r^k) := (\omega_5^{jk})$ festgelegt sind. Bezeichnet $\tilde{\sigma} := \kappa_2 \oplus \kappa_3 \oplus \kappa_4 \oplus \kappa \oplus \kappa \oplus \kappa$ die Darstellung, die durch Streichung der ersten beiden Komponenten von $I_4 \otimes \kappa$ aus Gl. (4.13) hervorgeht, so gilt $\sigma \oplus \tilde{\sigma} = B\sigma_{\mathrm{mon}}B^\dagger$, womit die nach Abschnitt 4.2 notwendige Ergänzung von σ gefunden ist. Gleichzeitig kann

$$AMB^\dagger = \sqrt{5}\begin{pmatrix} \alpha & 0 & 0 & 0 & 0 & \beta & 0 & 0 & 0 & 0 & \gamma & 0 & 0 & 0 & 0 & \delta & 0 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 & 0 & 0 & -\alpha & 0 & 0 & 0 & 0 & \delta & 0 & 0 & 0 & 0 & -\gamma & 0 & 0 & 0 \end{pmatrix}$$

zu der unitären Matrix

$$\tilde{W} := Q\,(C \otimes I_5) \in \mathcal{U}(20)$$

mit der Symmetrie $(I_4 \otimes \kappa)\tilde{W} = \tilde{W}(I_4 \otimes \kappa)$ erweitert werden, wobei

$$C := \sqrt{5} \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & -\alpha & \delta & -\gamma \\ \gamma & -\delta & -\alpha & \beta \\ \delta & \gamma & -\beta & -\alpha \end{pmatrix} \in \mathcal{U}(4) \tag{4.14}$$

gilt und $Q \in \mathcal{U}(20)$ eine beliebige Permutationsmatrix ist, welche für $x \in \{0, \ldots, 4\}$ die Zeilen $x, x+5, x+10$ und $x+15$ miteinander vertauscht sowie die Zeilen 0 und 6 auf die Zeilen 0 bzw. 1 abbildet. Die Matrix C geht aus der Matrix

$$\begin{pmatrix} \alpha & \beta & \gamma & \delta \\ \beta & -\alpha & \delta & -\gamma \end{pmatrix} \in \mathbb{C}^{2\times 4}$$

durch eine unitäre Ergänzung hervor. Die Ergänzung $\tilde{M}$ von M wird nach Satz 4.9 durch die Basistransformation $\tilde{M} = (A^\dagger \oplus \tilde{A})\tilde{W}B$ erhalten, wobei $\tilde{A} \in \mathcal{U}(18)$ eine beliebige unitäre Matrix ist. Durch die Wahl $\tilde{A} := I_{18}$ kann hierbei $A \oplus \tilde{A} = I_{20}$ erhalten werden:

Satz 4.15 (Durchführung des Dodekaeder-POVMs) *Das Dodekaeder-POVM kann mit der unitären Transformation*

$$\tilde{M} := (A^\dagger \oplus \tilde{A})\tilde{W}B = Q(C \otimes F_5) \tag{4.15}$$

durchgeführt werden, wobei C in Gl. (4.14) definiert ist und Q die erste Zeile von $C \otimes F_5$ festhält und die siebte auf die zweite abbildet.

Zur Durchführung des Dodekaeder-POVMs auf einem Qubit-Register muß die Matrix $\tilde{M} \in \mathcal{U}(20)$ zu einer unitären (32×32)-Matrix $\tilde{M}_{32}$ erweitert werden. Hierzu kann beispielsweise F_5 von Gl. (4.15) durch die Matrix $(F_5 \oplus I_3) \in \mathcal{U}(8)$ ersetzt werden, falls gleichzeitig Q durch eine Permutationsmatrix $Q_{32} \in \mathcal{U}(32)$ ersetzt wird, die

$$Q_{32}|00000\rangle = |00000\rangle \quad \text{und} \quad Q_{32}|01001\rangle = |00001\rangle \tag{4.16}$$

in der Qubitnotation erfüllt. Eine einfach implementierbare Matrix, welche diese Bedingungen erfüllt, ist durch das CNOT auf dem zweiten Qubit gegeben, das vom letzten gesteuert wird. Die resultierende Matrix $\tilde{M}_{32}$ führt das um zwölf Nulloperatoren erweiterte Dodekaeder-POVM durch. Da die zusätzlichen Resultate nie auftreten, verändert diese Erweiterung das POVM nicht wesentlich.

Korollar 4.16 (Dodekaeder-POVM auf Qubit-Register) *Das Dodekaeder-POVM kann auf einem Qubit-Register mit der Matrix*

$$\tilde{M}_{32}^\dagger := \left(C^\dagger \otimes \left(F_5^\dagger \oplus I_3\right)\right) Q_{32}^\dagger$$

auf die Messung in der Standardbasis reduziert werden. Hierbei sind C und Q_{32} durch Gl. (4.14) bzw. (4.16) festgelegt.

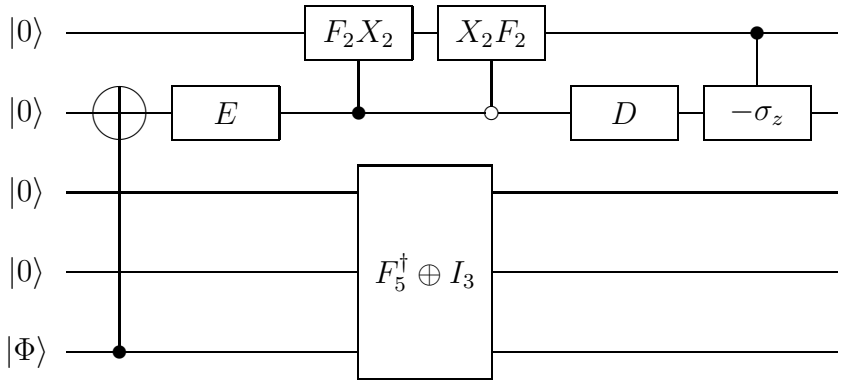

Abbildung 4.4: Ein Schaltkreis zur Implementierung des Dodekaeder-POVMs. Die Matrizen D und E werden in Gl. (4.17) definiert. Das Symbol $\circ$ bedeutet, daß auf der Steuerleitung vor und nach dem Gatter eine σ_x-Operation ausgeführt wird. (Schaltkreis aus [DJB04] übernommen.)

Die Zuordnung der POVM-Operatoren $|\Psi_{j,k}\rangle\langle\Psi_{j,k}|$ und der Resultate bei der Messung in der Standardbasis sind in der folgenden Tabelle zusammengefaßt:

$\|\Psi_{0,0}\rangle$	00000	$\|\Psi_{0,1}\rangle$	01000	$\|\Psi_{0,2}\rangle$	10000	$\|\Psi_{0,3}\rangle$	11000
$\|\Psi_{1,0}\rangle$	00001	$\|\Psi_{1,1}\rangle$	01001	$\|\Psi_{1,2}\rangle$	10001	$\|\Psi_{1,3}\rangle$	11001
$\|\Psi_{2,0}\rangle$	00010	$\|\Psi_{2,1}\rangle$	01010	$\|\Psi_{2,2}\rangle$	10010	$\|\Psi_{2,3}\rangle$	11010
$\|\Psi_{3,0}\rangle$	00011	$\|\Psi_{3,1}\rangle$	01011	$\|\Psi_{3,2}\rangle$	10011	$\|\Psi_{3,3}\rangle$	11011
$\|\Psi_{4,0}\rangle$	00100	$\|\Psi_{4,1}\rangle$	01100	$\|\Psi_{4,2}\rangle$	10100	$\|\Psi_{4,3}\rangle$	11100

Der zu $\tilde{M}_{32}^\dagger$ gehörende Schaltkreis ist in Abb. 4.4 dargestellt. Die Matrix $C^\dagger$, die auf den oberen beiden Qubits operiert, wird hierbei als Produkt

$$C^\dagger = (I_2 \oplus (-\sigma_z))\,(I_2 \otimes D)\,R\,(I_2 \otimes E)$$

geschrieben, wobei die Matrizen

$$D := \begin{pmatrix} u_- & -u_+ \\ u_+ & u_- \end{pmatrix} \quad \text{und} \quad E := \begin{pmatrix} v_- & v_+ \\ v_+ & -v_- \end{pmatrix} \tag{4.17}$$

für die Werte

$$u_\pm := \sqrt{\frac{1}{2} \pm \sqrt{\frac{3+\sqrt{5}}{24}}} \quad \text{und} \quad v_\pm := \mp\sqrt{\frac{1}{2} \pm \sqrt{\frac{\sqrt{5}-1}{8\sqrt{5}}}}$$

genutzt werden. Ferner ist die Matrix R das Produkt

$$R := \sqrt{\frac{1}{2}} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & \sqrt{2} \end{pmatrix} \sqrt{\frac{1}{2}} \begin{pmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & \sqrt{2} & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}. \tag{4.18}$$

In Abb. 4.4 entsprechen die beiden Matrizen dieses Produkts den zwei Operationen auf dem ersten Qubit, die vom zweiten gesteuert werden. Die eingebettete Fourier-Transformation $F_5 \oplus I_3$ kann wie in Anhang B.2 in einen Schaltkreis überführt werden, womit der Aufwand des Dodekaeder-POVMs abgeschätzt werden kann:

Satz 4.17 (Aufwand des Dodekaeder-POVMs) *Das Dodekaeder-POVM kann mit dem Schaltkreis von Abb. 4.4 durchgeführt werden. Dieser kann in* 54 *Ein-Qubit- und* 38 *CNOT-Gatter zerlegt werden.*

Beweis: Nach Satz B.3 werden für $F_5^\dagger \oplus I_3$ höchstens 44 Ein-Qubit- und 32 CNOT-Gatter benötigt. Wird der negierte Eingang von X_2F_2 durch zwei σ_x-Gatter in einen normalen Eingang überführt, so können nach Lemma 5.4 in [BBC$^+$95] die gesteuerten Operationen X_2F_2 und F_2X_2 jeweils durch zwei Ein-Qubit- und zwei CNOT-Gatter ersetzt werden. Das Gatter $-\sigma_z$ kann nach Lemma 5.5 in [BBC$^+$95] durch zwei Ein-Qubit- und ein CNOT-Gatter ersetzt werden. □

Die volle Symmetriegruppe des Dodekaeders ist zu der alternierenden Gruppe A_5 isomorph, welche die sechzig Permutationen von fünf Elementen mit positivem Signum umfaßt (siehe Kapitel 21 in [Ter99]). Wie bei dem Tetraeder-POVM bildet eine zyklische Gruppe die Grundlage der Konstruktion des Schaltkreises. Wie Satz 4.17 zeigt, reicht schon diese zyklische Untergruppe aus, um einen einfachen Schaltkreis für das Dodekaeder-POVM zu erhalten, denn im Vergleich dazu benötigt z. B. das in [VMS04] dargestellte Verfahren zur Konstruktion von Schaltkreisen für beliebige Transformationen bei fünf Qubits bis zu 3228 Ein-Qubit- und 4156 CNOT-Gatter.

4.4.2 POVM zu einer alternierenden Gruppe

Anhand eines POVMs auf einem dreidimensionalen System kann untersucht werden, wie die im Paket AREP des Computeralgebrasystems GAP (siehe [S$^+$97]) implementierten symmetriebasierten Zerlegungsverfahren für Darstellungen die Durchführung eines POVMs vereinfachen. Als Symmetriegruppe wird hierbei die alternierende Gruppe

$$A_4 := \langle (0\,1\,2), (0\,1\,3) \rangle$$

mit der durch

$$\sigma((0\,1\,2)) := \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} \quad \text{und} \quad \sigma((0\,1\,3)) := \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$$

definierten Darstellung $\sigma : A_4 \to \mathcal{U}(3)$ zugrunde gelegt. Da σ irreduzibel ist, führt jeder initiale Operator mit einer geeigneten Normierung zu einem POVM (siehe Abschnitt 2.3):

Definition 4.18 (Alternierendes POVM) *Es sei* $|\Psi\rangle := (\alpha, \beta, \gamma)^T \in \mathbb{C}^3$ *ein Vektor mit* $\langle\Psi|\Psi\rangle = 1/4$. *Dann definieren die zwölf Operatoren* $\Pi_g := \sigma(g)|\Psi\rangle\langle\Psi|\sigma(g)^\dagger$ *mit* $g \in A_4$ *ein POVM. Zur Vereinfachung wird dieses als alternierendes POVM bezeichnet.*

Für das alternierende POVM folgt mit der Anordnung

j	g_j	j	g_j	j	g_j
0	id	4	(1 2 3)	8	(1 3 2)
1	(0 1)(2 3)	5	(0 2 1)	9	(0 3 1)
2	(0 2)(1 3)	6	(0 3 2)	10	(0 1 2)
3	(0 3)(1 2)	7	(0 1 3)	11	(0 2 3)

der Gruppenelemente nach Gl. (4.4) die Matrix

$$M := \begin{pmatrix} \alpha & \alpha & -\alpha & -\alpha & \beta & \beta & -\beta & -\beta & \gamma & \gamma & -\gamma & -\gamma \\ \beta & -\beta & \beta & -\beta & \gamma & -\gamma & \gamma & -\gamma & \alpha & -\alpha & \alpha & -\alpha \\ \gamma & -\gamma & -\gamma & \gamma & \alpha & -\alpha & -\alpha & \alpha & \beta & -\beta & -\beta & \beta \end{pmatrix} \in \mathbb{C}^{3\times 12}\,.$$

Nach Lemma 4.10 hat M die Symmetrie $\sigma M = M\sigma_{\text{mon}}$ mit der regulären Darstellung σ_{mon} von A_4. Ähnlich wie bei AREP kann zur Vereinfachung $[d,\pi]$ mit $\pi \in S_d$ für die $(d\times d)$-Permutationsmatrix geschrieben werden, welche an den Positionen $(j,\pi(j))$ die Einsen hat. Werden darüber hinaus wie bei GAP die Zykel gemäß $(0\ 1)(1\ 2) = (0\ 2\ 1)$ verknüpft, so gilt die Rechenregel $[d,\pi][d,\tilde{\pi}] = [d,\pi\tilde{\pi}]$. Für das alternierende POVM folgen mit dieser Notation

$$\sigma_{\text{mon}}((0\ 1\ 2)) = [3,(0\ 1\ 2)]\otimes[4,(0\ 1\ 2)] \quad \text{und} \quad \sigma_{\text{mon}}((0\ 1\ 3)) = [3,(0\ 2\ 1)]\otimes[4,(0\ 1\ 3)]\,.$$

Mit AREP wird für σ_{mon} die Zerlegungsmatrix

$$B := (F_3\oplus I_9)[12,\pi_0](I_3\otimes F_2\otimes F_2)[12,\pi_1] \in \mathcal{U}(12)$$

berechnet, wobei die beiden Permutationen

$$\pi_0 = (1\ 4\ 7)(2\ 8\ 5\ 11)(6\ 9) \ \text{ und } \ \pi_1 = (0\ 11\ 4\ 3\ 9\ 6)(1\ 8\ 7\ 2\ 10\ 5)$$

genutzt werden. Mit der Permutation $\pi_2 := (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8)$ kann B auch als

$$B = (F_3\oplus I_9)[12,\pi_0][12,\pi_2](F_2\otimes F_2\otimes I_3)[12,\pi_2]^\dagger[12,\pi_1] \in \mathcal{U}(12) \tag{4.19}$$

geschrieben werden; hierbei wird die Reihenfolge der Komponenten in $I_3\otimes F_2\otimes F_2$ umgekehrt, womit bei den weiteren Konstruktionen Vereinfachungen erhalten werden. Die Darstellung σ_{mon} zerfällt durch B in die direkte Summe

$$B\sigma_{\text{mon}}B^\dagger = \kappa_0\oplus\kappa_1\oplus\kappa_2\oplus\kappa_3\oplus\kappa_3\oplus\kappa_3$$

der irreduziblen Darstellungen κ_j. Für die eindimensionalen κ_0, κ_1 und κ_2 gelten

$$\kappa_j((0\,1\,2)) := (\omega_3^{2j}) \quad \text{sowie} \quad \kappa_j((0\,1\,3)) := (\omega_3^{j})\,,$$

wobei $\omega_3 := e^{2\pi i/3}$ eine dritte Einheitswurzel ist. Ferner wird durch

$$\kappa_3((0\ 1\ 2)) := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{und} \quad \kappa_3((0\ 1\ 3)) := \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

die einzige höherdimensionale irreduzible Darstellung von A_4 festgelegt. Diese ist aber aufgrund der durch AREP berechneten Matrix B nicht die Darstellung σ, sondern nur zu dieser äquivalent. Zur Angleichung beider Darstellungen wird mit AREP die Matrix

$$A := \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

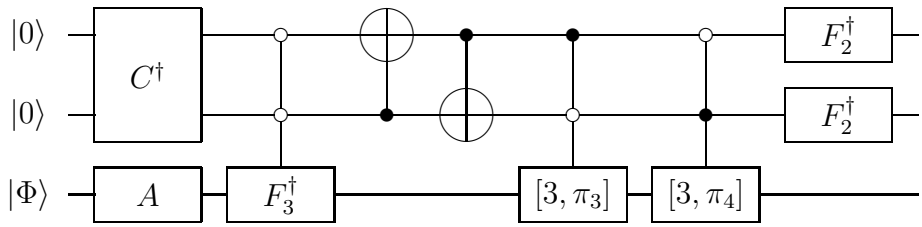

Abbildung 4.5: Schaltkreisschema zur Durchführung des alternierenden POVMs auf einem dreidimensionalen System durch Ankopplung zweier Qubits. Es werden hierbei die Permutationen $\pi_3 := (0\ 2\ 1)$ und $\pi_4 := (0\ 1\ 2)$ genutzt. Die Symbole $\circ$ kennzeichnen einen Steuereingang, auf dem vor und nach dem Gatter σ_x-Operationen ausgeführt werden.

bestimmt, für die $A\sigma A^\dagger = \kappa_3$ gilt. Es folgt nun die Matrix

$$AMB^\dagger = \begin{pmatrix} 0 & 0 & 0 & 2\alpha & 0 & 0 & 2\gamma & 0 & 0 & 2\beta & 0 & 0 \\ 0 & 0 & 0 & 0 & 2\alpha & 0 & 0 & 2\gamma & 0 & 0 & 2\beta & 0 \\ 0 & 0 & 0 & 0 & 0 & 2\alpha & 0 & 0 & 2\gamma & 0 & 0 & 2\beta \end{pmatrix} \in \mathbb{C}^{3\times 12}$$

im Verkettungsraum $\mathrm{Int}(\kappa_3, \kappa_0 \oplus \kappa_1 \oplus \kappa_2 \oplus \kappa_3 \oplus \kappa_3 \oplus \kappa_3)$. Wird $A\sigma A^\dagger$ durch

$$\tilde{\sigma} := \kappa_3 \oplus \kappa_3 \oplus \kappa_0 \oplus \kappa_1 \oplus \kappa_2$$

bis auf die Reihenfolge der Komponenten zu der Darstellung $B\sigma_{\mathrm{mon}}B^\dagger$ ergänzt, so gibt es im damit folgenden Verkettungsraum

$$\mathrm{Int}(\kappa_3 \oplus \kappa_3 \oplus \kappa_3 \oplus \kappa_0 \oplus \kappa_1 \oplus \kappa_2,\ \kappa_0 \oplus \kappa_1 \oplus \kappa_2 \oplus \kappa_3 \oplus \kappa_3 \oplus \kappa_3)$$

Matrizen $C \otimes I_3$ mit

$$C := \begin{pmatrix} 0 & \gamma_{0,0} & \gamma_{0,1} & \gamma_{0,2} \\ 0 & \gamma_{1,0} & \gamma_{1,1} & \gamma_{1,2} \\ 0 & \gamma_{2,0} & \gamma_{2,1} & \gamma_{2,2} \\ 1 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{C}^{4\times 4}\,. \tag{4.20}$$

Hierbei werden die zu κ_0, κ_1 und κ_2 gehörenden Komponenten zu eins gesetzt, womit nicht alle Elemente in diesem Verkettungsraum erreicht werden, aber dennoch genug, um gemäß Satz 4.9 eine unitäre Ergänzung von M zu konstruieren: Die Matrix $AMB^\dagger$ legt durch

$$\gamma_{0,0} := 2\alpha, \quad \gamma_{0,1} := 2\gamma \quad \text{und} \quad \gamma_{0,2} := 2\beta$$

die erste Zeile von C fest. Die anderen Einträge können beliebig gewählt werden unter der Bedingung, daß C unitär ist. Gemäß Abschnitt 4.2 wird nach Festlegung von C durch $\tilde{M}^\dagger := B^\dagger(C^\dagger \otimes I_3)(A \oplus \tilde{A})$ für alle $\tilde{A} \in \mathcal{U}(9)$ eine Matrix erhalten, die das alternierende POVM auf die Messung in der Standardbasis reduziert. Wird hierbei $\tilde{A} := I_3 \otimes A$ gewählt, so folgt $A \oplus \tilde{A} = I_4 \otimes A$. Zusammen mit der Zerlegung von B aus Gl. (4.19) folgt eine Matrix zur Durchführung des alternierenden POVMs:

Satz 4.19 (Durchführung des alternierenden POVMs) *Das alternierende POVM kann durch*

$$\tilde{M}^\dagger := [12, \pi_1^{-1}\pi_2](F_2^\dagger \otimes F_2^\dagger \otimes I_3)[12, \pi_2^{-1}\pi_0^{-1}](F_3^\dagger \oplus I_9)(C^\dagger \otimes I_3)(I_4 \otimes A)$$

mit $\tilde{W} = C \otimes I_3$ für C aus Gl. (4.20) auf die Standardbasismessung reduziert werden.

Da die Matrix $\tilde{M}$ auf einem zwölfdimensionalen System operiert, ist eine Übersetzung in einen Schaltkreis nicht unmittelbar möglich. Werden zur Verallgemeinerung von Quantenschaltkreisen statt Qubits auch höherdimensionale Systeme zugelassen, so folgt das Schaltkreisschema von Abb. 4.5. Hierbei wird die Permutation $[12, \pi_1^{-1}\pi_2]$ weggelassen, denn diese kann durch eine Uminterpretation der Meßresultate ersetzt werden. Die Permutation $[12, \pi_2^{-1}\pi_0^{-1}]$ wird hingegen durch die gesteuerten Permutations- und CNOT-Gatter in der Mitte des Schaltkreises implementiert. Mit den in [VMS04] beschriebenen Verfahren kann $C^\dagger$ in höchstens zehn Ein-Qubit- und vier CNOT-Gatter zerlegt werden.

4.4.3 Zyklisches POVM

Symmetrien mit zyklischer Gruppe treten bei Systemen auf, die eine periodische Zeitentwicklung haben, d. h. es gilt $|\Phi_{t+t_0}\rangle = |\Phi_t\rangle$ für den Zustand $|\Phi_t\rangle$ zur Zeit t und der Periodenlänge t_0. Eine solche Zeitentwicklung liegt vor, falls die Eigenwerte des Hamilton-Operators H rationale Vielfache eines Wertes $\lambda \in \mathbb{R}$ sind; nach dem Spektralsatz kann durch einen Basiswechsel angenommen werden, daß bei einem d-dimensionalen System der Hamilton-Operator

$$H = \lambda \operatorname{diag}\left(\frac{p_0}{q_0}, \ldots, \frac{p_{d-1}}{q_{d-1}}\right)$$

für $\lambda \neq 0$ und $p_j, q_j \in \mathbb{Z}$ mit $\mathrm{ggT}(p_j, q_j) = 1$ vorliegt. Die Periodenlänge ist in diesem Fall

$$t := 2\pi \frac{\mathrm{kgV}(q_0, \ldots, q_{d-1})}{\lambda}.$$

Ist z. B. wie beim harmonischen Oszillator die Differenz zwischen benachbarten Eigenwerten konstant, so folgen bei geeigneter Wahl von λ und der Diskretisierung der Periode in n Abschnitte die durch $|\Phi_j\rangle := \sigma(r^j)|\Phi_0\rangle$ festgelegten Zustände mit dem Anfangszustand $|\Phi_0\rangle\langle\Phi_0|$ und der Darstellung

$$\sigma(r) := \operatorname{diag}(1, \omega_n, \omega_n^2, \ldots, \omega_n^{d-1}) \in \mathcal{U}(d)$$

der zyklischen Gruppe $C_n := \langle r : r^n = 1\rangle$. Die Schätzung, welcher dieser Zustände vorliegt, ist beispielsweise von Interesse, falls das System als Uhr dient und durch eine Messung die Zeit bestimmt werden soll (siehe [JB03]); damit verwandt ist die Ramsey-Spektroskopie, bei der t bekannt ist, aber nicht die Eigenwerte des Hamilton-Operators (siehe z. B. [HMP+97]). Nach den Untersuchungen in Kap. 3 folgt, daß für einige Kriterien optimale Messungen existieren, welche dieselbe Symmetrie haben. Umfaßt das optimale POVM hierbei genau eine Bahn von Operatoren $\Pi_j = |\Psi_j\rangle\langle\Psi_j|$, so kann durch eine Drehung, die mit der Symmetrieoperation kommutiert, angenommen werden, daß der initiale Vektor $|\Psi_0\rangle := (1, \ldots, 1)/\sqrt{n}$ vorliegt. Durch die Symmetrie werden alle anderen Operatoren des POVMs erhalten:

Definition 4.20 (Zyklisches POVM) *Es sei $n \geq d$. Das zyklische POVM auf einem d-dimensionalen System besteht aus den Operatoren $\Pi_j := |\Psi_j\rangle\langle\Psi_j|$ mit den Vektoren*

$$|\Psi_j\rangle := \sqrt{\frac{1}{n}} \begin{pmatrix} 1 \\ \omega_n^j \\ \omega_n^{2j} \\ \vdots \\ \omega_n^{(d-1)j} \end{pmatrix} \in \mathbb{C}^d \quad \textit{für} \quad j \in \{0, \ldots, n-1\}.$$

Der Ausgangspunkt der Konstruktion einer unitären Matrix zur Durchführung des POVMs ist die Matrix M aus Gl. (4.4), die durch

$$M = \sum_{j=0}^{n-1} |\Psi_j\rangle\langle j| = \sqrt{\frac{1}{n}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{d-1} & \omega_n^{2(d-1)} & \dots & \omega_n^{(n-1)(d-1)} \end{pmatrix} \in \mathbb{C}^{d\times n}$$

festgelegt ist und aus den ersten d Zeilen von $F_n \in \mathcal{U}(n)$ aus Def. 1.24 besteht. Die Matrix $M \in \mathbb{C}^{d\times n}$ hat die durch $\sigma M = M\sigma_{\text{mon}}$ definierte Symmetrie, wobei σ_{mon} nach Lemma 4.10 die reguläre Darstellung von C_n ist. Für die bei M genutzte Anordnung $r^0, r^1, \dots, r^{n-1}$ der Elemente von C_n ist diese durch $\sigma_{\text{mon}}(r) := X_n$ festgelegt, wobei X_n die zyklische Schiebematrix von Def. 4.11 ist. Gemäß Satz 4.9 werden für die Konstruktion von $\tilde{M}$ beide Darstellungen in irreduzible Komponenten zerlegt. Da σ schon die direkte Summe irreduzibler Darstellungen ist, kann $A := I_d$ gesetzt werden. Die Darstellung σ_{mon} wird hingegen wie in Beispiel 2.9 durch die Fourier-Matrix $B := F_n$ in irreduzible Komponenten zerlegt, denn es gilt $F_n X_n F_n^\dagger = Z_n$. Die Matrix im Verkettungsraum der zerlegten Darstellungen ist damit die Diagonalmatrix

$$AMB^\dagger = I_d M F_n^\dagger = \text{diag}(1, 1, \dots, 1) \in \mathbb{C}^{d\times n}\,.$$

Nach Satz 4.9 wird zur Konstruktion einer unitären Ergänzung von M die Darstellung σ durch $\tilde{\sigma}$ so ergänzt, daß dabei $F_n\sigma_{\text{mon}}F_n^\dagger$ entsteht. Dazu werden die in σ und $F_n\sigma_{\text{mon}}F_n^\dagger$ enthaltenen irreduziblen Darstellungen

$$\kappa_j : C_n \to \mathcal{U}(1),\ r^k \mapsto (\omega_n^{jk}),$$

miteinander verglichen: Die Darstellung σ und $F_n\sigma_{\text{mon}}F_n^\dagger$ sind die direkte Summen der κ_j für $j \in \{0, 1, \dots, d-1\}$ bzw. $j \in \{0, 1, \dots, n-1\}$, womit

$$\tilde{\sigma} := \kappa_d \oplus \dots \oplus \kappa_{n-1}$$

gesetzt wird. Da jede irreduzible Darstellung κ_j die Dimension eins hat und für $j \neq \ell$ zu κ_ℓ inäquivalent ist, folgt nach Lemma 2.23 der Verkettungsraum

$$\text{Int}(\kappa_0 \oplus \dots \oplus \kappa_{n-1}, \kappa_0 \oplus \dots \oplus \kappa_{n-1}) = \{\text{diag}(\lambda_0, \dots, \lambda_{n-1}) : \lambda_j \in \mathbb{C}\} \subseteq \mathbb{C}^{n\times n}.$$

Die Matrix $AMB^\dagger$ legt hierbei die ersten d Einträge zu $\lambda_j = 1$ fest. Eine einfache unitäre Ergänzung von $AMB^\dagger$ in diesem Verkettungsraum wird durch $\tilde{W} := I_d$ erhalten. Damit zeigt das Beispiel der zyklischen POVMs, daß eine starke Vereinfachung der unitären Ergänzung erhalten werden kann, falls diese im Verkettungsraum der zerlegten Darstellungen durchgeführt wird. Nach Abschnitt 4.2 wird die Erweiterung von M durch $\tilde{M} := (A^\dagger \oplus \tilde{A})\tilde{W}B$ für eine unitäre Matrix $\tilde{A} \in \mathcal{U}(n-d)$ erhalten. Hierbei kann $\tilde{A} = I_{n-d}$ gewählt werden, womit $A \oplus \tilde{A} = I_n$ folgt:

Satz 4.21 (Durchführung des zyklischen POVMs) *Das zyklische POVM mit n Operatoren auf einem d-dimensionalen System kann mit*

$$\tilde{M}^\dagger = B^\dagger \tilde{W}^\dagger (A \oplus \tilde{A}) = F_n^\dagger I_n I_n = F_n^\dagger$$

auf die Messung in der Standardbasis reduziert werden.

Werden zyklische POVMs auf einem Qubit-Register mit $n = 2^k$, $k \geq 1$, Operatoren untersucht, so kann F_n direkt in einen Schaltkreis übersetzt werden. Mit den bekannten Verfahren zur effizienten Implementierung der DFT (siehe Satz 3.1 in [Röt01]) folgt, daß das zyklische POVM ebenfalls effizient durchgeführt werden kann:

Korollar 4.22 (Aufwand des zyklischen POVM) *Das 2^k Operatoren umfassende zyklische POVM auf einem Qubit-Register kann mit $O(k^2)$ Ein-Qubit- und CNOT-Gattern durchgeführt werden.*

4.4.4 Heisenberg-Weyl-POVM

In der Physik sind der Ort und der Impuls die wichtigsten Größen, die für ein Teilchen untersucht werden. POVMs zur Messung dieser Größen können bestimmt werden, indem von geeigneten Symmetrieforderungen ausgegangen wird, welche die wesentlichen Eigenschaften der Messungen erfassen: Beispielsweise soll bei der Messung des Ortes eines Teilchens das Resultat unter Verschiebungen und Drehungen kovariant sein, d. h. wird das gesamte Bezugssystem verschoben oder gedreht, so werden entsprechend transformierte Resultate erhalten. Darüber hinaus wird gefordert, daß Resultate einer Ortsmessung invariant unter Impulsänderungen sind. Ähnliche Kovarianz- und Invarianzforderungen werden auch an Messungen des Impulses gestellt. Die dabei genutzten Symmetrieoperationen bilden eine Untergruppe der Galilei-Gruppe (siehe Abschnitt III.1 in [BGL95]).

Wird die Suche von Orts- und Impulsmessungen auf projektive Messungen beschränkt, so ist durch die Kovarianz- und Invarianzforderungen nur eine Messung möglich (siehe Abschnitt III.2.2 in [BGL95]): Für die Wellenfunktionen $\psi(x) \in \mathcal{L}^2(\mathbb{R})$ im Raum $\mathcal{L}^2(\mathbb{R})$ der quadratintegrablen Funktionen eines Teilchens in einer Dimension wird diese Messung beispielsweise durch die Spektralschar der Impuls- und Ortsoperatoren $\mathcal{P}$ bzw. $\mathcal{Q}$ beschrieben, die durch

$$(\mathcal{P}\psi)(x) := -i\frac{d}{dx}\psi(x) \quad \text{und} \quad (\mathcal{Q}\psi)(x) := x\psi(x)$$

definiert sind (siehe z. B. Abschnitt 3.1 in [Dav76]). Werden hingegen POVMs bei der Suche zugelassen, so können viele verschiedene Messungen des Ortes und des Impulses gefunden werden (siehe Abschnitt III.2.3 in [BGL95]). Allen möglichen Messungen ist jedoch gemein, daß sie der Heisenbergschen Unschärferelation unterliegen: Der Ort und der Impuls eines Teilchens können durch eine Messung nicht gemeinsam präzise bestimmt werden. Die approximative Bestimmung beider Größen ist möglich (siehe Abschnitt 3.4 in [Dav76]): Für eine normierte Wellenfunktion $\psi \in \mathcal{L}^2(\mathbb{R})$, die als Vektor $|\psi\rangle$ geschrieben werden kann und jeweils einen verschwindenden Erwartungswert für den Impuls- und Ortsoperator hat, wird die Operatoren-Familie

$$M_{s,t} := \frac{1}{2\pi} U_{s,t}|\psi\rangle\langle\psi|U_{s,t}^\dagger$$

gebildet, wobei $U_{s,t}|\psi\rangle$ der Funktion

$$(U_{s,t}\psi)(x) := e^{-ixs}\psi(x-t)$$

entspricht. Es folgt die Gleichung

$$\int_{s,t} M_{s,t}\, ds\, dt = I,$$

welche zeigt, daß die $M_{s,t}$ ein POVM bilden (siehe Beweis von Th. 4.1 in Abschnitt 3.4 von [Dav76]). Hierbei gibt $\mathrm{tr}(\rho M_{s,t})$ die Wahrscheinlichkeitsdichte der Resultate bei Vorliegen des Zustands ρ an. Dieses POVM vermittelt eine gemeinsame Messung des Orts und des Impulses eines Teilchens, indem s und t als Ort bzw. Impuls interpretiert werden. Beide Größen zusammen bilden einen Punkt (s,t) im Phasenraum $\mathbb{R}\times\mathbb{R}$. Daher wird eine gemeinsame Messung von Ort und Impuls auch als Phasenraummessung bezeichnet.

Für die Implementierung dieser Messungen mit Hilfe eines Quantenrechners werden diese Messungen auf endlich viele Resultate und endlich-dimensionale Systeme beschränkt. Dies entspricht dem Diskretisieren der Orts- und Impulskoordinaten des Phasenraums, wobei diese zyklisch aufeinander folgen; die zyklischen Impulswerte entsprechen dem Kristallimpuls in der Festkörperphysik (siehe [Zim72]). Das Teilchen kann sich damit nur an d verschiedenen Orten aufhalten und die Impulse können analog nur d verschiedene Werte annehmen. Die Verschiebung geht bei dieser Diskretisierung in die zyklische Verschiebung X_d und der Impulsverschiebung in die Phasenmatrix Z_d über. Das POVM ist bzgl. X_d und Z_d invariant, also auch bzgl. der von diesen Matrizen erzeugten Gruppe:

Definition 4.23 (Heisenberg-Weyl-Gruppe) *Die Heisenberg-Weyl-Gruppe zu einem d-dimensionalen System wird von den Elementen X_d und Z_d erzeugt.*

Die Heisenberg-Weyl-Gruppe ist endlich und umfaßt die d^3 Elemente $\omega_d^a Z_d^b X_d^c$ mit $a,b,c\in\{0,\ldots,d-1\}$ und der d-ten Einheitswurzel $\omega_d := e^{2\pi i/d}$. Da G eine Matrixgruppe ist, kann als Darstellung $\sigma: G\to\mathcal{U}(d)$ mit $\sigma(g)=g$ betrachtet werden:

Lemma 4.24 (Irreduzibilität der Darstellung) *Die durch $\sigma(g)=g$ gegebene Darstellung der Heisenberg-Weyl-Gruppe ist irreduzibel.*

Beweis: Der zu σ gehörende Charakter (siehe Def. 13.3 in [JL01]) ist durch

$$\chi(\omega_d^a Z_d^b X_d^c) := \mathrm{tr}(\omega_d^a Z_d^b X_d^c) = \omega_d^a \mathrm{tr}(Z_d^b X_d^c) = \begin{cases} d\omega_d^a, & b=c=0 \\ 0, & \text{sonst} \end{cases}$$

festgelegt. Da für das durch

$$\langle\chi|\chi\rangle := \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi(g^{-1})$$

definierte Innenprodukt (siehe Prop. 14.5 in [JL01]) dieses Charakters mit sich selbst die Gleichung $\langle\chi|\chi\rangle = 1$ gilt, folgt, daß σ eine irreduzible Darstellung von G ist (siehe Def. 14.3 in [JL01]). □

Da σ irreduzibel ist, folgt für jeden initialen Operator Π mit $\mathrm{tr}(\Pi)=1/d^2$ ein gruppenerzeugtes POVM, das d^3 Operatoren umfaßt. Hierbei entsteht jedoch jeder Operator d mal, denn bei der Konjugation von Π mit $g=\omega_d^a Z_d^b X_d^c$ fallen die Phasenfaktoren ω_d^a weg. Werden die Operatoren mit $a\neq 0$ gestrichen, so verbleibt ein POVM mit d^2 Operatoren, falls die Spur von Π zu $\mathrm{tr}(\Pi)=1/d$ abgeändert wird:

Definition 4.25 (Heisenberg-Weyl-POVM) *Das Heisenberg-Weyl-POVM enthält für ein d-dimensionales Quantensystem und den initialen Operator* $\Pi = |\Psi\rangle\langle\Psi|$ *mit der Spur* $\mathrm{tr}(|\Psi\rangle\langle\Psi|) = 1/d$ *die durch* $\Pi_{jd+k} := |\Psi_{jd+k}\rangle\langle\Psi_{jd+k}|$ *definierten Operatoren für*

$$|\Psi_{jd+k}\rangle := Z_d^k X_d^j |\Psi\rangle$$

mit $j, k \in \{0, \ldots, d-1\}$.

Da das POVM d^2 Resultate hat, muß zur Durchführung die Dimension d des gemessenen Systems zu d^2 erweitert werden; dies wird durch die Hinzunahme eines d-dimensionalen Hilfssystems erreicht, denn ist dieses mit dem Zustand $|0\rangle\langle 0|$ initialisiert, so sind die beiden Zustandsvektoren $|0\rangle \otimes |\Phi\rangle$ und $|\Phi\rangle \oplus 0_{d^2-d}$ gleich. Grundlage der Konstruktion einer unitären Matrix zur Durchführung des POVMs ist die Matrix M aus Gl. (4.4). Der initiale Vektor $|\Psi\rangle = (v_0, \ldots, v_{d-1})^T$ führt hierbei zu

$$\begin{aligned} M &= \sum_{j,k=0}^{d-1} Z_d^k X_d^j |\Psi\rangle\langle jd+k| = \sum_{j,k=0}^{d-1} Z_d^k X_d^j |\Psi\rangle \left(\langle j| \otimes \langle k|\right) \\ &= \begin{pmatrix} v_0 & v_0 & \ldots & v_0 & v_{d-1} & \ldots & v_{d-1} & \ldots & v_1 & \ldots & v_1 \\ v_1 & v_1\omega_d & \ldots & v_1\omega_d^{d-1} & v_0 & \ldots & v_0\omega_d^{d-1} & \ldots & v_2 & \ldots & v_2\omega_d^{d-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ v_{d-1} & v_{d-1}\omega_d^{d-1} & \ldots & v_{d-1}\omega_d & v_{d-2} & \ldots & v_{d-2}\omega_d & \ldots & v_0 & \ldots & v_0\omega_d \end{pmatrix}, \end{aligned}$$

wobei $|jd+k\rangle = |j\rangle \otimes |k\rangle$ genutzt wird. Die Symmetrie $\sigma M = M\sigma_{\mathrm{mon}}$ von Lemma 4.7 wird mit den Erzeugern X_d und Z_d von G durch die Gleichungen

$$Z_d M = M(I_d \otimes X_d) \text{ und } X_d M = M(X_d \otimes Z_d^\dagger)$$

beschrieben. Daher ist die Darstellung $\sigma_{\mathrm{mon}} : G_d \to \mathcal{U}(d^2)$ durch $\sigma_{\mathrm{mon}}(Z_d) = I_d \otimes X_d$ und $\sigma_{\mathrm{mon}}(X_d) = X_d \otimes Z_d^\dagger$ definiert. Als erster Schritt der Zerlegung von σ_{mon} wird die Komponente X_d von $\sigma_{\mathrm{mon}}(X_d)$ mit der Fourier-Matrix F_d aus Def. 1.24 diagonalisiert. Die Symmetrie von M kann damit in

$$Z_d M = M(F_d \otimes F_d^\dagger)(I_d \otimes Z_d)(F_d^\dagger \otimes F_d) \quad \text{und} \quad X_d M = M(F_d \otimes F_d^\dagger)(Z_d^\dagger \otimes X_d)(F_d^\dagger \otimes F_d)$$

umgeformt werden. Die Matrizen $I_d \otimes Z_d$ und $Z_d^\dagger \otimes X_d$ können als direkte Summen

$$(I_d \otimes Z_d) = Z_d \oplus Z_d \oplus \ldots \oplus Z_d \quad \text{und} \quad (Z_d^\dagger \otimes X_d) = X_d \oplus \omega_d^{d-1} X_d \oplus \ldots \oplus \omega_d X_d$$

geschrieben werden. Bis auf die Phasenfaktoren ω_d^j entspricht die zugehörige Darstellung damit der direkten Summe von d Kopien der irreduziblen Darstellung σ. Diese Faktoren können durch eine geeignete Konjugation entfernt werden: Aufgrund $Z_d X_d Z_d^\dagger = \omega_d X_d$ gelten mit

$$Z := I_d \oplus Z_d^{d-1} \oplus Z_d^{d-2} \oplus \ldots \oplus Z_d^2 \oplus Z_d \in \mathbb{C}^{d^2 \times d^2}$$

die Gleichungen $Z(I_d \otimes X_d)Z^\dagger = (Z_d^\dagger \otimes X_d)$ und $Z(I_d \otimes Z_d)Z^\dagger = (I_d \otimes Z_d)$. Damit werden

$$Z_d M = M(F_d \otimes F_d^\dagger) Z (I_d \otimes Z_d) Z^\dagger (F_d^\dagger \otimes F_d) \text{ und } X_d M = M(F_d \otimes F_d^\dagger) Z (I_d \otimes X_d) Z^\dagger (F_d^\dagger \otimes F_d)$$

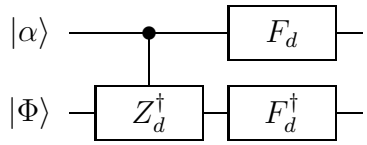

Abbildung 4.6: Schema zur Durchführung des Heisenberg-Weyl-POVMs auf einem d-dimensionalen System. Der initiale Operator legt über Gl. (4.22) den Zustandsvektor $|\alpha\rangle$ des Hilfssystems fest. Das gesteuerte $Z_d^\dagger$-Gatter bedeutet, daß für den Zustand $|j\rangle\langle j|$ des oberen Systems die Operation Z_d^{-j} auf dem unteren durchgeführt wird.

erhalten, wobei $I_d \otimes X_d$ die Faktoren ω_d^j nicht mehr enthält. Diese Gleichungen zeigen, daß mit der Notation von Satz 4.9 die Zerlegung

$$B\sigma_{\mathrm{mon}}B^\dagger = \sigma \oplus \ldots \oplus \sigma \quad \text{mit} \quad B := Z^\dagger(F_d^\dagger \otimes F_d)$$

gilt. Die Darstellung $B\sigma_{\mathrm{mon}}B^\dagger$ enthält d irreduzible Komponenten σ; ferner gilt $A := I_d$, da σ eine irreduzible Darstellung ist. Es folgt, daß die Matrix

$$AMB^\dagger = \sqrt{d}\,(v_0, \ldots, v_{d-1})F_d^\dagger \otimes I_d \in \mathbb{C}^{d\times d^2} \tag{4.21}$$

ein Element des Verkettungsraums

$$\mathrm{Int}(\sigma, I_d \otimes \sigma) = \{(\alpha_0, \ldots, \alpha_{d-1}) \otimes I_d : \alpha_j \in \mathbb{C}\} \subseteq \mathbb{C}^{d\times d^2}$$

ist. Die Ergänzung der Darstellung σ zu $I_d \otimes \sigma$ gelingt durch Hinzunahme von $d-1$ Komponenten σ. Der resultierende Verkettungsraum ist nach Lemma 2.23 durch

$$\mathrm{Int}(I_d \otimes \sigma, I_d \otimes \sigma) = \{C \otimes I_d : C \in \mathbb{C}^{d\times d}\} \subseteq \mathbb{C}^{d^2\times d^2}$$

bestimmt. Die Matrix $AMB^\dagger \in \mathbb{C}^{d\times d^2}$ legt die erste Zeile von C fest, falls die ergänzte unitäre Matrix als $C \otimes I_d$ geschrieben wird. Diese Zeile ist nach Gl. (4.21) durch

$$\langle\alpha| := \sqrt{d}\,(v_0, \ldots, v_{d-1})\,F_d^\dagger \tag{4.22}$$

gegeben. Die anderen Zeilen von C können beliebig unter der Forderung, daß C unitär ist, gewählt werden. Eine mögliche unitäre Transformation $\tilde{M}$ für die Durchführung des Heisenberg-Weyl-POVMs ist durch

$$\tilde{M} = (A^\dagger \oplus \tilde{A})(C \otimes I_d)B = (C \otimes I_d)Z^\dagger(F_d^\dagger \otimes F_d) \tag{4.23}$$

definiert. In dieser Gleichung wird $\tilde{A} = I_{d^2-d}$ gesetzt, denn dies führt zu der Matrix $A \oplus \tilde{A} = I_d \oplus I_{d^2-d} = I_{d^2}$.

Satz 4.26 (Durchführung des Heisenberg-Weyl-POVMs) *Das Heisenberg-Weyl-POVM mit dem initialen Operator $\Pi = |\Psi\rangle\langle\Psi|$ kann nach Ankopplung eines mit $|0\rangle\langle 0|$ initialisierten Systems durch $\tilde{M}^\dagger$ aus Gl. (4.23) auf die orthogonale Messung in der Standardbasis reduziert werden.*

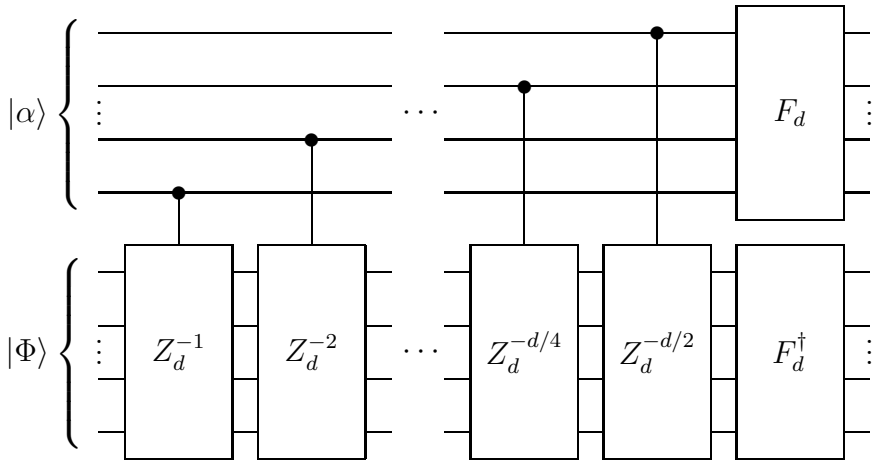

Abbildung 4.7: Schaltkreis für das Heisenberg-Weyl-POVM. Der Zustandsvektor $|\alpha\rangle$ des Hilfssystems wird durch Gl. (4.22) festgelegt. (Schaltkreis aus [DJR05] übernommen.)

In der Zerlegung von $\tilde{M}$ aus Gl. (4.23) ist nur die Matrix C von dem initialen Operator Π des POVMs abhängig. Dies kann genutzt werden, um einen einzigen Schaltkreis für alle möglichen $\Pi = |\Psi\rangle\langle\Psi|$ zu konstruieren, wobei der initiale Operator Π des durchgeführten POVMs durch den Zustand des Hilfssystems festgelegt wird: Grundlage ist hierfür die Gleichung

$$\tilde{M}^\dagger(|0\rangle \otimes |\Phi\rangle) = (F_d \otimes F_d^\dagger)Z(C^\dagger \otimes I_d)\,(|0\rangle \otimes |\Phi\rangle) = (F_d \otimes F_d^\dagger)Z(|\alpha\rangle \otimes |\Phi\rangle)\,.$$

Damit wird das POVM auch dann durchgeführt, falls $(F_d \otimes F_d^\dagger)Z$ auf dem mit $|\alpha\rangle \otimes |\Phi\rangle$ initialisierten System durchgeführt wird.

Satz 4.27 (Durchführungsschema für Heisenberg-Weyl-POVM) *Das Heisenberg-Weyl-POVM mit initialem Operator $\Pi = |\Psi\rangle\langle\Psi|$ kann durch das Schema in Abb. 4.6 durchgeführt werden, falls das Hilfssystem mit dem durch $|\alpha\rangle = \sqrt{d}F_d|\overline{\Psi}\rangle$ beschriebenen Zustand initialisiert ist, wobei $|\overline{\Psi}\rangle$ aus $|\Psi\rangle$ durch elementweise Konjugation hervorgeht.*

Das Schema von Abb. 4.6 kann für ein Register mit k Qubits in einen Schaltkreis übersetzt werden. Zur Bestimmung des Aufwands werden die Fourier-Transformationen und das gesteuerte Gatter Z_d in Ein-Qubit- und CNOT-Gatter zerlegt. Hierbei wird ausgenutzt, daß Z_d als Tensorprodukt

$$Z_d = \begin{pmatrix} 1 & 0 \\ 0 & \omega_d^{d/2} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & \omega_d^{d/4} \end{pmatrix} \otimes \ldots \otimes \begin{pmatrix} 1 & 0 \\ 0 & \omega_d \end{pmatrix} \in \mathcal{U}(d) \tag{4.24}$$

mit k Ein-Qubit-Operationen geschrieben werden kann. Zusammen mit den bekannten Zerlegungsverfahren der DFT-Matrizen führt dies zu einem effizienten Verfahren zur Durchführung des POVMs:

Korollar 4.28 (Aufwand des Heisenberg-Weyl-POVMs) *Das Heisenberg-Weyl-POVM auf einem Register mit k Qubits kann mit dem Schaltkreis von Abb. 4.7 durchgeführt werden, falls das Hilfssystem mit $|\alpha\rangle$ aus Gl. (4.22) initialisiert ist. Der Schaltkreis kann in $O(k^2)$ Ein-Qubit- und CNOT-Gatter zerlegt werden.*

Beweis: Nach Satz 3.1 in [Röt01] können die Matrizen F_d und $F_d^\dagger$ für $d = 2^k$ jeweils mit $O(k^2)$ vielen Ein-Qubit- und CNOT-Gattern durchgeführt werden. Ferner kann jede der k gesteuerten Z_d^{-j}-Operationen in Abb. 4.7 wie in Gl. (4.24) zerlegt werden; jede Qubit-Transformation erhält hierbei zusätzlich eine Steuerleitung. Nach Kor. 5.3 in [BBC$^+$95] kann jede dieser gesteuerten Operationen in vier Ein-Qubit- und zwei CNOT-Gatter zerlegt werden. □

Wie Kor. 4.28 zeigt, kann die Durchführung des Heisenberg-Weyl-POVMs mit polynomialem Aufwand auf die Präparation eines Zustands reduziert werden. Da sich $|\Psi\rangle$ des initialen Operators $\Pi = |\Psi\rangle\langle\Psi|$ nach Gl. (4.22) nur um eine Fourier-Transformation von $|\alpha\rangle$ unterscheidet, folgt ein effizientes Verfahren für das POVM, falls der Zustand $\sqrt{d}|\Psi\rangle\langle\Psi|$ effizient präpariert werden kann. In Abschnitt 6.4 von [DJR05] führt dies für die durch

$$|\Psi\rangle := \sqrt{\frac{1}{\kappa}}(1, \alpha, \alpha^2, \ldots, \alpha^{d/2-2}, \alpha^{d/2-1}, \alpha^{d/2-1}, \alpha^{d/2-2}, \ldots, \alpha^2, \alpha, 1)^T \in \mathbb{C}^d \qquad (4.25)$$

mit der Normierung $\kappa = 2d(1 + |\alpha|^2 + |\alpha|^4 + \ldots + |\alpha|^{d-2})$ beschriebene Familie von Heisenberg-Weyl-POVMs zu effizienten Verfahren. Der Vektor $|\Psi\rangle$ ist für geeignete $\alpha \in \mathbb{C}$ im Orts- und Impulsbereich ausreichend lokalisiert, so daß eine brauchbare Phasenraummessung der Zustände erhalten werden kann.

4.5 Experimentelle Durchführung

Es sind mehrere Experimente zur Messung von POVMs vorgeschlagen und zum Teil auch durchgeführt worden. Einige dieser Vorschläge beruhen auf Ionen oder Rydberg-Atomen (siehe [RRS02, FAABS01]), die meisten Vorschläge und durchgeführten Experimente nutzen hingegen quantenoptische Systeme. Der Grund hierfür ist, daß sich kleine optische Systeme im Vergleich zu anderen Quantensystemen gut beherrschen lassen. Im folgenden werden neben quantenoptischen Grundlagen auch einige Vorschläge und experimentelle Daten zusammenfassend dargestellt.

4.5.1 Quantenoptische Grundlagen

In der Quantenoptik wird die quantenmechanische Beschreibung bestimmter elektromagnetischer Felder untersucht; Ausgangspunkt sind hierbei die Maxwellschen Gleichungen (siehe z. B. Abschnitt 18-1 in [FLS89a]). Die Eigenschaften der Lösungen unter den Randbedingungen der Quantenoptik können anhand vereinfachter Modelle diskutiert werden. Beispielsweise können die Untersuchungen von eindimensionalen Gebieten mit elektrisch perfekt leitenden Beschränkungen ausgehen. In dieser Situation gibt es Lösungen der Maxwellschen Gleichungen, die durch

$$E_x(z,t) := \sqrt{\frac{2\omega^2}{V\epsilon_0}} q(t) \sin(kz) \qquad (4.26)$$

für das elektrische Feld und

$$B_y(z,t) := \left(\frac{\mu_0\epsilon_0}{k}\right) \sqrt{\frac{2\omega^2}{V\epsilon_0}} \dot{q}(t) \cos(kz) \qquad (4.27)$$

für das magnetische Feld mit geeigneten $\epsilon_0, \mu_0, V, \omega$ und k beschrieben werden (siehe Abschnitt 2.1 in [GK05]). Hierbei bezeichnen x und y die Koordinatenachsen, die der Schwingungsrichtung des elektrischen bzw. magnetischen Feldes entsprechen. Die zum elektrischen Feld gehörende Richtung legt die Polarisation des Feldes fest. Ferner bezeichnet $q(t)$ einen zeitabhängigen Phasenfaktor und $p(t) := \dot{q}(t)$ dessen Ableitung. Es folgt die Hamilton-Funktion

$$H(t) := \frac{1}{2}(p(t)^2 + \omega^2 q(t)^2)\,,$$

die zeigt, daß das Feld formal mit einem harmonischen Oszillator identifiziert werden kann, der durch den Ort $q(t)$ und den Impuls $p(t)$ beschrieben wird (siehe Kap. 5 in [Hun79] und Abschnitt 21-4 in [FLS89b]). Für den Übergang zu einer quantenmechanischen Beschreibung des harmonischen Oszillators und des Feldes werden p und q durch hermitesche Operatoren $\hat{p}$ und $\hat{q}$ ersetzt (siehe z. B. Abschnitt 1.2.3 in [GR94]), welche die Kommutatorrelation $[\hat{p}, \hat{q}] = -i\hbar I$ erfüllen, wobei I die Identitätsabbildung bezeichnet und $\hbar := h/2\pi$ mit dem Planckschen Wirkungsquantum h gebildet wird. Durch die Ersetzung von p und q durch $\hat{p}$ bzw. $\hat{q}$ folgt der Hamilton-Operator

$$\hat{H} := \frac{1}{2}(\hat{p}^2 + \omega^2 \hat{q}^2)\,.$$

Eine andere Darstellung von $\hat{H}$, die zur Vereinfachung vieler Rechnungen führt, wird mit dem Vernichtungs- und dem Erzeugungsoperator erhalten (siehe Abschnitt 2.1 in [GK05]):

Definition 4.29 (Vernichtungs- und Erzeugungsoperator) *Die Operatoren*

$$\hat{a} := \sqrt{\frac{1}{2\hbar\omega}}(\omega\hat{q} + i\hat{p}) \quad \textit{und} \quad \hat{a}^\dagger := \sqrt{\frac{1}{2\hbar\omega}}(\omega\hat{q} - i\hat{p})$$

heißen Vernichtungs- bzw. Erzeugungsoperator.

Mit $\hat{a}$ und $\hat{a}^\dagger$ kann der Hamilton-Operator zu

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) = \hbar\omega\left(\hat{n} + \frac{1}{2}\right)$$

umgeschrieben werden, wobei $\hat{n} := \hat{a}^\dagger\hat{a}$ der Anzahloperator ist. Seine Eigenzustände $|n\rangle$ mit den Eigenwerten $n \in \mathbb{N}$ werden als Anzahl- oder Fock-Zustände bezeichnet (siehe Abschnitt 4.2.1 in [BR04]). Ist $|n\rangle\langle n|$ der Zustand eines Systems, so hat es aufgrund der Eigenwertgleichung $\hat{H}|n\rangle = E_n|n\rangle$ die Energie

$$E_n := \hbar\omega\left(n + \frac{1}{2}\right) = \hbar\omega n + \frac{\hbar\omega}{2}\,.$$

Wird $\hbar\omega/2$ als Grundenergie des Systems betrachtet, so kann E_n in n Quanten, die jeweils die Energie $\hbar\omega$ haben und Photonen genannt werden, aufgeteilt werden. Die Bezeichnung der Erzeugungs- und Vernichtungsoperatoren folgt aus den Gleichungen

$$\hat{H}\hat{a}^\dagger|n\rangle = (E_n + \hbar\omega)\hat{a}^\dagger|n\rangle \quad \text{und} \quad \hat{H}\hat{a}|n\rangle = (E_n - \hbar\omega)\hat{a}|n\rangle\,,$$

die so interpretiert werden können, daß $\hat{a}^\dagger$ und $\hat{a}$ ein Photon der Energie $\hbar\omega$ erzeugen bzw. vernichten (siehe Abschnitt 2.1 in [GK05]). Demnach kann ihre Wirkung auf den Vektoren $|n\rangle$ durch

$$\hat{a}|0\rangle = 0, \quad \hat{a}|n\rangle = \sqrt{n}\,|n-1\rangle \quad \text{und} \quad \hat{a}^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle$$

beschrieben werden. Eine besondere Linearkombination der Eigenvektoren $|n\rangle$ sind die kohärenten Zustände (siehe Abschnitt 3.1 in [GK05]):

Definition 4.30 (Kohärenter Zustand) *Für jedes $\alpha \in \mathbb{C}$ wird der zugehörige kohärente Zustand $|\alpha\rangle\langle\alpha|$ definiert durch*

$$|\alpha\rangle := e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle\,.$$

Der kohärente Zustand $|\alpha\rangle\langle\alpha|$ erfüllt die Eigenwertgleichung $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. Ausgehend vom Grundzustand $|0\rangle\langle 0|$ kann der kohärente Zustand $|\alpha\rangle\langle\alpha|$ durch Anwendung des Verschiebeoperators (*displacement operator*, siehe Abschnitt 3.2 in [GK05])

$$\hat{D}(\alpha) := e^{\alpha\hat{a}^\dagger - \overline{\alpha}\hat{a}} \tag{4.28}$$

erhalten werden, d. h. es gilt $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$. Kohärente Zustände werden als klassische Zustände angesehen, da sie beispielsweise nicht gequetscht sind (*squeezed*, siehe Abschnitt 7.1 in [GK05]). Eine einfache Definition der Quetschung folgt mit den Quadraturoperatoren (siehe Abschnitt 21.1 in [MW95]):

Definition 4.31 (Quadraturoperatoren) *Die beiden Operatoren*

$$\hat{Q}_\beta := e^{i\beta}\hat{a}^\dagger + e^{-i\beta}\hat{a} \quad \textit{und} \quad \hat{P}_\beta := e^{i(\beta+\pi/2)}\hat{a}^\dagger + e^{-i(\beta+\pi/2)}\hat{a}$$

sind die Quadraturoperatoren zum Winkel β.

Die Quadraturoperatoren erfüllen die Kommutatorrelation $[\hat{Q}_\beta, \hat{P}_\beta] = 2iI$, womit die Unschärferelation

$$\langle(\Delta\hat{Q}_\beta)^2\rangle\langle(\Delta\hat{P}_\beta)^2\rangle \geq 1 \tag{4.29}$$

folgt. Hierbei bezeichnet $\langle X\rangle := \mathrm{tr}(\rho X)$ den Erwartungswert des Operators X für den Zustand ρ des Systems und

$$\langle(\Delta X)^2\rangle := \langle X^2\rangle - \langle X\rangle^2$$

die zugehörige Varianz. Die Quetschung eines Zustands liegt vor, falls die Quadraturoperatoren bestimmte Varianzen haben (siehe Abschnitt 21.1 in [MW95]):

Definition 4.32 (Gequetschtes Feld) *Ein Feld ist gequetscht, falls ein Winkel β existiert, so daß $\langle(\Delta\hat{Q}_\beta)^2\rangle < 1$ gilt.*

Durch Quetschung wird die Varianz einer der beiden Quadraturoperatoren verkleinert, während gleichzeitig die Varianz der anderen gemäß der Unschärferelation vergrößert wird. Für kohärente Zustände gilt die Gleichung $\langle(\Delta\hat{Q}_\beta)^2\rangle = \langle(\Delta\hat{P}_\beta)^2\rangle = 1$, womit diese nicht gequetscht sind (siehe Abschnitt 21.1 in [MW95]). Da Quetschung nur

bei Zuständen auftritt, die als nicht-klassisch angesehen werden, ist der experimentelle Nachweis von besonderem Interesse. Hierzu werden Aufbauten genutzt, die aus optischen Elementen wie beispielsweise Strahlteiler oder Phasenelemente bestehen. Auch bei diesen Elementen stellen die Erzeugungs- und Vernichtungsoperatoren die Grundlage einer einfachen Beschreibung dar (siehe Abschnitt 5.1.2 in [BR04]):

Definition 4.33 (Strahlteiler) *Es seien $\hat{a}_0, \hat{a}_1$ und $\hat{a}_2, \hat{a}_3$ die Vernichtungsoperatoren der Ein- bzw. Ausgänge eines Strahlteilers. Dann gilt*

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} \sqrt{\epsilon} & \sqrt{1-\epsilon} \\ \sqrt{1-\epsilon} & -\sqrt{\epsilon} \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}$$

für den Reflexionskoeffizienten $\epsilon \in [0,1]$ und den Transmissionskoeffizienten $1-\epsilon$.

Eine allgemeinere Modellierung von Strahlteilern kann in Abschnitt 12.12 von [MW95] gefunden werden. Für $\epsilon = 1/2$ liegt der balancierte Strahlteiler vor, dessen Transformationsmatrix die DFT-Matrix F_2 aus Def. 1.24 ist. Die Koeffizienten eines Strahlteilers können ebenfalls durch sein Teilungsverhältnis $p : q$ mit $p, q \in \mathbb{N}$ angegeben werden, das dem Reflexionskoeffizienten $\epsilon^2 = p/(p+q)$ entspricht. Neben Strahlteilern sind auch Phasenelemente (*phase shifter*, siehe Abschnitt 3.2 in [Cal01]) wichtige optische Elemente. Diese können ebenfalls mit dem Erzeugungs- und Vernichtungsoperator einfach beschrieben werden:

Definition 4.34 (Phasenelement) *Ein Phasenelement für $\phi \in [0, 2\pi]$ entspricht der Transformation*

$$\hat{b} := U\hat{a}U^\dagger \quad \textit{mit} \quad U := e^{-i\phi\hat{n}},$$

wobei $\hat{a}$ und $\hat{b}$ die Vernichtungsoperatoren des Ein- bzw. Ausgangs sind.

Die Messungen, die in der Quantenoptik von Bedeutung sind, werden durch Detektoren erhalten, die im idealen Fall ein Signal ausgeben, falls nicht das durch $|0\rangle$ beschriebene Feld anliegt. Das zugehörige POVM umfaßt die Operatoren $\Pi_0 := |0\rangle\langle 0|$ und $\Pi_1 := \sum_{j=1}^{\infty} |j\rangle\langle j|$. Kann innerhalb eines festgelegten Zeitintervalls auch die Anzahl der Detektionen bestimmt werden, wird die orthogonale Messung mit den Operatoren $\Pi_j := |j\rangle\langle j|$, $j \in \mathbb{N}$, durchgeführt (siehe Abschnitt 3.2 in [Cal01]). Ein experimentelles Problem sind hierbei irrtümliche Detektionen nicht vorhandener Photonen (*dark counts*).

4.5.2 Optische Implementierung von POVMs

Nach dem Naimark-Theorem kann jedes POVM durch eine unitäre Transformation auf eine orthogonale Messung reduziert werden. In der Quantenoptik werden unitäre Transformationen beispielsweise durch Strahlteiler und Phasenelemente erhalten; prinzipiell können mit diesen Elementen durch den in [RZBB94] beschriebenen Aufbau alle unitären Transformationen $U \in \mathcal{U}(n)$ und damit auch alle POVMs implementiert werden. Dieser in Abb. 4.8 skizzierte Aufbau hat jeweils n Ein- und Ausgänge, weshalb der Aufbau auch als $2n$-Port bezeichnet wird (siehe z. B. Abschnitt 3 in [BHS01]). Die durchzuführende unitäre Transformation bzw. Messung legt die Phasenelemente und die Teilungsverhältnisse der Strahlteiler fest. Die nach Def. 4.1 notwendigen $n - d$ zusätzlichen Dimensionen für die Durchführung eines POVMs werden hierbei durch unbenutzte Eingänge erhalten; jedem

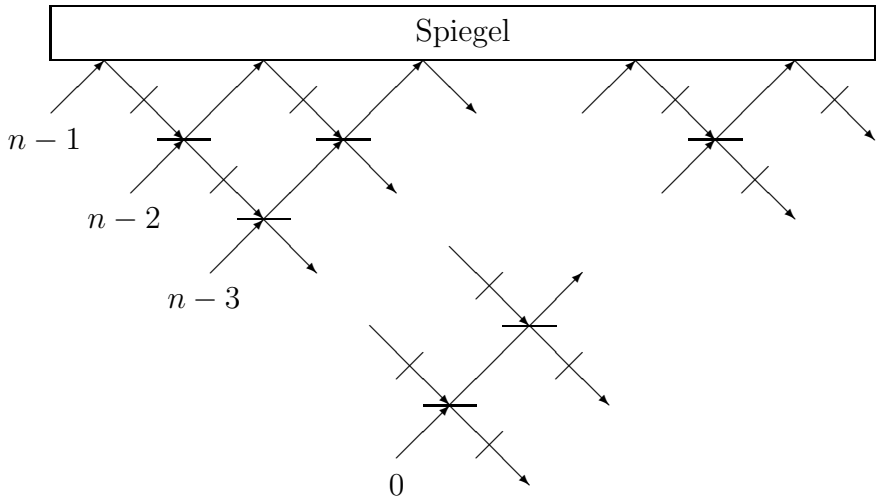

Abbildung 4.8: Quantenoptische Implementierung beliebiger unitärer Transformationen mit einem $2n$-Port nach [RZBB94]. Die horizontalen und diagonalen Linien entsprechen Strahlteilern bzw. Phasenelementen.

der n POVM-Operatoren wird ein Detektor an einem Ausgang zugewiesen. Da jedem Ein- und Ausgang eine Dimension des zugehörigen Hilbert-Raums entspricht, können die Schaltkreise aus den Abschnitten 4.4.3 und 4.4.4 mit einem $2n$-Port nicht effizient durchgeführt werden. Dahingegen sind für POVMs mit wenigen Operatoren Experimente vorgeschlagen und auch durchgeführt worden. Ziel dieser Experimente ist der Nachweis, daß die Unterscheidung von Zuständen mittels POVMs besser möglich ist als mit orthogonalen Messungen.

Fehlerfreie Unterscheidung von Zuständen

Ist von einem System nur bekannt, daß es sich im Zustand $|\alpha\rangle\langle\alpha|$ oder $|\beta\rangle\langle\beta|$ mit nicht orthogonalen $|\alpha\rangle$ und $|\beta\rangle$ befindet, so gibt es keine Messung, die eine fehlerfreie Entscheidung, welcher Zustand vorliegt, garantiert: Entweder besteht die Möglichkeit, daß eine fehlerhafte Entscheidung getroffen wird oder daß die Messung nicht ausreichend Informationen zur Entscheidung liefert. Die zweite Möglichkeit läßt es zu, daß nie eine falsche Entscheidung getroffen wird (*unambiguous state discrimination*, siehe z. B. [Che98]):

Definition 4.35 (Fehlerfreie Unterscheidung) *Das POVM mit den Operatoren* $\Pi_?$ *und* $\Pi_0, \ldots, \Pi_{n-1}$ *unterscheidet die Zustände* $\rho_0, \ldots, \rho_{n-1}$ *fehlerfrei, falls* $\mathrm{tr}(\rho_k \Pi_j) = 0$ *für* $j \neq k$ *mit* $j, k \in \{0, \ldots, n-1\}$ *gilt.*

Wird bei dem Resultat j das Vorliegen von ρ_j angenommen, so tritt nie eine falsche Entscheidung auf. Da das Resultat ? jedoch keine Zuordnung ermöglicht, kann nicht bei jeder Messung eine Entscheidung getroffen werden. Für zwei verschiedene Zustände $\rho_0 := |\alpha\rangle\langle\alpha|$ und $\rho_1 := |\beta\rangle\langle\beta|$ eines Qubits ist eine fehlerfreie Unterscheidung mit einem POVM möglich; dabei werden für reelles $\langle\alpha|\beta\rangle$ die Operatoren

$$\Pi_0 := \frac{1}{1+\langle\alpha|\beta\rangle}(I_2 - |\beta\rangle\langle\beta|), \quad \Pi_1 := \frac{1}{1+\langle\alpha|\beta\rangle}(I_2 - |\alpha\rangle\langle\alpha|) \quad \text{und} \quad \Pi_? := I_2 - \Pi_0 - \Pi_1$$

genutzt (siehe z. B. Abschnitt III in [Bra99]). Die Wahrscheinlichkeit des Resultats ? ist hierbei $|\langle\alpha|\beta\rangle|^2$, d. h. bei orthogonalen $|\alpha\rangle$ und $|\beta\rangle$ ist immer eine korrekte Entscheidung

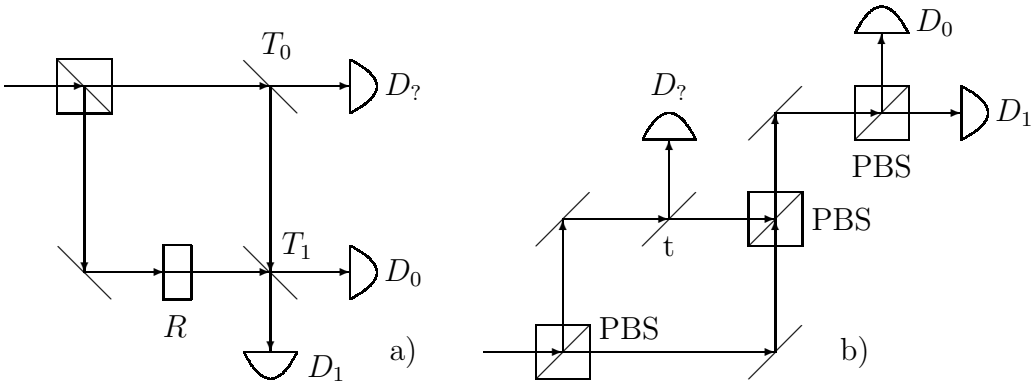

Abbildung 4.9: Aufbau a) nach [Bra99] und b) nach [HMG+96] zur fehlerfreien Unterscheidung zweier nicht-orthogonaler Zustände. Der Strahlteiler mit Transmissionskoeffizienten t entspricht der polarisationsabhängigen Dämpfung in der Faser. $D_?$ modelliert die Absorption in der Faser, D_0 und D_1 entsprechen den fehlerfreien Detektionen der beiden möglichen Zuständen.

möglich und je kleiner der Winkel zwischen beiden Zustandsvektoren ist, desto häufiger tritt das Ergebnis ? auf (siehe Abschnitt III.A in [Che00]).

Die quantenoptische Durchführung der fehlerfreien Unterscheidung zweier Zustände mit $\langle\alpha|\beta\rangle = \cos(\theta)$ für $\theta \in [0, 2\pi]$ wird in [Bra99] vorgeschlagen: Der in Abb. 4.9a) dargestellte Aufbau besteht aus einem polarisierenden Strahlteiler (PBS, *polarizing beam splitter*), der eingehende Photonen mit zueinander orthogonalen Polarisationen in verschiedene Richtungen weiterleitet (siehe Abschnitt II in [BML97]). Daneben wird ein Element R genutzt, das den Polarisierungswinkel um 90° dreht, sowie Strahlteiler T_0 und T_1, welche die Transmissionskoeffizienten $1 - \tan(\theta/2)^2$ bzw. $1/2$ haben. Die Detektoren D_0, D_1 und $D_?$ werden den Operatoren Π_0, Π_1 und $\Pi_?$ zugeordnet.

Das erste durchgeführte Experiment zur fehlerfreien Zustandsunterscheidung wird in [HMG+96] beschrieben. Eine Vereinfachung der Implementierung wird durch eine Faser erhalten, die Photonen einer bestimmten Polarisation sehr stark dämpft, während dazu orthogonal polarisierte nur sehr schwach gedämpft werden. Der Aufbau ist schematisch in Abb. 4.9b) dargestellt, wobei die Dämpfung der Faser durch einen Strahlteiler mit geeignetem Teilungsverhältnis und einen Detektor modelliert wird (siehe [HMG+96]). Am Ende der Faser werden die Photonen durch einen Strahlteiler auf zwei Detektoren geleitet, die den Operatoren Π_0 und Π_1 entsprechen. Ein Nachteil dieses Experiments ist, daß das Resultat ? nicht durch Detektoren gemessen werden kann. Damit kann im Experiment nicht festgestellt werden, ob ein Photon in der Faser absorbiert wird oder ob beispielsweise ein Detektor versagt hat. Bei der Durchführung des Experiments konnte nach [HMG+96] bei $\langle\alpha|\beta\rangle = 1/2$ weniger als zwei Prozent Fehler erhalten werden. Das Experiment von [HMG+96] wird in [CCBR01] verbessert, indem alle drei Meßresultate 0, 1 und ? durch Detektoren registriert werden. Die experimentell erhaltenen Resultate reichen bis auf ein Prozent an die theoretisch mögliche Schranke heran.

Neben der Polarisierung können auch die möglichen Pfade der Photonen als Quantensysteme genutzt werden; jeder mögliche Pfad wird hierbei als Mode bezeichnet (siehe Abschnitt 2.1.5 in [BR04]). Ein experimenteller Vorschlag mit einem 6-Port zur fehlerfreien Unterscheidung zweier Zustände eines Qubits, das zwei Moden entspricht, wird in

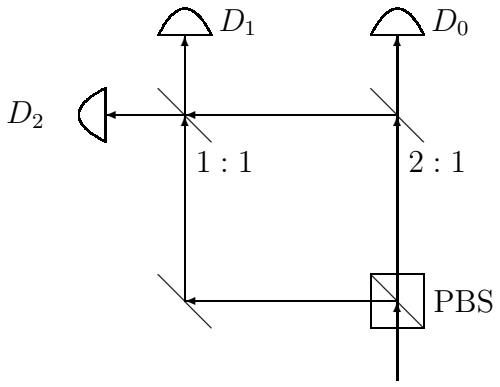

Abbildung 4.10: Experimenteller Aufbau nach [Ren04] zur Messung der Drillinge.

[BHS01] vorgeschlagen. Dieser Experimentvorschlag wird in [MSB04] erweitert, wobei drei Zustände eines dreidimensionalen Systems mit Hilfe eines 8-Ports fehlerfrei unterschieden werden. Im Experiment werden in ca. 82 Prozent der Messungen Resultate erhalten, die eine Entscheidung für einen der drei möglichen Zustände zulassen. Der theoretisch mögliche Anteil dieser Messungen ist $83,3$ Prozent; bei diesen Resultaten werden im Experiment in $1,7$ Prozent der Fälle falsche Entscheidungen getroffen.

Zyklisches POVM mit drei Operatoren

Die Drillinge $|\Phi_j\rangle\langle\Phi_j|$ aus Bsp. 3.12 haben eine zyklische Symmetrie der Ordnung drei und können daher nach Satz 3.5 und 3.40 bezüglich der Detektionsfehlerwahrscheinlichkeit und der Transinformation durch ein POVM optimal unterschieden werden, welches drei Operatoren mit derselben zyklischen Symmetrie umfaßt (siehe auch [TFMS04]). In [Ren04] wird ein experimenteller Aufbau vorgeschlagen, um dieses POVM zu messen. Der in Abb. 4.10 dargestellte Aufbau besteht aus einem polarisierenden Strahlteiler, drei Detektoren und zwei Strahlteilern mit den Teilungsverhältnissen $1:1$ sowie $2:1$.

Das erste Experiment zur Durchführung des POVMs wird in [CKC+01] beschrieben. Hierbei konnten ca. $0,491$ bit der theoretisch möglichen $0,585$ bit erhalten werden. Damit gelang der erste experimentelle Nachweis, daß POVMs mehr Information über Zustände liefern können als orthogonale Messungen, denn diese können höchstens $0,459$ bit ergeben.

In [TFMS04] werden für dasselbe POVM experimentelle Daten für zwei verschiedene Versuchsaufbauten angegeben, beide sind in Abb. 4.11 dargestellt. Eine Implementierung beruht auf der Polarisation der Photonen, die andere auf den Moden. Beide Aufbauten nutzen neben drei Detektoren polarisierende Strahlteiler und Phasenelemente mit geeigneten Phasen P_0, P_1 und P_2. Für die Polarisation und Moden konnten im Experiment ca. $0,560$ bit bzw. $0,557$ bit erhalten werden. Die beiden verschiedenen Implementierungsarten können kombiniert werden, um eine Messung der Doppeldrillinge aus Abschnitt 3.6.2 durchzuführen.

Optimale Messung der Doppeldrillinge

Wie in [PW91] und Abschnitt 3.2 diskutiert wird, kann durch die gemeinsame Messung der Doppeldrillinge $|\Phi'_j\rangle := |\Phi_j\rangle \otimes |\Phi_j\rangle$ aus Abschnitt 3.6.2 mehr Information erhalten werden als durch die Einzelmessung der Zustände $|\Phi_j\rangle\langle\Phi_j|$. In [FTMS03, TFMS04] wird

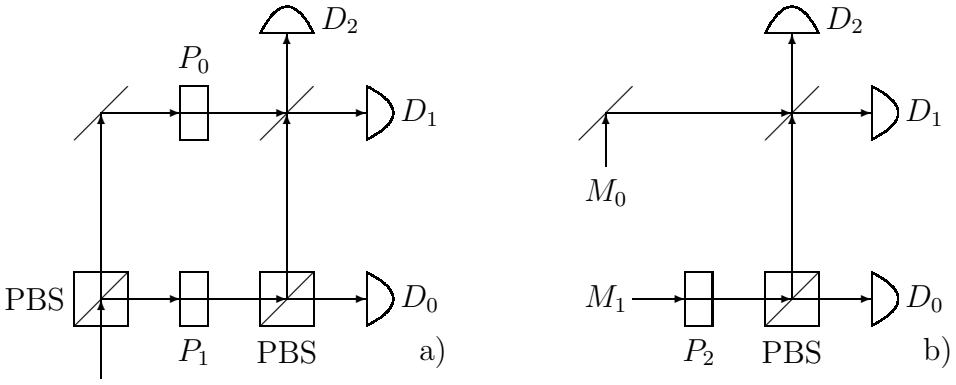

Abbildung 4.11: Experimentelle Aufbauten nach [TFMS04] zur Messung des POVMs mit drei Operatoren und zyklischer Symmetrie: a) Implementierung mit Polarisation sowie b) Implementierung mit Moden. Hierbei bezeichnen M_0 und M_1 die beiden Moden, die dem Eingangssignal entsprechen.

untersucht, ob dies auch experimentell bestätigt werden kann. Hierzu wird das in [PW91] diskutierte POVM, das die Operatoren $\Pi_j := |\Psi_j\rangle\langle\Psi_j|$ für

$$\begin{aligned} |\Psi_0\rangle &:= a\,|\Phi_0'\rangle + b\,|\Phi_1'\rangle + b\,|\Phi_2'\rangle\,, \\ |\Psi_1\rangle &:= b\,|\Phi_0'\rangle + a\,|\Phi_1'\rangle + b\,|\Phi_2'\rangle \quad \text{und} \\ |\Psi_2\rangle &:= b\,|\Phi_0'\rangle + b\,|\Phi_1'\rangle + a\,|\Phi_2'\rangle \end{aligned}$$

mit den Werten

$$a := \frac{4+\sqrt{2}}{3\sqrt{3}} \quad \text{sowie} \quad b := -\frac{2-\sqrt{2}}{3\sqrt{3}}$$

umfaßt, experimentell durchgeführt. Die Experimente von [FTMS03] zeigen, daß durch die gemeinsame Messung der Doppeldrillinge ca. $0,656$ bit Information pro Qubit erhalten werden kann; nach Abschnitt 3.6.2 ist $0,6845$ bit optimal. Die experimentell erhaltene Information liegt damit sogar oberhalb der C_1-Kapazität (siehe Def. 3.13) von $0,6454$ bit der Zustände (siehe Abschnitt 3.2).

Das Tetraeder-POVM

In Abschnitt 6.2 von [Ren04] wird für das Tetraeder-POVM aus Def. 4.12 eine optische Implementierung vorgeschlagen, wobei die Qubits der Polarisation entsprechen. Der Aufbau ist in Abb. 4.12 dargestellt und wurde mit dem Verfahren aus [RZBB94] konstruiert. Er besteht aus einem polarisierenden Strahlteiler, vier Strahlteilern und vier Detektoren, die jeweils einem der Resultate zugeordnet werden. Andere optische Aufbauten für das Tetraeder-POVM werden in [ŘEK04, EMGK05] vorgeschlagen.

Das Tetraeder-POVM ist bezüglich der Transinformation optimal zur Unterscheidung von Zuständen mit derselben Symmetrie (siehe Prop. 8 in [Dav78]). In [CKC+01] wird ein Experiment beschrieben, bei dem gezeigt wird, daß mit dem Tetraeder-POVM mehr Information als mit jeder orthogonalen Messung erhalten werden kann: Es werden mit dem Tetraeder-POVM ca. $0,363$ bit erhalten, wohingegen eine orthogonale Messung theoretisch höchstens $0,311$ bit ergeben kann.

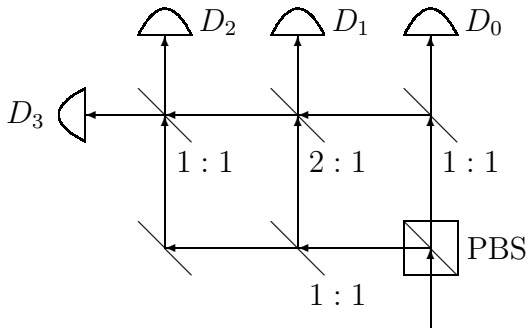

Abbildung 4.12: Aufbau von Abschnitt 6.2 in [Ren04] zur Messung des Tetraeder-POVMs.

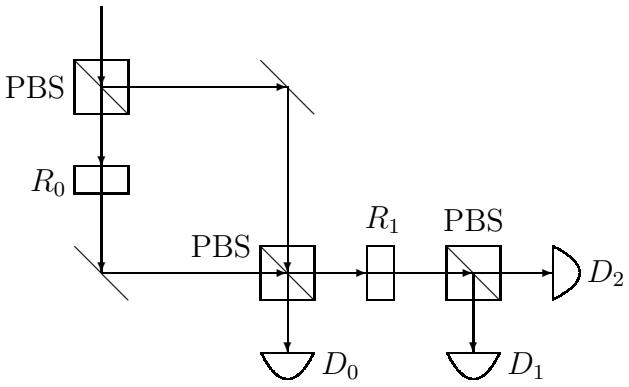

Abbildung 4.13: Experimenteller Aufbau nach [SBJ+99, MFA+01] für die Zustände mit der zyklischen Symmetrie.

Unterscheidung von Zuständen mit zyklischer Symmetrie

Liegen die n Zustände $|\Phi_j\rangle\langle\Phi_j|$ mit den Zustandsvektoren

$$|\Phi_j\rangle := \sqrt{\frac{1}{n}} \begin{pmatrix} 1 \\ \omega_n^j \end{pmatrix} \in \mathbb{C}^2$$

für $j \in \{0, \ldots, n-1\}$ vor, wobei $\omega_n := e^{2\pi i/n}$ eine n-te Einheitswurzel ist, so existiert nach Satz 3.40 ein bzgl. der Transinformation optimales POVM mit Operatoren vom Rang eins und derselben Symmetrie. Für große n ist die quantenoptische Durchführung problematisch, denn es werden n Detektoren zur Durchführung dieses POVMs benötigt. Nach Satz 3.38 existiert auch ein optimales POVM, das nur drei Operatoren vom Rang eins umfaßt. Diese POVMs werden für $n \geq 2$ in [SBJ+99] bestimmt; im Gegensatz zu den Zuständen muß ein optimales POVM nicht symmetrisch sein und es können auch verschiedene Normierungen der Operatoren erhalten werden. In [SBJ+99] wird ein Experiment mit der Polarisation von Photonen vorgeschlagen, um diese POVMs zu implementieren. Der Aufbau dieses Vorschlags ist in Abb. 4.13 wiedergegeben. Er besteht aus drei polarisierenden Strahlteilern, drei Detektoren und zwei Elementen, welche die Polarisation um $R_0 := \gamma$ und $R_1 := \pi/8$ für ein geeignetes $\gamma \in \mathbb{R}$ drehen. In [MFA+01] werden für $n = 3, 5, 7$ experimentelle Daten für die erhaltene Information angegeben: Für $n = 3$ und $n = 5$ kann mit den POVMs mehr Information erhalten werden als es theoretisch mit orthogonalen Messungen möglich ist. Bei $n = 7$ kann die theoretische Schranke orthogo-

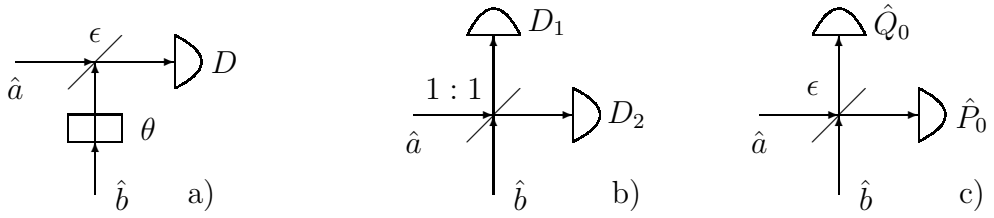

Abbildung 4.14: a) Homodyne Detektion nach [MW95]. Die Phase θ des Referenzstrahls kann eingestellt werden. Der Strahlteiler hat den Reflexionskoeffizienten ϵ. b) Balancierte homodyne Detektion nach [BGL95] mit einem Strahlteiler des Teilungsverhältnisses 1 : 1. c) Aufbau zur Phasenraummessung nach Abb. 7.7 in [BGL95].

naler Messungen aufgrund experimenteller Fehler jedoch nicht mehr durch das POVM übertroffen werden.

4.5.3 Phasenraummessung mit homodyner Detektion

Die Kommutatorrelation $[\hat{Q}_\beta, \hat{P}_\beta] = 2iI$ der Quadraturoperatoren $\hat{Q}_\beta$ und $\hat{P}_\beta$ zeigt, daß diese wie der Orts- und der Impulsoperator eines Teilchens zueinander kanonisch konjugierte Operatoren sind. Deshalb kann auch für sie eine Phasenraummessung, d. h. eine gemeinsame Messung beider Operatoren unter Einhaltung der Unschärferelation, definiert werden. Experimentell kann diese Messung mit Verfahren durchgeführt werden, welche die homodyne oder balancierte homodyne Detektion nutzen.

Homodyne Detektion

Die homodyne Detektion ist ein Verfahren zur Messung der Quadraturoperatoren von elektromagnetischen Feldern; insbesondere kann mit homodyner Detektion experimentell festgestellt werden, ob ein Feld gequetscht ist (siehe [SHY+85, Man82]). Das Verfahren nutzt den in Abb. 4.14a) dargestellten Aufbau, bei dem das zu messende Feld, welches durch den Vernichtungsoperator $\hat{a}$ beschrieben wird, auf einen Strahlteiler mit dem Transmissionskoeffizienten $1-\epsilon$ trifft (siehe Abschnitt 21.6 in [MW95]). Das Feld wird durch den Strahlteiler mit einem starken, nicht quantenmechanisch beschriebenen Referenzfeld gleicher Frequenz überlagert, dessen Phase θ gesteuert werden kann. Der Strahlteiler ist fast perfekt durchlässig, d. h. $1-\epsilon$ ist nahe eins, so daß ein Feld mit dem Vernichtungsoperator $\hat{a}+vI$ auf den Detektor trifft, wobei $v = |v|e^{i\theta}$ die Amplitude des Referenzfeldes ist. Wird die Anzahl der Signale des Detektors D in einem bestimmten Zeitintervall registriert, können die Erwartungswerte

$$\langle\hat{n}\rangle = \eta\langle(\hat{a}^\dagger + \overline{v}I)(\hat{a}+vI)\rangle \quad \text{und} \quad \langle\hat{n}(\hat{n}-I)\rangle = \eta^2\langle(\hat{a}^\dagger + \overline{v}I)^2(\hat{a}+vI)^2\rangle$$

experimentell ermittelt werden, wobei η eine Konstante ist, die von der Länge des Zeitintervalls und den Eigenschaften des Detektors abhängt. Damit ist es möglich, die Größe $\langle\hat{n}(\hat{n}-1)\rangle - \langle\hat{n}\rangle^2 = \langle(\Delta\hat{n})^2\rangle - \langle\hat{n}\rangle$ zu bestimmen (siehe Abschnitt 21.6 in [MW95]). Für großes $|v|$, d. h. es liegt ein starkes Referenzfeld vor, kann diese Größe durch

$$\langle(\Delta\hat{n})^2\rangle - \langle\hat{n}\rangle \approx \begin{cases} \eta^2|v|^2\langle{:}\,(\Delta\hat{Q}_\beta)^2\,{:}\rangle\,, & \text{für } \theta-\beta = 0 \\ \eta^2|v|^2\langle{:}\,(\Delta\hat{P}_\beta)^2\,{:}\rangle\,, & \text{für } \theta-\beta = \pi/2 \end{cases}$$

approximiert werden (siehe [MW95, Man82]), wobei die Doppelpunkte den Normalordnungsoperator bezeichnen (siehe Abschnitt 3.7 in [GK05]). Liegt ein gequetschtes Feld vor, d. h. es gibt einen Winkel β mit

$$\langle : (\Delta\hat{Q}_\beta)^2 : \rangle = \langle (\Delta\hat{Q}_\beta)^2 \rangle - 1 < 0\,,$$

so kann bei einem Experiment die Quetschung durch $\langle (\Delta\hat{n})^2 \rangle - \langle \hat{n} \rangle < 0$ registriert werden, falls θ geeignet eingestellt wird. Die Messung der Quadraturamplituden selbst durch die homodyne Detektion wird in Abschnitt VII.3.6 in [BGL95] diskutiert.

Balancierte homodyne Detektion

Ein weiteres Verfahren zur Messung der Quadraturoperatoren von Feldern ist die balancierte homodyne Detektion (siehe z. B. Abschnitt 7.3 in [GK05]). Der zugehörige Aufbau in Abb. 4.14b) zeigt, daß wie bei der homodynen Detektion das zu messende Feld durch einen Strahlteiler mit einem Referenzstrahl überlagert wird. Im Gegensatz zur homodynen Detektion hat dieser Strahlteiler den Transmissionskoeffizienten $\epsilon = 1/2$ und es werden an beiden Ausgängen Detektoren angebracht. Gehören zu den Ausgängen die Vernichtungsoperatoren $\hat{c}$ und $\hat{d}$ mit

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = \sqrt{\frac{1}{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}$$

so werden durch die Zähler die Erwartungswerte $\langle \hat{c}^\dagger \hat{c} \rangle$ und $\langle \hat{d}^\dagger \hat{d} \rangle$ gemessen. Durch Bildung der Differenz der Zählresultate kann für ein starkes Referenzstrahl mit Amplitude $|v|$ der Erwartungswert

$$\langle \hat{n}_{cd} \rangle := \langle \hat{c}^\dagger \hat{c} \rangle - \langle \hat{d}^\dagger \hat{d} \rangle = |v| \langle \hat{Q}_{\pi/2-\theta} \rangle$$

bestimmt werden, wobei θ die Phase des Referenzstrahls bezeichnet (siehe Abschnitt 7.3 in [GK05]). Durch verschiedene Einstellungen dieser Phase können alle Quadraturoperatoren und deren Varianzen gemessen werden. Da bei Vorhandensein einer Quetschung die Ungleichung $\langle (\Delta\hat{n}_{cd})^2 \rangle < |v|^2$ für eine geeignete Phase θ gilt, kann die Quetschung experimentell detektiert werden (siehe z. B. [SHY$^+$85]). Die exakte Messung der Quadraturoperatoren wird nur im Grenzfall eines unendlich starken Referenzfeldes erhalten. Liegen nur endlich starke Felder vor, so können auch in diesem Fall die gemessenen Operatoren angegeben werden (siehe [TS04]).

Phasenraummessung

Mit der homodynen oder balancierten homodynen Detektion ist es durch Einstellung der Phase β des Referenzfeldes möglich, die Quadraturoperatoren $\hat{Q}_\beta$ und $\hat{P}_\beta$ zu messen. Mit einem zusätzlichen Referenzfeld, das wie in Abb. 4.14c) durch einen Strahlteiler mit dem zu messenden Feld überlagert wird, ist es möglich, beide Quadraturoperatoren unter Einhaltung der Unschärferelation (4.29) gemeinsam zu messen. Im einfachsten Fall hat der Strahlteiler das Teilungsverhältnis 1 : 1 und es wird der Zustand $|0\rangle\langle 0|$ als Referenzstrahl mit dem zu messenden Feld überlagert. Damit umfaßt nach [LP93] das gemessene POVM die Operatoren

$$\Pi_\alpha := |\alpha\rangle\langle\alpha| \quad \text{mit} \quad \alpha := q + ip \in \mathbb{C}\,,$$

wobei q und p den Resultaten der Phasenraummessung entsprechen. Damit ist eine Messung der durch

$$Q(\alpha) := \frac{1}{\pi}\mathrm{tr}(\rho|\alpha\rangle\langle\alpha|)\,, \alpha \in \mathbb{C}\,,$$

definierten Q-Funktion (siehe z. B. Abschnitt 12.2.1 in [Sch01]) des Zustandes ρ möglich. Die Q-Funktion ist beispielsweise von Bedeutung, falls Erwartungswerte von bestimmten Produkten der Erzeugungs- und Vernichtungsoperatoren berechnet werden (siehe Abschnitt 12.3 in [Sch01]).

Wird statt $|0\rangle\langle 0|$ der durch die Wellenfunktion ψ beschriebene reine Zustand als Referenzfeld genutzt und hat der Strahlteiler den Transmissionskoeffizienten $1-\epsilon = \cos^2(\theta)$, so wird das POVM mit den Operatoren

$$\Pi_\alpha := \frac{1}{\pi}\hat{D}(\alpha)|\xi\rangle\langle\xi|\hat{D}(\alpha)^\dagger$$

gemessen (siehe Abschnitt VII.3.7 in [BGL95]), wobei $\hat{D}(\alpha)$ den Verschiebeoperator aus Gl. (4.28) bezeichnet und $|\xi\rangle\langle\xi|$ den durch die Funktion

$$\xi(y) := \sqrt{\frac{1}{\tan(\theta)}}\,\overline{\psi}\left(-\frac{y}{\tan(\theta)}\right)$$

definierten Operator vom Rang eins, wobei $\overline{\psi}$ die komplexe Konjugation von ψ bezeichnet.

Kapitel 5

Durchführung mit minimaler Störung

Wird eine Messung nicht am Ende eines Experiments durchgeführt, so ist neben dem Resultat auch der dabei entstehende Zustand des gemessenen Systems von Interesse. Dies ist beispielsweise bei mehrstufigen Meßprozessen der Fall, bei denen Messungen in Abhängigkeit vorher erhaltener Resultate gewählt werden, um so schrittweise mehr Information über ein System zu gewinnen (siehe z. B. [PW91]). Dabei ist es zweckmäßig, daß die durch eine Messung verursachte Störung des Zustands für die dabei ermittelte Information minimal ist. Weitere Fälle, bei denen die Störung von Bedeutung ist, finden sich auch in der Kryptographie: Hier kann zum Beispiel ein Angreifer eines Schlüsselaustauschs durch schwach störende Messungen versuchen, unbemerkt Informationen zu erhalten (siehe z. B. Abschnitt VI.E in [GRTZ02]).

Für die minimal störende Messung ist die im vorherigen Kapitel untersuchte Durchführung nicht geeignet, denn bei dieser wird der Zustand nach der Messung allein durch das Meßresultat einer orthogonalen Messung festgelegt und ist daher vom ursprünglichen Zustand unabhängig. Die Grundidee zur Lösung dieses Problems ist, daß nicht das System selbst gemessen wird, sondern *nur* ein Hilfssystem, das vor der Messung in Wechselwirkung mit dem zu messenden System steht. In diesem Kapitel wird untersucht, wie dies mit Hilfe eines Quantenrechners erreicht wird. Es werden hierbei wie in Kap. 4 unitäre Transformationen und Schaltkreise konstruiert, die das POVM auf eine orthogonale Messung reduzieren. Es stellt sich heraus, daß auch bei dieser Reduktion die Symmetrie eines POVMs als Grundlage der Konstruktion effizienter Meßverfahren genutzt werden kann.

5.1 Störung einer Messung

Bei quantenmechanischen Systemen, deren Zustand nicht bekannt ist, kann prinzipiell nicht verhindert werden, daß Messungen diesen verändern. Der durchschnittliche Unterschied zwischen dem Zustand vor und nach einer Messung wird mit der als Störung bezeichneten Größe erfaßt (*disturbance*, siehe z. B. Abschnitt 4.3 in [Bar98]). Ausgangspunkt für die Definition der Störung ist die Güte (*fidelity*, siehe Abschnitt 9.2.2 in [NC00]):

Definition 5.1 (Güte von Zuständen) *Die Güte zweier Zustände ρ und $\tilde{\rho}$ eines Sys-*

tems ist

$$F(\rho,\tilde{\rho}) := \mathrm{tr}\sqrt{\rho^{1/2}\tilde{\rho}\rho^{1/2}}\,.$$

Die Güte von Zuständen ist symmetrisch, d. h. es gilt $F(\rho,\tilde{\rho}) = F(\tilde{\rho},\rho)$. Ferner ist sie durch $0 \leq F(\rho,\tilde{\rho}) \leq 1$ beschränkt, wobei $F(\rho,\tilde{\rho}) = 1$ für gleiche und $F(\rho,\tilde{\rho}) = 0$ für orthogonale Zustände auftritt, d. h. ρ und $\tilde{\rho}$ haben orthogonale Träger, womit auch $\mathrm{tr}(\rho\tilde{\rho}) = 0$ gilt. Diese und weitere Eigenschaften der Güte zeigen, daß sie als Ähnlichkeitsmaß für Zustände genutzt werden kann (siehe Abschnitt 9.2.2 in [NC00]). Zur Definition der Störung einer Messung wird angenommen, daß vor der Messung ein unbekannter Zustand $\rho = |\Phi\rangle\langle\Phi|$ vorliegt, der gemäß der Gleichverteilung gewählt wird. Nach einer Messung mit dem Resultat j liegt gemäß Def. 1.28 der Zustand

$$\rho'_j := \frac{1}{\mathrm{tr}(\rho\Pi_j)} \sum_{k=0}^{n_j-1} A_{j,k}\rho A_{j,k}^\dagger \tag{5.1}$$

vor, wobei die $A_{j,k}$ die zu der Messung gehörenden Kraus-Operatoren aus Def. 1.27 sind. Die Störung wird durch die Mittelung der Güte von ρ und ρ'_j mit den zugehörigen Wahrscheinlichkeiten erhalten (siehe Gl. (4.8) in [Bar98]):

Definition 5.2 (Störung einer Messung) *Es sei $\rho = |\Phi\rangle\langle\Phi|$ ein reiner Zustand und ρ'_j der Zustand aus Gl. (5.1) nach der Messung mit Resultat j. Für das normierte, unitär invariante Maß Ω_Φ des Zustandraums ist*

$$1 - \int d\Omega_\Phi \sum_{j=0}^{n-1} \mathrm{tr}(\rho\Pi_j)(F(\rho'_j,\rho))^2$$

die Störung der Messung.

Die Untersuchung der Störung einer Messung führt zu der Problematik, welche Beziehung zwischen der Information, die durch eine Messung über ein System gewonnen werden kann, und der dadurch notwendig verursachten Störung besteht (*information-disturbance trade-off*, siehe [FP96, Bar00]). Diese Betrachtungen sind beispielsweise in der Quantenkryptographie von großer Bedeutung.

5.2 Messung mit minimaler Störung

Die Nichteindeutigkeit der Zerlegung von POVM-Operatoren in Kraus-Operatoren hat zur Folge, daß jedem POVM verschiedene Meßgeräte entsprechen, die den Zustand auch bei demselben Resultat auf unterschiedliche Art verändern. Ist ein POVM gegeben, so kann unter den zugehörigen Meßgeräten unmittelbar eines spezifiziert werden, das nach Def. 5.2 eine minimale Störung zur Folge hat (siehe Th. 4.2 in [Bar98]):

Lemma 5.3 (Kraus-Operatoren einer minimal störenden POVM-Messung) *Es sei ein POVM mit den Operatoren Π_j gegeben. Ein diesem POVM entsprechendes Meßgerät stört den Zustand nach Def. 5.2 minimal, falls bei Resultat j der Zustand gemäß*

$$\rho \mapsto \frac{1}{\mathrm{tr}(\rho\Pi_j)} \sqrt{\Pi_j}\rho\sqrt{\Pi_j} \tag{5.2}$$

abgebildet wird.

Die Zustandsabbildung von Gl. (5.2) bedeutet, daß jedem POVM-Operator Π_j der einzelne Kraus-Operator $A_{j,0} := \sqrt{\Pi_j}$ zugeordnet wird. Diese Abbildung kann auf einem Quantenrechner durch eine unitäre Transformation und eine Messung in der Standardbasis erreicht werden (siehe Abschnitt 2.2.8 in [NC00]): Hat das POVM hierbei n Operatoren, so wird das zu messende System um ein n-dimensionales Hilfssystem mit dem initialen Zustand $|0\rangle\langle 0|$ erweitert. Anschließend wird eine geeignete unitäre Transformation $\tilde{M}$ auf dem Gesamtsystem durchgeführt, so daß eine orthogonale Messung des Hilfssystems zu der Messung des POVMs führt. Das dabei notwendige $\tilde{M}$ wird hierbei durch die Operatoren des POVMs festgelegt:

Definition 5.4 (Minimal störende Durchführung) *Das POVM mit den Operatoren Π_j wird durch $\tilde{M} \in \mathcal{U}(dn)$ minimal störend durchgeführt, falls*

$$\tilde{M}(|0\rangle \otimes |\Phi\rangle) = \sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_j}|\Phi\rangle \,. \tag{5.3}$$

Die Forderung aus Gl. (5.3) legt $\tilde{M}$ nur auf dem d-dimensionalen Teilraum

$$\mathcal{H} := \{|0\rangle \otimes |\Phi\rangle : |\Phi\rangle \in \mathbb{C}^d\} \tag{5.4}$$

von $\mathbb{C}^n \otimes \mathbb{C}^d$ fest. Die Abbildung auf dem orthogonalen Komplement kann beliebig sein, denn durch die Initialisierung $|0\rangle\langle 0|$ des Hilfssystems ist der Zustand, auf den $\tilde{M}$ angewandt wird, immer zu dem Komplement orthogonal. Die Abbildung aus Def. 5.4 von $\mathcal{H}$ in den gesamten Raum wird durch die Matrix

$$M := \sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_j} = \begin{pmatrix} \sqrt{\Pi_0} \\ \vdots \\ \sqrt{\Pi_{n-1}} \end{pmatrix} \in \mathbb{C}^{dn \times d} \tag{5.5}$$

beschrieben, falls die $d(n-1)$ Nullen der Elemente von $\mathcal{H}$ weggelassen werden. Die unitäre Matrix $\tilde{M}$ aus Gl. (5.3) geht aus M hervor, indem $d(n-1)$ orthogonale Spalten ergänzt werden. Da die Operatoren Π_j ein POVM bilden, gilt

$$M^\dagger M = \left(\sqrt{\Pi_0} \ldots \sqrt{\Pi_{n-1}}\right) \begin{pmatrix} \sqrt{\Pi_0} \\ \vdots \\ \sqrt{\Pi_{n-1}} \end{pmatrix} = \sum_{j=0}^{n-1} \Pi_j = I_d \tag{5.6}$$

für die Gram-Matrix der Spalten von M. Diese Gleichung zeigt, daß M orthogonale Spalten hat und daß deshalb die unitäre Ergänzung von M zu $\tilde{M}$ immer möglich ist, d. h. jedes POVM kann mit minimaler Störung nach Def. 5.4 durchgeführt werden (siehe Abschnitt 2.2.8 in [NC00]). Die Nichteindeutigkeit von $\tilde{M}$ kann genutzt werden, um den Aufwand der Durchführung eines POVMs zu minimieren.

5.3 Ausnutzung der Symmetrie

Nach Def. 2.13 gehören zu einem (G, σ, π)-symmetrischen POVM mit den Operatoren Π_j die beiden Darstellungen $\sigma : G \to \mathcal{U}(d)$ und $\pi : G \to S_n$, so daß $\sigma(g)\Pi_j\sigma(g)^\dagger = \Pi_{\pi(g)(j)}$ gilt. Die Matrix M aus Gl. (5.5) besteht jedoch aus den Wurzeln der Π_j, so daß die Symmetrie dieser Wurzeln untersucht werden muß:

Lemma 5.5 (Symmetrie der Wurzeln) *Es sei P ein POVM mit den Operatoren Π_j und der Symmetrie (G, σ, π). Dann gilt*

$$\sigma(g)\sqrt{\Pi_j}\sigma(g)^\dagger = \sqrt{\Pi_{\pi(g)(j)}}\,, \tag{5.7}$$

d. h. die Wurzeln $\sqrt{\Pi_j}$ haben dieselbe Symmetrie wie die Operatoren Π_j.

Beweis: Es muß gezeigt werden, daß für semipositive Matrizen B und C sowie einer unitären Matrix A aus der Gleichung $ABA^\dagger = C$ auch die Gleichung $A\sqrt{B}A^\dagger = \sqrt{C}$ folgt. Da die Matrizen $A\sqrt{B}A^\dagger$ und $\sqrt{C}$ beide semipositiv und Wurzeln von C sind, folgt dies aber aus der Eindeutigkeit der semipositiven Wurzel (siehe Th. 2.2.1 in [Mur90]). □

Nach Lemma 5.5 führt die Konjugation der Operatoren $\sqrt{\Pi_j}$ mit der Matrix $\sigma(g)$ zu einer Permutation der Komponenten von M:

$$(I_n \otimes \sigma(g)) \left(\sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_j} \right) \sigma(g)^\dagger = \sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_{\pi(g)(j)}} \tag{5.8}$$

Damit durch diese Konjugation eine Symmetrie von M definiert wird, muß die Permutation der Komponenten $\sqrt{\Pi_j}$ durch den Austausch von I_n der linken Seite von Gl. (5.8) mit einer geeigneten Permutationsmatrix aufgehoben werden:

Definition 5.6 (Matrixform einer Permutationsdarstellung) *Für die Permutationsdarstellung $\pi : G \to S_n$ wird die Darstellung $\sigma_\pi : G \to \mathcal{U}(n)$ mit*

$$\sigma_\pi(g) := \sum_{j=0}^{n-1} |\pi(g)(j)\rangle\langle j|$$

definiert, die jedem Gruppenelement eine Permutationsmatrix zuordnet.

Mit den Darstellungen σ und $\sigma_\pi \otimes \sigma$, wobei $\sigma_\pi \otimes \sigma$ durch $(\sigma_\pi \otimes \sigma)(g) := \sigma_\pi(g) \otimes \sigma(g)$ definiert ist, kann eine Symmetrie von M definiert werden:

Satz 5.7 (Symmetrie der Messung) *Es sei P ein POVM mit der Symmetrie (G, σ, π). Dann hat die in Gl. (5.5) definierte Matrix M die Symmetrie $(G, \sigma_\pi \otimes \sigma, \sigma)$.*

Beweis: Es gilt für alle $g \in G$ die Gleichung

$$\begin{aligned}(\sigma_\pi(g) \otimes \sigma(g)) \left(\sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_j} \right) \sigma(g)^\dagger &= \sum_{j=0}^{n-1} \sigma_\pi(g)|j\rangle \otimes \sigma(g)\sqrt{\Pi_j}\sigma(g)^\dagger \\ &= \sum_{j=0}^{n-1} |\pi(g)(j)\rangle \otimes \sqrt{\Pi_{\pi(g)(j)}}.\end{aligned}$$

Die letzte Zeile entspricht Gl. (5.5) bis auf eine Umordnung der Summanden. □

Da die Matrix M nach Gl. (5.6) orthonormale Spalten hat, kann Satz 2.39 angewandt werden. Es folgt, daß es eine unitäre Ergänzung $\tilde{M}$ von M gibt, die eine Symmetrie hat.

Satz 5.8 (Minimal störende Messung eines symmetrischen POVMs) *Es sei P ein POVM mit der Symmetrie (G, σ, π). Ferner seien A und B Matrizen, welche die Darstellungen $\sigma_\pi \otimes \sigma$ bzw. σ gemäß*

$$A(\sigma_\pi \otimes \sigma)A^\dagger = \bigoplus_{j=0}^{z-1}(I_{m_j} \otimes \kappa_j) \quad \textit{und} \quad B\sigma B^\dagger = \bigoplus_{j=0}^{z-1}(I_{n_j} \otimes \kappa_j)$$

in direkte Summen irreduzibler Komponenten κ_j zerlegen, wobei alle κ_j inäquivalent seien. Dann existiert eine Matrix $N \in \mathbb{C}^{dn \times d(n-1)}$, so daß

$$\tilde{M} := A^\dagger(AMB^\dagger|N)(B \oplus \tilde{B}) = (M|A^\dagger N\tilde{B})$$

das POVM für alle $\tilde{B} \in \mathcal{U}(d(n-1))$ mit minimaler Störung durchführt. Hierbei hat die Matrix $\tilde{M}$ die Symmetrie

$$(\sigma_\pi \otimes \sigma)\tilde{M} = \tilde{M}(\sigma \oplus \tilde{B}\tilde{\sigma}\tilde{B}^\dagger) \quad \textit{mit} \quad \tilde{\sigma} := \tilde{B}^\dagger \left(\bigoplus_{j=0}^{z-1}(I_{m_j - n_j} \otimes \kappa_j) \right) \tilde{B}\,.$$

Der Beweis von Satz 5.8 führt ähnlich wie in Abschnitt 4.2 zu einem Entwurfsprinzip für unitäre Transformationen zur Durchführung von Messungen mit minimaler Störung:

- Bestimme eine Symmetrie (G, σ, π) des POVMs
- Finde Zerlegungsmatrizen A und B für $\sigma_\pi \otimes \sigma$ bzw. σ
- Konstruiere $\tilde{\sigma}$ so, daß $A(\sigma \oplus \sigma_\pi)A^\dagger$ und $B\sigma B^\dagger \oplus \tilde{\sigma}$ bis auf die Reihenfolge der Komponenten gleich sind
- Finde N so, daß $(AMB^\dagger|N)$ unitär ist und im Verkettungsraum von $A(\sigma \oplus \sigma_\pi)A^\dagger$ und $B\sigma B^\dagger \oplus \tilde{\sigma}$ liegt
- Bilde $\tilde{M} := A^\dagger(AMB^\dagger|N)(B \oplus \tilde{B}) = (M|A^\dagger N\tilde{B})$ mit beliebigem unitären $\tilde{B}$

5.4 Gruppenerzeugte POVMs

Bei der Durchführung von gruppenerzeugten POVMs nach Kap. 4 kann die Fourier-Transformation der Symmetriegruppe genutzt werden, um die dort auftretende reguläre Darstellung σ_{mon} der Symmetrie $(G, \sigma, \sigma_{\text{mon}})$ von M in irreduzible Komponenten zu zerlegen (siehe Abschnitt 4.3). Dadurch wird die Zerlegung einer der Darstellungen vollständig auf die Fourier-Transformation reduziert. Bei der minimal störenden Durchführung gruppenerzeugter POVMs liegt ebenfalls die reguläre Darstellung vor:

Lemma 5.9 (Permutation bei gruppenerzeugten POVMs) *Es sei P ein gruppenerzeugtes POVM mit der Darstellung σ der Gruppe G, wobei $g_0, \ldots, g_{n-1}$ die Anordnung der Elemente sei. Dann hat M aus Gl. (5.5) die Symmetrie $(G, \sigma_\pi \otimes \sigma, \sigma)$, wobei σ_π die reguläre Darstellung von G ist.*

Beweis: Es sei $g_0, \ldots, g_{n-1}$ die Anordnung der Gruppenelemente. Mit den initialen Operator Π wird $\Pi_j := \sigma(g_j)\Pi\sigma(g_j)^\dagger$ definiert. Es folgt

$$\sigma(h)\Pi_j\sigma(h)^\dagger = \Pi_{\pi(h)(j)}$$

mit der Darstellung π aus Def. 2.5. □

Im Vergleich zur Durchführung aus Kap. 4 mit dem Naimark-Theorem gestaltet sich die Zerlegung der Darstellungen bei der Messung von gruppenerzeugten POVMs mit minimaler Störung schwieriger, denn im Gegensatz zu σ_{mon} aus Abschnitt 4.3 kann σ_π nicht immer alleine durch die Fourier-Matrix der Symmetriegruppe zerlegt werden, obwohl beide Darstellungen identisch sind; der Grund hierfür ist, daß die reguläre Darstellung σ_π nur als Komponente des Tensorprodukts $\sigma_\pi \otimes \sigma$ auftritt. Auch wenn sowohl σ_π als auch σ durch Konjugation mit C bzw. D in die direkten Summen

$$\bigoplus_{j=0}^{z-1}(I_{m_j} \otimes \kappa_j) \quad \text{und} \quad \bigoplus_{j=0}^{z-1}(I_{n_j} \otimes \kappa_j)$$

irreduzibler Darstellungen κ_j zerlegt werden, führt die Konjugation von $\sigma_\pi \otimes \sigma$ mit $C \otimes D$ nicht notwendigerweise zu einer Zerlegung von $\sigma_\pi \otimes \sigma$ in irreduzible Komponenten. Der Grund hierfür ist, daß Tensorprodukte $\kappa_j \otimes \kappa_\ell$ irreduzibler Darstellungen nicht irreduzibel sein müssen. Das Auffinden der Zerlegung von $\kappa_j \otimes \kappa_\ell$ in irreduzible Komponenten wird für lineare und speziell-lineare Gruppen als Clebsch-Gordan-Problem bezeichnet; die Zerlegung in irreduzible Komponenten wird hierbei durch die Littlewood-Richardson-Regel erhalten (siehe §25.3 in [FH91]).

Für die Durchführung gruppenerzeugter POVMs mit minimaler Störung ist demnach durch die Fourier-Transformation nur ein erster Schritt der Zerlegung von $\sigma_\pi \otimes \sigma$ in irreduzible Komponenten gegeben: Die Zerlegung von $\sigma_\pi \otimes \sigma$ wird auf die Zerlegung der Darstellungen σ und $\kappa_j \otimes \kappa_\ell$ reduziert. Die weiteren Schritte sind die Zerlegung der Darstellungen $\kappa_j \otimes \kappa_\ell$ in irreduzible Komponenten und die anschließende Sortierung der irreduziblen Darstellungen.

5.5 Beispiele

Das in Abschnitt 5.3 entwickelte Entwurfsprinzip kann sowohl bei POVMs mit zyklischer Symmetrie als auch bei POVMs mit Heisenberg-Weyl-Symmetrie angewandt werden, um effiziente, minimal störende Durchführungen zu erhalten. Im Vergleich zu den Meßalgorithmen aus Abschnitt 4.4 werden jedoch durch die zusätzliche Forderung der minimalen Störung kompliziertere Schaltkreise erhalten: Es werden größere Hilfssysteme benötigt und demnach auch mehr Ein-Qubit- und CNOT-Operationen.

5.5.1 Zyklische POVMs

Die zyklischen POVMs aus Def. 4.20 können gemäß den Diskussionen von Abschnitt 4.4.3 zur Ermittlung zeitlicher Information genutzt werden, indem die Zustände von Systemen mit periodischer Zeitentwicklung geschätzt werden. Diese Zustände entsprechen bei Qubits unter geeigneten Voraussetzungen Punkten auf der Bloch-Kugel, die im gleichen

Abstand auf dem Äquator liegen. Solche Zustände treten darüber hinaus auch bei der Phasenschätzung (*phase estimation*, siehe [CEMM98]) auf, bei der ein System im Zustand $|\Phi\rangle\langle\Phi|$ vorliegt, wobei $|\Phi\rangle$ Eigenvektor einer unitären Transformation U mit unbekanntem Eigenwert ω ist. Bei der Phasenschätzung soll ω ermittelt werden, wofür gesteuerte U^j-Gatter zur Verfügung stehen. Die Zustände mit der zyklischen Symmetrie folgen durch Anwendung der gesteuerten U^j-Gatter, denn dadurch wird die Zustandsentwicklung

$$\sqrt{\frac{1}{2}}(|0\rangle + |1\rangle) \otimes |\Phi\rangle \mapsto \sqrt{\frac{1}{2}}(|0\rangle + \omega^j|1\rangle) \otimes |\Phi\rangle$$

bei entsprechender Initialisierung des steuernden Qubits erhalten. Die Bestimmung des vorliegenden Zustands des Qubits mittels einer geeigneten Messung entspricht beispielsweise bei geeignetem U dem Faktorisierungsalgorithmus von Shor (siehe [CEMM98]).

Zum Entwurf eines Verfahrens, das die zylischen POVMs auf einem Qubit mit minimaler Störung mißt, werden die Gruppe $C_n := \langle r : r^n = 1\rangle$ und deren unitäre Darstellung $\sigma : C_n \to \mathcal{U}(2)$ mit $\sigma(r^j) = R_n^j$ für

$$R_n := \begin{pmatrix} 1 & 0 \\ 0 & \omega_n \end{pmatrix}$$

betrachtet, wobei $\omega_n := e^{2\pi i/n}$ eine n-te Einheitswurzel ist. Die Bahn des Vektors

$$\sqrt{\frac{1}{n}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{C}^2$$

besteht aus n Vektoren, die zu den POVM-Operatoren

$$\Pi_j := \frac{1}{n} \begin{pmatrix} 1 & 0 \\ 0 & \omega_n^j \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \omega_n^{-j} \end{pmatrix} = \frac{1}{n} \begin{pmatrix} 1 & \omega_n^{-j} \\ \omega_n^j & 1 \end{pmatrix} \tag{5.9}$$

mit $j \in \{0, \ldots, n-1\}$ führen. Gemäß Abschnitt 5.2 werden die Quadratwurzeln

$$\sqrt{\Pi_j} = \sqrt{\frac{1}{2n}} \begin{pmatrix} 1 & \omega_n^{-j} \\ \omega_n^j & 1 \end{pmatrix}$$

gebildet, welche nach Gl. (5.5) die Matrix

$$M = \sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_j} \in \mathbb{C}^{2n \times 2}$$

mit der durch $(X_n \otimes R_n)M = MR_n$ definierten Symmetrie zur Folge haben. Hierbei ist $\sigma_\pi(r^j) := X_n^j$ die reguläre Darstellung von C_n, und die Symmetrie von M folgt wegen

$$\begin{aligned} (X_n \otimes R_n)MR_n^\dagger &= (X_n \otimes R_n) \left(\sum_{j=0}^{n-1} |j\rangle \otimes \sqrt{\Pi_j} \right) R_n^\dagger \\ &= \sum_{j=0}^{n-1} |(j+1) \bmod n\rangle \otimes \sqrt{\Pi_{(j+1) \bmod n}} = M. \end{aligned}$$

Da das zyklische POVM ein gruppenerzeugtes POVM ist, werden die beiden Darstellungen σ_π und σ gemäß Abschnitt 5.4 getrennt zerlegt, denn dadurch kann für σ_π die Fourier-Transformation genutzt werden. Die anschließende Zerlegung der Darstellungen $\kappa_j \otimes \kappa_\ell$ in irreduzible Darstellungen ist hierbei trivial, denn die zyklische Gruppe hat nur irreduzible Darstellungen vom Grad eins und somit ist das Tensorprodukt $\kappa_j \otimes \kappa_\ell$ irreduzibler Darstellungen wieder irreduzibel (siehe Lemma 2.25 in [CB93]). Es wird zunächst die Darstellung $\sigma_\pi(r^j) = X_n^j$ zerlegt: Mit der Fourier-Transformation wird X_n zu der Phasenmatrix Z_n diagonalisiert, d. h. es gilt $F_n X_n F_n^\dagger = Z_n$ für F_n aus Def. 1.24. Die Symmetrie von M kann daher als Symmetrie

$$(Z_n \otimes R_n)((F_n \otimes I_2)M) = ((F_n \otimes I_2)M)R_n \tag{5.10}$$

von $(F_n \otimes I_2)M$ geschrieben werden. Hierbei sind schon alle Darstellungen der Symmetrie in irreduzible Komponenten zerlegt; diese werden in einem weiteren Schritt zu $Z_n \otimes I_2$ umsortiert, so daß gleiche Darstellungen direkt aufeinander folgen. Dies kann mit X_{2n} erreicht werden, denn es gilt $Z_n \otimes R_n = X_{2n}^\dagger (Z_n \otimes I_2) X_{2n}$. Durch Einsetzung in Gl. (5.10) wird

$$(Z_n \otimes I_2)\,(X_{2n}(F_n \otimes I_2)M) = (X_{2n}(F_n \otimes I_2)M)\,R_n \tag{5.11}$$

erhalten. Dies zeigt, daß mit der Notation von Satz 5.8 für $\sigma_\pi \otimes \sigma$ die Zerlegungsmatrix $A := X_{2n}(F_n \otimes I_2)$ genutzt werden kann; zusätzlich wird $B := I_2$ gesetzt, denn die Darstellung σ ist bereits eine direkte Summe irreduzibler Darstellungen. Es folgt deshalb die Matrixsymmetrie $(Z_n \otimes I_2)(AMB^\dagger) = (AMB^\dagger)R_n$ mit

$$AMB^\dagger = X_{2n}(F_n \otimes I_2)M = \sqrt{\frac{1}{2}} \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix} \in \mathbb{C}^{2n \times 2}.$$

Diese Matrix wird nach dem Entwurfsprinzip von Abschnitt 5.3 mittels einer Matrix N zu $(AMB^\dagger|N) \in \mathcal{U}(2n)$ erweitert, wobei

$$(Z_n \otimes I_2)(AMB^\dagger|N) = (AMB^\dagger|N)(I_2 \otimes Z_n)$$

die gewünschte Symmetrie festlegt[1]. Hierbei kann N so gewählt werden, daß $(AMB^\dagger|N)$ als Produkt $(I_n \otimes F_2)K^\dagger$ mit der Permutationsmatrix $K \in \mathcal{U}(2n)$ geschrieben werden kann, die durch

$$K|2j\rangle = |j\rangle \quad \text{und} \quad K|2j+1\rangle = |n+j\rangle$$

mit $j \in \{0, \ldots, n-1\}$ definiert ist.

[1]Zur Vereinfachung der Permutationen der Darstellungen wird das Implementierungsschema von Satz 5.8 leicht abgeändert, indem eine andere Anordnung der irreduziblen Darstellungen auf der rechten Seite betrachtet wird.

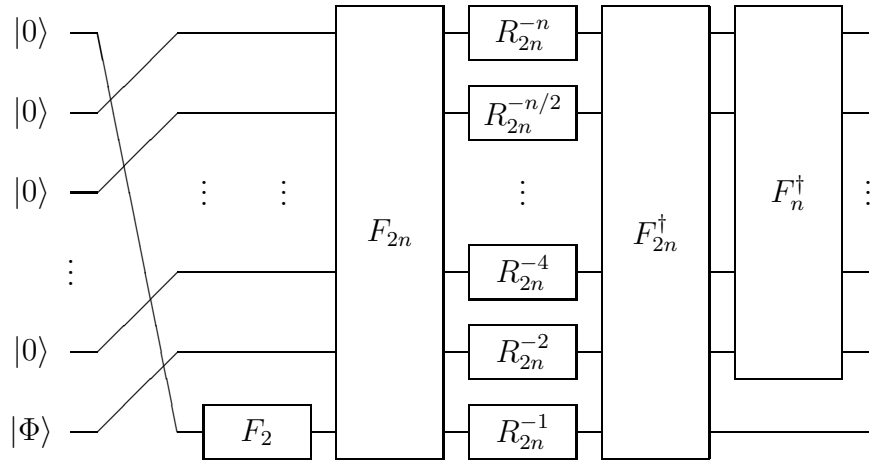

Abbildung 5.1: Schaltkreis für die Durchführung des zyklischen POVMs mit $n = 2^k$ Operatoren auf einem Qubit. Der Schaltkreis hat $k+1$ Qubits; auf der rechten Seite werden die oberen k Qubits in der Standardbasis gemessen. (Schaltkreis aus [JD06] übernommen.)

Satz 5.10 (Durchführung des zyklischen POVMs) *Das zyklische POVM auf einem Qubit mit n Operatoren kann mit*

$$\tilde{M} := A^\dagger(AMB^\dagger|N)(B \oplus \tilde{B}) = (F_n^\dagger \otimes I_2)X_{2n}^\dagger(I_n \otimes F_2)K^\dagger \in \mathcal{U}(2n)$$

minimal störend durchgeführt werden. Mit $\tilde{B} := I_{2n-2}$ folgt hierbei $B \oplus \tilde{B} = I_{2n}$.

Eine effiziente Implementierung von $\tilde{M}$ mit Ein-Qubit- und CNOT-Operationen kann für $n = 2^k$, $k \geq 1$, gefunden werden. Das gemessene Qubit wird hierbei um ein Quantenregister erweitert, das aus k Qubits besteht. Die unitäre Matrix K entspricht damit der zyklischen Verschiebung

$$|x_0 x_1 \ldots x_{k-1} x_k\rangle \mapsto |x_k x_0 x_1 \ldots x_{k-1}\rangle$$

von Qubits. Um die Matrix $X_{2n}^\dagger$ in Ein-Qubit- und CNOT-Gatter zu zerlegen, werden die Gleichungen $X_{2n}^\dagger = F_{2n}^\dagger Z_{2n}^\dagger F_{2n}$ und

$$Z_{2n}^\dagger = R_{2n}^{-n} \otimes R_{2n}^{-n/2} \otimes \ldots \otimes R_{2n}^{-1}$$

genutzt. Der Schaltkreis, welcher der unitären Transformation

$$\tilde{M} = (F_n^\dagger \otimes I_2)F_{2n}^\dagger(R_{2n}^{-n} \otimes R_{2n}^{-n/2} \otimes \ldots \otimes R_{2n}^{-1})F_{2n}(I_n \otimes F_2)K^\dagger$$

entspricht, ist in Abb. 5.1 gezeigt.

Korollar 5.11 (Aufwand des zyklischen POVMs) *Es sei $k \geq 1$. Dann kann das zyklische POVM auf einem Qubit mit den $n := 2^k$ Operatoren aus Gl. (5.9) mit dem Schaltkreis von Abb. 5.1 minimal störend durchgeführt werden. Dieser Schaltkreis kann in $O(k^2)$ Ein-Qubit- und CNOT-Operationen zerlegt werden.*

Beweis: Die F_n und F_{2n} können jeweils in $O(k^2)$ Ein-Qubit- und CNOT-Gatter zerlegt werden (siehe Satz 3.1 in [Röt01]). Die zyklische Verschiebung der Qubits kann durch $O(k)$ Ein-Qubit- und CNOT-Gatter ersetzt werden (siehe Satz 1.20 in [Röt01]). □

5.5.2 Heisenberg-Weyl-POVMs

Das Implementierungsschema von Abb. 4.6 läßt es zu, daß mit den Heisenberg-Weyl-POVMs aus Def. 4.25 Phasenraummessungen durchgeführt werden. So können beispielsweise der Ort und der Impuls eines Teilchens gleichzeitig gemessen werden. Sollen zur Verfolgung seiner Bewegung mehrere dieser Messungen aufeinander folgen, so ist es zweckmäßig, daß jede Messung das System minimal stört. Zur Konstruktion eines geeigneten Meßverfahrens sei $d \geq 2$ die Dimension des Systems und $G = \langle X_d, Z_d \rangle$ wie in Abschnitt 4.4.4 die Heisenberg-Weyl-Gruppe, die von X_d und Z_d erzeugt wird. Für einen semipositiven Operator Π mit $\mathrm{tr}(\Pi) = 1/d$ wird das POVM mit den d^2 Operatoren

$$Z_d^k X_d^j \Pi X_d^{-j} Z_d^{-k} \quad \text{für} \quad j,k = 0,\ldots,d-1$$

gebildet; im Gegensatz zu Abschnitt 4.4.4 kann Π ein initialer Operator von beliebigem Rang sein. Die Darstellung σ der Gruppe ist durch die Identitätsabbildung gegeben, d. h. es gelten $\sigma(X_d) = X_d$ und $\sigma(Z_d) = Z_d$. Die Matrix M von Gl. (5.5) ist durch

$$M = \sum_{j,k=0}^{d-1} |jd+k\rangle \otimes Z_d^k X_d^j \sqrt{\Pi} X_d^{-j} Z_d^{-k} \in \mathbb{C}^{d^3 \times d} \tag{5.12}$$

festgelegt. Die Symmetrie $(\sigma_\pi \otimes \sigma)M = M\sigma$ von M wird durch

$$(I_d \otimes X_d \otimes Z_d)\, M = M Z_d \quad \text{und} \quad (X_d \otimes I_d \otimes X_d)\, M = M X_d$$

vollständig beschrieben, da X_d und Z_d die Erzeuger der Symmetriegruppe sind. Gemäß Satz 5.8 wird die Darstellung $\sigma_\pi \otimes \sigma$ auf der linken Seite in eine direkte Summe von irreduziblen Darstellungen zerlegt, wobei zunächst die zyklischen Verschiebungen X_d der ersten und zweiten Tensorkomponente mit der Fourier-Transformation F_d diagonalisiert werden. Dadurch entstehen die Gleichungen

$$(I_d \otimes Z_d \otimes Z_d)\,((F_d \otimes F_d \otimes I_d)\, M) = ((F_d \otimes F_d \otimes I_d)\, M)\, Z_d$$

und

$$(Z_d \otimes I_d \otimes X_d)\,((F_d \otimes F_d \otimes I_d)\, M) = ((F_d \otimes F_d \otimes I_d)\, M)\, X_d\,.$$

Die Matrizen auf der linken Seite können als

$$(I_d \otimes Z_d \otimes Z_d) = \bigoplus_{j=0}^{d^2-1} \omega_d^{j \bmod d} Z_d \quad \text{und} \quad (Z_d \otimes I_d \otimes X_d) = \bigoplus_{j=0}^{d^2-1} \omega_d^{j \operatorname{div} d} X_d$$

geschrieben werden, wobei $j \operatorname{div} d$ den Ganzzahlanteil von j/d bezeichnet. Folglich wird die Darstellung in eine direkte Summe von Darstellungen zerlegt, die jeweils bis auf Phasenfaktoren die Darstellung σ sind. Diese Phasenfaktoren werden durch Konjugation mit geeigneten Matrizen beseitigt; zur Notationsvereinfachung werden dazu die Matrizen

$$X_{\mathrm{mod}} := \bigoplus_{j=0}^{d^2-1} X_d^{j \bmod d} \quad \text{und} \quad Z_{\mathrm{div}} := \bigoplus_{j=0}^{d^2-1} Z_d^{j \operatorname{div} d}$$

definiert. Die Matrizen X_{mod} und Z_{div} enthalten an den passenden Stellen diejenigen Potenzen von X_d und Z_d, die benötigt werden, um die Phasenfaktoren in $I_d \otimes Z_d \otimes Z_d$ bzw. $Z_d \otimes I_d \otimes X_d$ zu entfernen. Grundlage hierfür sind die Kommutatorrelationen

$$Z_d^\dagger X_d Z_d = \omega_d^{-1} X_d \quad \text{und} \quad X_d Z_d X_d^\dagger = \omega_d^{-1} Z_d \,,$$

welche die Gleichungen

$$X_{\mathrm{mod}} \left(\bigoplus_{j=0}^{d^2-1} \omega_d^{j \bmod d} Z_d \right) X_{\mathrm{mod}}^\dagger = \bigoplus_{j=0}^{d^2-1} Z_d$$

sowie

$$Z_{\mathrm{div}}^\dagger \left(\bigoplus_{j=0}^{d^2-1} \omega_d^{j \operatorname{div} d} X_d \right) Z_{\mathrm{div}} = \bigoplus_{j=0}^{d^2-1} X_d$$

zur Folge haben. Mit diesen kann

$$X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger \left(I_d \otimes Z_d \otimes Z_d\right) Z_{\mathrm{div}} X_{\mathrm{mod}}^\dagger = \left(I_d \otimes I_d \otimes Z_d\right)$$

und

$$X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger \left(Z_d \otimes I_d \otimes X_d\right) Z_{\mathrm{div}} X_{\mathrm{mod}}^\dagger = \left(I_d \otimes I_d \otimes X_d\right)$$

geschrieben werden, wobei keine Phasenfaktoren mehr vorhanden sind. Folglich können

$$\left(I_d \otimes I_d \otimes Z_d\right) X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger \left(\left(F_d \otimes F_d \otimes I_d\right) M\right) = X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger \left(\left(F_d \otimes F_d \otimes I_d\right) M\right) Z_d$$

und

$$\left(I_d \otimes I_d \otimes X_d\right) X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger \left(\left(F_d \otimes F_d \otimes I_d\right) M\right) = X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger \left(\left(F_d \otimes F_d \otimes I_d\right) M\right) X_d$$

erhalten werden. Diese beiden Gleichungen legen zusammen die durch

$$\left(I_d \otimes I_d \otimes \sigma\right) \left(AMB^\dagger\right) = \left(AMB^\dagger\right)\sigma \tag{5.13}$$

definierte Symmetrie von $AMB^\dagger = X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger (F_d \otimes F_d \otimes I_d) M$ fest. Mit der Notation von Satz 5.8 folgen die Matrizen

$$A := X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger (F_d \otimes F_d \otimes I_d) \;\text{ und }\; B := I_d, \tag{5.14}$$

weil σ schon eine irreduzible Darstellung ist (siehe Lemma 4.24). Die Matrix $AMB^\dagger$ ist ein Element des Verkettungsraums $\mathrm{Int}(I_d \otimes I_d \otimes \sigma, \sigma)$, womit sie nach Lemma 2.23 für ein geeignetes $|\Phi_0\rangle \in \mathbb{C}^{d^2}$ die Zerlegung

$$AMB^\dagger = |\Phi_0\rangle \otimes I_d \in \mathbb{C}^{d^3 \times d}$$

hat. Im Anhang B.3 wird gezeigt, daß

$$|\Phi_0\rangle := \left(F_d^\dagger \otimes I_d\right) \left(\sum_{q=0}^{d-1} |q\rangle\langle q| \otimes X_d^{-q} \right) \left(\sqrt{d} \sum_{j,k=0}^{d-1} \sqrt{\Pi}_{j,k} |j\rangle \otimes |k\rangle \right) \tag{5.15}$$

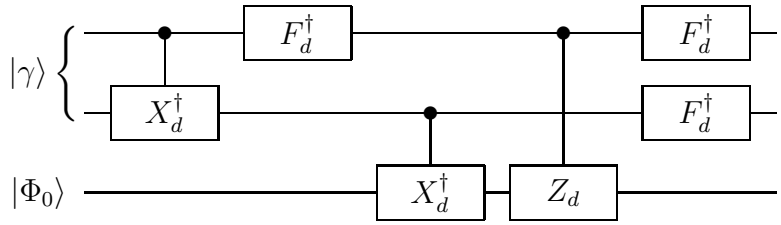

Abbildung 5.2: Schaltkreisschema für das POVM mit Heisenberg-Weyl-Symmetrie auf einem d-dimensionalen System. Der Basiszustand $|j\rangle\langle j|$ einer Steuerleitung bewirkt die Durchführung der j-ten Potenz der gesteuerten Operation. Auf der rechten Seite des Schaltkreises werden die beiden oberen Systeme in der Standardbasis gemessen (Abbildung aus [JD06] übernommen).

gilt, wobei $\sqrt{\Pi}_{j,k}$ den Eintrag von $\sqrt{\Pi}$ in der j-ten Zeile und k-ten Spalte bezeichnet. Die Darstellung σ auf der rechten Seite von Gl. (5.13) wird nach dem Entwurfsprinzip von Abschnitt 5.3 zu der direkten Summe, die aus d^2 Kopien von σ besteht, erweitert; da alle Darstellungen hierbei gleich sind, ist keine Sortierung der irreduziblen Komponenten notwendig. Die Matrix $(AMB^\dagger|N)$ des resultierenden Verkettungsraums muß nach Lemma 2.23 die Zerlegung $C \otimes I_d$ mit $C \in \mathcal{U}(d^2)$ haben, wobei die erste Spalte von C der Vektor $|\Phi_0\rangle$ ist. Um beliebige, orthogonale Spalten $|\Phi_j\rangle$ von C zu erhalten, wird $\{|\Phi_0\rangle\}$ zu einer ONB $\{|\Phi_0\rangle, |\Phi_1\rangle, \ldots, |\Phi_{d^2-1}\rangle\}$ von $\mathbb{C}^{d^2}$ ergänzt. Damit wird die unitäre Matrix

$$\tilde{M} := A^\dagger(AMB^\dagger|N)(B \oplus \tilde{B}) = A^\dagger(C \otimes I_d) = A^\dagger \left(\sum_{j=0}^{d^2-1} |\Phi_j\rangle\langle j| \otimes I_d \right) \tag{5.16}$$

gewonnen. Durch $\tilde{B} := I_{d(n-1)}$ kann $B \oplus \tilde{B} = I_{d^2}$ erhalten werden.

Satz 5.12 (Durchführung des Heisenberg-Weyl-POVMs) *Das Heisenberg-Weyl-POVM kann mit der Matrix $\tilde{M}$ aus Gl. (5.16) minimal störend durchgeführt werden.*

Es wird im folgenden analog zu Abschnitt 4.4.4 untersucht, wie ein POVM durch eine vom initialen Operator Π unabhängige Tranformation auf eine Zustandspräparation reduziert werden kann. Grundlage ist hierzu die Gleichung

$$\tilde{M}(|0\rangle \otimes |\Psi\rangle) = A^\dagger \left(\sum_{j=0}^{d^2-1} |\Phi_j\rangle\langle j| \otimes I_d \right) (|0\rangle \otimes |\Psi\rangle) = A^\dagger(|\Phi_0\rangle \otimes |\Psi\rangle),$$

die zeigt, daß die Implementierung von $C \otimes I_d$ in Gl. (5.16) ausgelassen werden kann, falls das Hilfssystem mit $|\Phi_0\rangle$ von Gl. (5.15) initialisiert wird. Insgesamt muß daher nur die unitäre Matrix

$$(F_d^\dagger \otimes F_d^\dagger \otimes I_d) Z_{\mathrm{div}} X_{\mathrm{mod}}^\dagger (F_d^\dagger \otimes I_d \otimes I_d) \left(\sum_{q=0}^{d-1} |q\rangle\langle q| \otimes X_d^{-q} \otimes I_d \right)$$

nach der Initialisierung des Hilfssystems mit dem Zustandsvektor

$$|\gamma\rangle := \sqrt{d} \sum_{j,k=0}^{d-1} \sqrt{\Pi}_{j,k} |j\rangle \otimes |k\rangle \in \mathbb{C}^{d^2} \tag{5.17}$$

durchgeführt werden.

Satz 5.13 (Schema für Heisenberg-Weyl-POVMs) *Das Heisenberg-Weyl-POVM kann mit dem Schema aus Abb. 5.2 durchgeführt werden, falls das Hilfssystem im Zustand $|\gamma\rangle\langle\gamma|$ ist, wobei $|\gamma\rangle$ in Gl. (5.17) definiert wird.*

Das Schema besteht nur aus Fourier-Transformationen, zyklischen Schiebematrizen und Phasenmatrizen, die zum Teil Steuerleitungen haben. Wird angenommen, daß diese Operationen effizient auf d-dimensionalen Systemen durchgeführt werden können, so folgt aus einer effizienten Präparation des Zustands $|\gamma\rangle$ ein effizientes Verfahren zur Durchführung des zugehörigen POVMs mit minimaler Störung. Bei Qubit-Registern ist diese Annahme gerechtfertigt, denn alle Gatter können geeignet zerlegt werden:

Korollar 5.14 (Aufwand des Heisenberg-Weyl-POVMs) *Es sei $d := 2^k$ mit $k \geq 1$. Dann kann der Schaltkreis aus Abb. 5.2 für das Heisenberg-Weyl-POVM in $O(k^2)$ Ein-Qubit- und CNOT-Gatter zerlegt werden.*

Beweis: Die gesteuerten $X_d^\dagger$-Operationen können durch Konjugation mit $F_d^\dagger$ in gesteuerte Z_d-Operationen umgewandelt werden. Da F_d in $O(k^2)$ Ein-Qubit- und CNOT-Gatter zerlegt werden kann (siehe Satz 3.1 in [Röt01]), müssen nur noch die gesteuerten Z_d- und $Z_d^\dagger$-Gatter untersucht werden. Jedes dieser Gatter kann wie in Abb. 4.7 in k einfach gesteuerte Z_d^j-Gatter zerlegt werden. Nach Gl. (4.24) kann jedes Z_d^j-Gatter in k Ein-Qubit-Gatter zerlegt werden, die jeweils einfach gesteuert sind. Insgesamt entstehen für jedes gesteuerte Z_d-Gatter $O(k^2)$ einfach gesteuerte Ein-Qubit-Gatter, die jeweils in vier Ein-Qubit- und zwei CNOT-Gatter zerlegt werden können (siehe Kor. 5.3 in [BBC$^+$95]). □

Durch Ersetzung aller Gatter mit geeigneten Operatoren kann das Schaltkreisschema von Abb. 5.2 auf unendlich-dimensionale Systeme erweitert werden (siehe [JD06]). Damit wird ein Meßverfahren gewonnen, um beispielsweise gleichzeitig den Ort und den Impuls eines Teilchens mit minimaler Störung zu messen. Weitere, ähnliche Verfahren werden in [ASFL05, BCM91, Ste92] vorgeschlagen. Den Verfahren ist gemein, daß die Initialisierung zweier Hilfssysteme die gemessenen POVMs festlegt. Dabei entspricht der Rang der POVM-Operatoren dem Verschränkungsgrad der Hilfssysteme (siehe Abschnitt 5.6.2 und [JD06, ASFL05]). Im Schema von Abb. 5.2 tritt diese Eigenschaft ebenfalls auf, wie anhand der Grenzfälle gesehen werden kann: Bei dem initialen Operator $\Pi = |\alpha\rangle\langle\alpha|/d$ vom Rang eins mit $|\alpha\rangle \in \mathbb{C}^d$ und $\langle\alpha|\alpha\rangle = 1$ folgt der Vektor $|\gamma\rangle = |\alpha\rangle \otimes |\overline{\alpha}\rangle$, der unverschränkten Hilfssystemen entspricht. Wird hingegen das triviale Heisenberg-Weyl-POVM gemessen, d. h. alle Operatoren sind die Identitätsmatrix I_d und haben daher vollen Rang, so gilt $|\gamma\rangle = \sum_j |j\rangle \otimes |j\rangle$, womit beide Hilfssysteme maximal verschränkt sind.

5.6 Experimentelle Durchführung

Wie bei der Durchführung von POVMs in Kap. 4, die auf dem Naimark-Theorem beruht, sind auch quantenoptische Experimente für die minimal störende Messung vorgeschlagen und in einigen Fällen durchgeführt worden. Im Vergleich zu der Durchführung nach dem Naimark-Theorem gibt es aber weniger Vorschläge und experimentelle Daten, denn durch die zusätzlichen Forderungen an den Zustand nach der Messung sind kompliziertere Versuchsaufbauten notwendig.

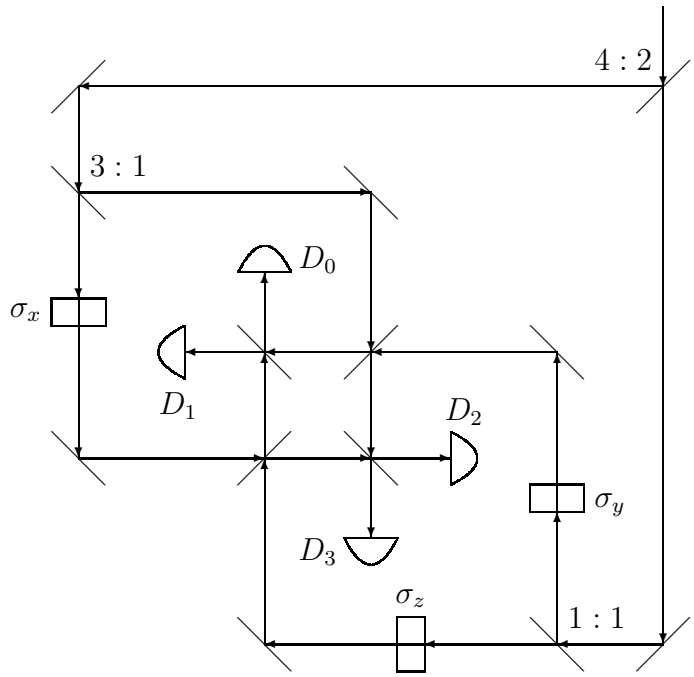

Abbildung 5.3: Aufbau nach [ŘEK04] zur Polarisationsmessung mit dem Tetraeder-POVM. Die vier Strahlteiler vor den Detektoren haben alle das Teilungsverhältnis 1 : 1.

5.6.1 Messung der Polarisation

Durch lineare optische Elemente können minimal störende Messungen der Polarisation durchgeführt werden. Als Hilfssysteme, die nach Abschnitt 5.2 mit dem zu messenden System wechselwirken müssen, werden die Moden der zu messenden Photonen genutzt.

Das Tetraeder-POVM

In [ŘEK04] wird für das Tetraeder-POVM aus Def. 4.12 der in Abb. 5.3 dargestellte Aufbau vorgeschlagen. Er besteht aus sieben Strahlteilern mit geeigneten Teilungsverhältnissen sowie vier Detektoren. Zusätzlich werden drei optische Elemente benötigt, welche die unitären Transformationen σ_x, σ_y und σ_z auf dem Polarisationszustand implementieren. Würde durch die Detektoren ein Photon so detektiert, daß es dabei nicht zerstört wird und darüber hinaus seine Polarisierung erhalten bleibt, so führte der Aufbau die Messung des Tetraeder-POVMs minimal störend durch (siehe [ŘEK04]). Hierbei ist jedoch nicht bekannt, wie diese Detektionen im Experiment erreicht werden können.

Verkettete Durchführung von POVMs

Die Reduktion der Polarisationsmessung auf die Modenmessung wie beim Tetraeder-POVM ist auch bei beliebigen POVMs möglich. In [AP05] wird hierfür ein Aufbau vorgeschlagen, der diese Reduktion bei beliebigen Kraus-Zerlegungen $\Pi_j = A_j^\dagger A_j \in \mathbb{C}^{2\times 2}$ ermöglicht, womit auch minimal störende Messungen durchgeführt werden können. Der Aufbau besteht bei n Operatoren aus $n-1$ hintereinander geschalteten Modulen, wobei jedes Modul so konstruiert wird, daß es einem POVM mit zwei Operatoren entspricht.

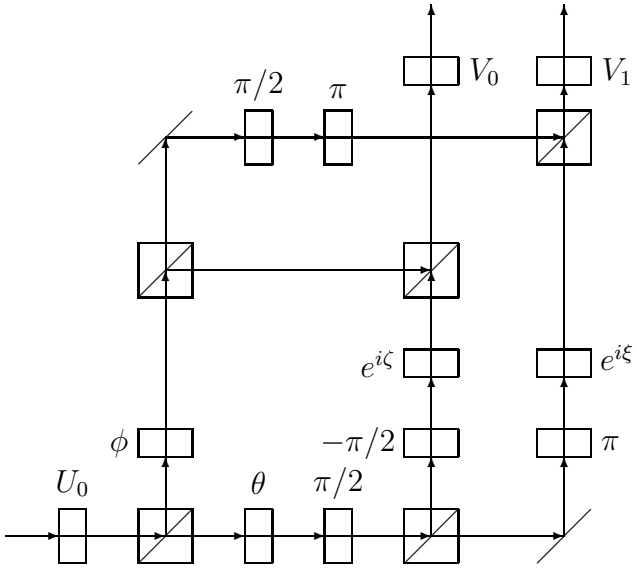

Abbildung 5.4: Modul von [AP05] zur Messung der Polarisation mit einem POVM, das die Kraus-Operatoren $A_0 = V_0 D_0 U_0$ und $A_1 = V_1 D_1 U_0$ hat. Die Winkel ξ, ζ, ϕ und θ werden über Gl. (5.18) durch D_0 und D_1 bestimmt.

Grundlage der Konstruktion eines Moduls zur Messung des POVMs mit den beiden Operatoren Π_0 und Π_1 ist die Singulärwertzerlegung $A_j = V_j D_j U_j$ der zugehörigen Kraus-Operatoren, wobei U_j sowie V_j unitär sind und D_j eine diagonale Matrix ist (siehe Th. 1 in [EF01]). Der Operator Π_0 wird durch U_0 diagonalisiert, womit

$$U_0 \Pi_0 U_0^\dagger = D_0^\dagger D_0 \quad \text{und} \quad U_0 \Pi_1 U_0^\dagger = I_2 - U_0 \Pi_0 U_0 = D_1^\dagger D_1$$

mit Diagonalmatrizen D_0 sowie D_1 resultieren. Diese Gleichungen zeigen, daß die Kraus-Operatoren die Zerlegungen $A_0 = V_0 D_0 U_0$ und $A_1 = V_1 D_1 U_0$ mit geeigneten V_j haben, wobei also $U_0 = U_1$ gilt. Die Diagonalmatrizen D_0 und D_1 können als

$$D_0 := \begin{pmatrix} e^{i\zeta}\cos(\theta) & 0 \\ 0 & \cos(\phi) \end{pmatrix} \quad \text{und} \quad D_1 := \begin{pmatrix} e^{i\xi}\sin(\theta) & 0 \\ 0 & \sin(\phi) \end{pmatrix} \tag{5.18}$$

mit geeigneten Winkeln ξ, ζ, ϕ und θ geschrieben werden, wodurch das POVM dem Modul von Abb. 5.4 entspricht, d. h. wird ohne Störung der Polarisation gemessen, durch welchen Ausgang das Photon das Modul verläßt, so liegen die Zustände

$$\frac{1}{\mathrm{tr}(\rho\Pi_0)} A_0 \rho A_0^\dagger \quad \text{bzw.} \quad \frac{1}{\mathrm{tr}(\rho\Pi_1)} A_1 \rho A_1^\dagger$$

mit den Wahrscheinlichkeiten $\mathrm{tr}(\rho\Pi_0)$ bzw. $\mathrm{tr}(\rho\Pi_1)$ vor (siehe [AP05]).

Die Messung von POVMs mit drei Operatoren wird durch die Verkettung zweier Module erreicht (siehe [AP05]). Wird Π_0 durch U_0 diagonalisiert, so gelten

$$U_0 \Pi_0 U_0^\dagger = D_0^\dagger D_0 \quad \text{und} \quad U_0(\Pi_1 + \Pi_2) U_0^\dagger = I_2 - U_0 \Pi_0 U_0^\dagger = D_1^\dagger D_1$$

mit geeigneten Diagonalmatrizen D_0 und D_1. Der Kraus-Operator A_0 kann hierbei wie im Fall von zwei POVM-Operatoren als $A_0 = V_0 D_0 U_0$ geschrieben werden. Ist D_1 inver-

tierbar[2], so bilden die beiden Operatoren

$$\tilde{\Pi}_1 := (D_1^\dagger)^{-1} U_0 \Pi_1 U_0^\dagger D_1^{-1} \quad \text{und} \quad \tilde{\Pi}_2 := (D_1^\dagger)^{-1} U_0 \Pi_2 U_0^\dagger D_1^{-1}$$

ein POVM mit den zugehörigen Kraus-Operatoren

$$\tilde{A}_1 := A_1 U_0^\dagger D_1^{-1} \quad \text{und} \quad \tilde{A}_2 := A_2 U_0^\dagger D_1^{-1} \,. \tag{5.19}$$

Mit zwei Modulen kann demnach das POVM durchgeführt werden, falls das erste Modul die beiden Kraus-Operatoren $V_0 D_0 U_0$ sowie $D_1 U_0$ implementiert und das zweite diejenigen aus Gl. (5.19): Die Hintereinanderausführung beider Module ergibt nämlich die beiden ursprünglichen Kraus-Operatoren

$$A_1 U_0^\dagger D_1^{-1} D_1 U_0 = A_1 \quad \text{und} \quad A_2 U_0^\dagger D_1^{-1} D_1 U_0 = A_2 \,.$$

In ähnlicher Weise können durch Verkettung mehrerer Module auch POVMs mit mehr als drei Operatoren gemessen werden (siehe [AP05]). Da für eine Messung mit n Operatoren $n-1$ Module benötigt werden, können beispielsweise die zyklischen POVMs aus Abschnitt 5.5.1 mit der Verkettung der Module nicht effizient durchgeführt werden.

In [AP06] wird der Aufbau so erweitert, daß die Polarisation zweier Photonen gemessen werden kann. Da dies nach [Cal02] allein mit linearen Elementen nicht möglich ist, wird bei diesem Aufbau durch Verschränkung die Polarisation zweier Photonen auf die Mode und die Polarisation eines Photons übertragen. Nach dieser Übertragung sind lineare Elemente ausreichend, um beliebige POVMs zu messen.

5.6.2 Messung mittels homodyner Detektion

Die in Abschnitt 4.5.3 diskutierte homodyne Detektion kann genutzt werden, um minimal störende Messungen durchzuführen. Dies ist beispielsweise in der Quantenkryptographie von Interesse, falls kohärente Zustände bei einem Schlüsselaustausch übertragen werden (siehe z. B. [Ral00a]). Hierbei stellt sich unter geeigneten Voraussetzungen heraus, daß die auf homodyner Detektion basierende Teleportation ein Verfahren ist, das bei einem gewünschten Informationsgewinn eine Messung mit minimaler Störung zuläßt (siehe [Ral00b]).

Teleportation

Die Grundaufgabe bei der Teleportation ist die Übertragung des Zustands eines Systems auf ein anderes System. Dabei wird angenommen, daß beide Systeme räumlich voneinander getrennt sind und daß verschränkte Systeme sowie Kommunikation mit nichtquantenmechanischen Systemen zur Verfügung stehen. Die Teleportation kann mit dem in Abb. 5.5a) dargestellten Aufbau erreicht werden (siehe [FSB+98]). Es wird dabei der verschränkte Zustand $|q\rangle\langle q|$ mit

$$|q\rangle := \sqrt{1-q^2} \sum_{n=0}^{\infty} q^n |n\rangle \otimes |n\rangle$$

[2]Falls D_1 nicht invertierbar ist, so gelten ohne Beschränkung der Allgemeinheit die Gleichungen $U_0 \Pi_1 U_0^\dagger = \alpha |0\rangle\langle 0|$ und $U_0 \Pi_2 U_0^\dagger = \beta |0\rangle\langle 0|$ mit geeigneten $\alpha, \beta \in \mathbb{R}$ aufgrund der Positivität von $U_0 \Pi_j U_0$. Damit können Π_1 und Π_2 zu einem Operator zusammengefaßt werden, da sie sich nur um einen skalaren Faktor unterscheiden.

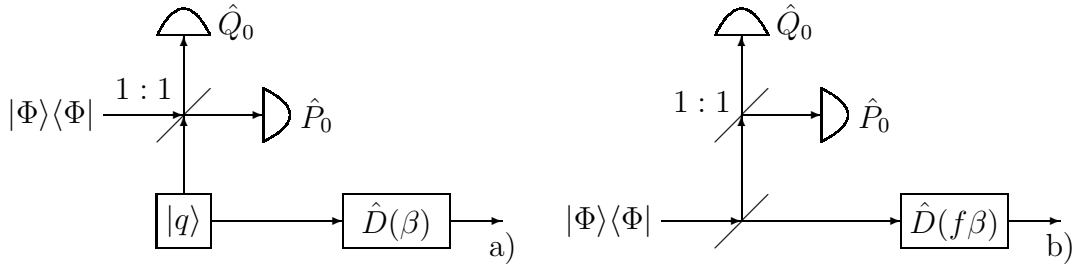

Abbildung 5.5: a) Aufbau zur Teleportation nach [HIKF00]. b) Strahlteilerschema nach [HIKF01] mit $f := 1 - q$. Der untere Strahlteiler hat den Reflexionskoeffizienten $\sqrt{1-q^2}$ und den Transmissionskoeffizienten q.

präpariert, wobei $|n\rangle \otimes |n\rangle$ dem Zustand entspricht, bei dem jede der beiden Moden jeweils genau n Photonen enthält. Der Parameter q gibt hierbei den Verschränkungsgrad an (siehe Abschnitt 5.2.5 in [WM95]); bei $q = 1$ läge eine vollständige Verschränkung vor, die aber nicht auftreten kann, da der zugehörige Zustand unendlich viel Energie hätte. Die erste Tensorkomponente des Zustands $|q\rangle\langle q|$ wird durch einen Strahlteiler des Teilungsverhältnisses 1 : 1 mit dem zu übertragenden Zustand $|\Phi\rangle\langle\Phi|$ überlagert. An den Ausgängen dieses Strahlteilers werden mit homodyner Detektion die Quadraturoperatoren $\hat{Q}_0$ bzw. $\hat{P}_0$ gemessen, wobei die Resultate q und p zu $\beta := q + ip \in \mathbb{C}$ zusammengefaßt werden. Liegt dieses Resultat vor, so wird der Zustand der anderen Tensorkomponente des verschränkten Zustands durch

$$|\Phi'(\beta)\rangle := \sqrt{\frac{1-q^2}{\pi}} \sum_{n=0}^{\infty} q^n |n\rangle\langle n|\hat{D}(-\beta)|\Phi\rangle$$

beschrieben (siehe [HIKF00]). Im Grenzfall $q \to 1$ resultiert der durch $\hat{D}(-\beta)|\Phi\rangle$ beschriebene Zustand, der bis auf den Verschiebeoperator $\hat{D}(-\beta)$ der ursprüngliche Zustand $|\Phi\rangle\langle\Phi|$ ist. Durch Anwendung von $\hat{D}(\beta)$ wird deshalb eine fehlerfreie Teleportation erreicht, womit β keine Information über $|\Phi\rangle\langle\Phi|$ enthalten kann. Da der Fall $q = 1$ aber nicht möglich ist, kann diese perfekte Rekonstruktion nicht erhalten werden[3]. Die Untersuchung des Falls $q < 1$ kann durch den Operator

$$\hat{T}(\beta) := \sqrt{\frac{1-q^2}{\pi}} \sum_{n=0}^{\infty} q^n \hat{D}(\beta)|n\rangle\langle n|\hat{D}(-\beta) \tag{5.20}$$

vereinfacht werden, mit dem der Zustand nach der Teleportation durch $|\Phi'(\beta)\rangle = \hat{T}(\beta)|\Phi\rangle$ beschrieben wird (siehe [HIKF00]), falls die Messung das Resultat β ergibt; dieser Fall tritt hierbei mit der Wahrscheinlichkeit $p(\beta) := \langle\Phi|\hat{T}(\beta)^\dagger\hat{T}(\beta)|\Phi\rangle$ auf. Durch die Darstellung

$$\hat{T}(\beta) = \sqrt{\frac{1-q^2}{\pi^3 q^2}} \int d^2\alpha \; e^{-\frac{1-q}{q}|\alpha-\beta|^2} |\alpha\rangle\langle\alpha|$$

dieses Operators (siehe [HIKF00]) wird deutlich, daß er für q nahe null, d. h. es liegt sehr wenig Verschränkung vor, ungefähr der Operator $|\beta\rangle\langle\beta|$ ist. Damit wird im Grenzfall, bei

[3]Im Gegensatz dazu ist die Teleportation endlich-dimensionaler Systeme perfekt möglich, d. h. der übertragene Zustand nach der Teleportation ist der ursprüngliche Zustand (siehe [BBC+93]).

dem keine Verschränkung vorliegt, aufgrund von $p(\beta) \approx |\langle\beta|\Phi\rangle|^2$ die Q-Funktion (siehe Abschnitt 3.7 in [GK05]) gemessen. Bei dem Resultat β liegt hierbei der Zustand $|\beta\rangle\langle\beta|$ nach der Messung vor. Dies zeigt, daß der Verschränkungsgrad wie in Abschnitt 5.5.2 festlegt, welche Information über den Zustand gewonnen wird und wie stark er bei der Messung gestört wird.

Die Teleportation wurde experimentell durchgeführt, wobei zwischen dem ursprünglichen und dem teleportierten Zustand die Güte

$$F\left(|\Phi\rangle\langle\Phi|, \hat{T}(\beta)|\Phi\rangle\langle\Phi|\hat{T}^\dagger(\beta)\right)^2 \approx 0,58$$

erhalten wurde (siehe [FSB+98]). Ein experimentelles Problem stellt die Präparation der verschränkten Zustände $|q\rangle\langle q|$ dar. Diese kann aber durch das Strahlteilerschema umgangen werden, falls nur die bei der Teleportation auftretende Zustandsabbildung relevant ist und nicht die Übertragung des Zustands selbst.

Strahlteilerschema

Das Strahlteilerschema folgt aus der Untersuchung, wie die Teleportation einen kohärenten Zustand $|\alpha\rangle\langle\alpha|$ in Abhängigkeit des gemessenen Resultats β überträgt. Mit dem Operator $\hat{T}(\beta)$ aus Gl. (5.20) wird der Zustand nach der Teleportation durch

$$\hat{T}(\beta)|\alpha\rangle = \sqrt{\frac{1-q^2}{\pi}} e^{-(1-q^2)\frac{|\alpha-\beta|^2}{2}} e^{(1-q)\frac{\alpha\overline{\beta}-\overline{\alpha}\beta}{2}} |q\alpha + (1-q)\beta\rangle \tag{5.21}$$

beschrieben (siehe [HIKF01]). Dieser entspricht bis auf einen Phasenfaktor und die Verschiebung um $(1-q)\beta$ dem kohärenten Zustand, der wie in Abb. 5.5b) durch einen Strahlteiler um den Faktor q abgeschwächt wird (siehe Abschnitt 5.1.5 in [BR04]) und dessen Quadraturoperatoren $\hat{Q}_0$ sowie $\hat{P}_0$ mit dem Verfahren aus Abschnitt 4.5.3 gemessen werden. Durch diese Messung wird für den nicht-reflektierten Teil der durch

$$|\Phi'\rangle := \sqrt{\frac{1-q^2}{\pi}} e^{-(1-q^2)\frac{|\alpha-\beta|^2}{2}} e^{(1-q^2)\frac{\alpha\overline{\beta}-\overline{\alpha}\beta}{2}} |q\alpha\rangle$$

beschriebene Zustand erhalten (siehe [HIKF01]). Die zusätzliche Phase und die Verschiebung um $(1-q)\beta$ von $\hat{T}(\beta)|\alpha\rangle$ aus Gl. (5.21) können durch eine Verschiebung nach dem Strahlteiler erhalten werden: Grundlage ist hierfür die Verknüpfungsregel

$$\hat{D}(\alpha)\hat{D}(\beta) = e^{\frac{\alpha\overline{\beta}-\overline{\alpha}\beta}{2}} \hat{D}(\alpha+\beta)$$

zweier Verschiebeoperatoren (siehe Abschnitt 11.3.1 in [MW95]), mit der

$$\hat{D}((1-q)\beta)|\Phi'\rangle = \hat{T}(\beta)|\alpha\rangle$$

folgt. Dies zeigt, daß durch den Strahlteiler, die Messung und die Verschiebung $\hat{D}((1-q)\beta)$ derselbe Zustand wie bei der Teleportation erhalten wird. Die Äquivalenz beider Verfahren gilt auch für beliebige Zustände, da sich jeder Zustand als Überlagerung kohärenter Zustände schreiben läßt (siehe Abschnitt 3.5 in [GK05]). Der Vorteil des Strahlteilerschemas im Vergleich zur Teleportation ist, daß keine verschränkten Zustände, sondern nur lineare Elemente und homodyne Detektion benötigt werden.

Minimale Störung bei gemessener Information

Ein Experiment mit dem Strahlteilerschema wird in [ASFL05] beschrieben. Hierbei wird untersucht, wie stark ein Zustand gestört werden muß, um eine bestimmte Information über diesen zu erhalten. Als Maß der erhaltenen Information und der Störung wird die Güte (siehe Def. 5.1) genutzt: Für die Störung wird die Güte $F := F(\rho, \rho')^2$ zwischen dem ursprünglichen Zustand $\rho = |\Phi\rangle\langle\Phi|$ und dem Zustand

$$\rho' := \hat{T}(\beta)|\Phi\rangle\langle\Phi|\hat{T}^\dagger(\beta)$$

nach der Messung untersucht. Für die bei der Messung gewonnene Information über den Zustand wird die Güte $G := F(\rho, \tilde{\rho})^2$ zwischen ρ und dem Zustand $\tilde{\rho}$ betrachtet, der durch Kenntnis der a-priori-Verteilung von ρ und den Meßresultaten präpariert werden kann (siehe [ASFL05]). Zwischen beiden Größen besteht die Ungleichung

$$F \leq \frac{1}{2}\frac{G}{1 - G - \sqrt{(1-G)(1-2G)}}\,, \tag{5.22}$$

die angibt, welche Güte F bei der Messung höchstens erhalten werden kann, falls eine bestimmte Information G über ρ erhalten werden soll (siehe [ASFL05]).

Im Experiment von [ASFL05] wurde der in Abb. 5.5b) dargestellte Aufbau genutzt. Der Zustand nach der Verschiebung $\hat{D}((1-q)\beta)$ wurde zur Bestimmung von F durch homodyne Detektion gemessen. Im Experiment konnte bei gegebener Güte G die nach der Ungleichung (5.22) maximal mögliche Güte F nahezu erreicht werden, falls die Effizienz der Detektion berücksichtigt wird.

Neben der minimal störenden Messung durch die Teleportation bzw. das Strahlteilerschema sind noch weitere Vorschläge bekannt, um minimal störende Messungen zu implementieren. Beispielsweise werden in [Ste92, BCM91] Hamilton-Operatoren angegeben, welche eine gemeinsame Messung des Ortes und des Impulses durch zwei Hilfssysteme zulassen. Darüber hinaus wird ein quantenoptischer Aufbau mit einem nicht-linearen optischen Element vorgeschlagen, um die Quadraturoperatoren zu messen.

Kapitel 6

Ausblick

Die Ergebnisse der vorliegenden Arbeit zeigen deutlich, daß Symmetrien sowohl bei der Optimierung als auch bei der Durchführung von Messungen in zahlreichen Fällen starke Vereinfachungen zur Folge haben. Darüber hinaus besteht zusätzlich die Möglichkeit, daß die im Rahmen der Untersuchungen entwickelten Techniken und neu gewonnenen Einsichten zu erfolgreichen Lösungsansätzen für einige bisher ungelöste Probleme der Quanteninformationstheorie führen:

- In [PW91, Woo05] wird die Frage diskutiert, ob Zustände, die in ein Tensorprodukt $|\Phi_0\rangle\langle\Phi_0| \otimes |\Phi_1\rangle\langle\Phi_1|$ zerfallen, auch immer durch POVMs mit Operatoren derselben Tensorzerlegung bzgl. der Transinformation optimal gemessen werden können. Bei den Doppeldrillingen ist dies der Fall, falls die in Abschnitt 3.6.2 numerisch bestimmte Transinformation maximal ist (siehe [Woo05]). Ebenso gilt dies für Zustände $|\Phi_j\rangle\langle\Phi_j| \otimes |\Phi_k\rangle\langle\Phi_k|$ zweier unkorrelierter Systeme, d. h. die Wahrscheinlichkeit, daß $|\Phi_j\rangle\langle\Phi_j|$ auftritt, ist von $|\Phi_k\rangle\langle\Phi_k|$ unabhängig und umgekehrt (siehe Th. 2 in [SKIH98]). Bilden wie bei den Doppeldrillingen symmetrische Zustände die Grundlage der Untersuchungen, so können durch das Tensorprodukt Darstellungen entstehen, die nicht irreduzibel sind. Deshalb bietet Satz 3.24 neue Vereinfachungen für die in [PW91, Woo05] behandelte Frage.

- Bei der Zustandstomographie soll ein unbekannter Zustand ermittelt werden, wobei viele Kopien des Zustands zur Verfügung stehen und für jede Kopie eine andere Messung möglich ist. Werden zur Vereinfachung die Messungen unabhängig von den vorher erhaltenen Resultaten gewählt, so ist der Fehler bei dieser Messung minimal, falls *Mutually Unbiased Bases* (MUBs) verwendet werden (siehe [WF89]). Für ein d-dimensionales System sind dies Orthonormalbasen $B_j := \{|\Psi_{j,k}\rangle\}$ mit der zusätzlichen Eigenschaft
$$|\langle\Psi_{j,k}|\Psi_{j',k'}\rangle|^2 = \frac{1}{d}$$
für alle k und k' sowie $j \neq j'$. Für $d := 2$ sind beispielsweise $B_0 := \{|0\rangle, |1\rangle\}$,
$$B_1 := \left\{\sqrt{\frac{1}{2}}\begin{pmatrix}1\\1\end{pmatrix}, \sqrt{\frac{1}{2}}\begin{pmatrix}1\\-1\end{pmatrix}\right\} \quad \text{und} \quad B_2 := \left\{\sqrt{\frac{1}{2}}\begin{pmatrix}1\\i\end{pmatrix}, \sqrt{\frac{1}{2}}\begin{pmatrix}1\\-i\end{pmatrix}\right\}$$
drei MUBs. Bei Primzahlpotenzen $d := p^m$ sind Konstruktionen für $d+1$ MUBs bekannt (siehe z. B. [GHW04]). Für die anderen Dimensionen ist nur bekannt,

daß die maximale Anzahl von MUBs jeweils zwischen drei und $d+1$ liegt (siehe [BBRV02]). Möglicherweise können durch Symmetrieannahmen weitere Konstruktionen für MUBs gefunden werden.

- Neben MUBs können bei der Zustandstomographie auch SIC-POVMs (*Symmetric Informationally Complete* POVMs, siehe z. B. [RBKSC04]) genutzt werden. Für ein d-dimensionales System besteht ein SIC-POVM aus d^2 Operatoren

$$\Pi_j := \frac{1}{d} |\Psi_j\rangle\langle\Psi_j|$$

mit den zusätzlichen Forderungen

$$\langle\Psi_j|\Psi_j\rangle = 1 \quad \text{und} \quad |\langle\Psi_j|\Psi_k\rangle|^2 = \frac{1}{d+1} \quad \text{für} \quad j \neq k\,.$$

Bei $d := 2$ gibt es beispielsweise ein SIC-POVM mit den Operatoren

$$\frac{1}{2}|\Psi\rangle\langle\Psi|,\ \frac{1}{2}Z_2|\Psi\rangle\langle\Psi|Z_2,\ \frac{1}{2}X_2|\Psi\rangle\langle\Psi|X_2 \ \text{ und } \ \frac{1}{2}Z_2X_2|\Psi\rangle\langle\Psi|X_2Z_2$$

für den Vektor

$$|\Psi\rangle := \sqrt{\frac{1}{6}} \begin{pmatrix} \sqrt{3+\sqrt{3}} \\ e^{i\pi/4}\sqrt{3-\sqrt{3}} \end{pmatrix}$$

und den Matrizen X_2 sowie Z_2 aus Def. 4.11. Das POVM ist damit ein spezielles Heisenberg-Weyl-POVM. Es wird vermutet, daß für beliebige endliche Dimensionen Operatoren $|\Psi\rangle\langle\Psi|$ existieren, die mit der Heisenberg-Weyl-Gruppe zu einem SIC-POVM führen (siehe z. B. [RBKSC04, App05, Gra04]). Falls Konstruktionen für SIC-POVMs gefunden werden, schließt sich unmittelbar die Frage an, ob sich diese mit den in Abschnitt 4.4.4 und 5.5.2 bereitgestellten Methoden auch effizient durchführen lassen.

Neben diesen Fragestellungen der Quanteninformationstheorie bieten sich als Ausgangspunkt weiterführender Untersuchungen unmittelbar die Probleme der verborgenen Untergruppen an. Hierfür bieten die in der vorliegenden Arbeit entworfenen symmetriebasierten Verfahren möglicherweise einen neuen Weg, um effiziente Quantenalgorithmen zu konstruieren.

Anhang A

Notationen und Symbole

Mengen und Gruppen

$\mathbb{C}, \mathbb{N}, \mathbb{R}$	komplexe, natürliche, reelle Zahlen
$\mathrm{GL}(\mathbb{C}, d)$	invertierbare $(d \times d)$-Matrizen über $\mathbb{C}$
$\mathcal{O}(d)$, $\mathcal{U}(d)$	orthogonale, unitäre Gruppe
P, S	POVM, Ensemble (siehe Def. 1.29 und Def. 1.6)
C_n, ω_n	zyklische Gruppe mit n Elementen, n-te Einheitswurzel
S_n	symmetrische Gruppe auf n Elementen

Vektoren, Operatoren und Matrizen

$\|\Phi\rangle$, $\langle\Phi\|$, $\|j\rangle$	Ket, Bra (siehe Def. 1.1) und j-ter Vektor der Standardbasis
I_d, I	Identitätsmatrix der Größe $d \times d$, Identitätsoperator
F_d	DFT-Matrix (siehe Def. 1.24)
X_d, Z_d	Schiebe- und Phasenmatrix (siehe Def. 4.11)
ρ	Dichtematrix (siehe Def. 1.5)
$\mathrm{tr}(A)$	Spur von A
Π, Π_j, $A_{j,k}$	POVM-, Kraus-Operator (siehe Def. 1.29 und Def. 1.27)
σ_x, σ_y, σ_z	Pauli-Matrizen (siehe Def. 1.9)
$\mathcal{P}$, $\mathcal{Q}$	Impulsoperator, Ortsoperator
$(M\|N)$	Zusammensetzung von Matrizen (Def. 2.34)
$\hat{D}(\alpha)$	Verschiebeoperator (siehe Gl. (4.28))
$\|\alpha\rangle\langle\alpha\|$	kohärenter Zustand (siehe Def. 4.30)

Darstellungen

σ, τ	Darstellungen (siehe Def. 2.1)
$\mathrm{Int}(\sigma, \tau)$	Verkettungsraum von σ und τ (siehe Def. 2.21)
π, σ_π	Permutationsdarstellung, Matrixform von π (siehe Def. 5.6)
σ_{mon}, σ_{reg}	monomiale, reguläre Darstellung (siehe Def. 2.5)
$\deg(\sigma)$	Grad von σ (siehe Def. 2.1)
κ, κ_j	irreduzible Darstellungen (siehe Def. 2.3)

Anhang B

Beweise und Konstruktionen

B.1 Ergänzung mehrerer irreduzibler Darstellungen

In Lemma 2.36 wird eine Matrix M mit orthonormalen Spalten und der Symmetrie

$$(\sigma \oplus (I_m \otimes \kappa))M = M(\tau \oplus (I_n \otimes \kappa)) \tag{B.1}$$

um $(m-n)\deg(\kappa)$ Spalten erweitert. Gleichzeitig wird die Darstellung auf der rechten Seite von Gl. (B.1) um $m-n$ irreduzible Komponenten κ ergänzt. Durch mehrfache Anwendung des Lemmas können alle irreduziblen Darstellungen der Symmetrie einer Matrix nacheinander angeglichen werden, während die Matrix jeweils um orthonormale Spalten ergänzt wird. Damit hierbei Lemma 2.36 direkt angewandt werden kann, müssen die irreduziblen Komponenten der Darstellungen umgeordnet werden:

Lemma B.1 (Permutation von Darstellungen) *Es sei $\sigma_0 \oplus \ldots \oplus \sigma_{p-1}$ die direkte Summe von p Darstellungen einer Gruppe G und $\pi \in S_p$ sei eine Permutation der zugehörigen Indizes $0, \ldots, p-1$. Dann existiert eine Permutationsmatrix U, welche durch die Konjugation*

$$U(\sigma_0 \oplus \ldots \oplus \sigma_{p-1})U^\dagger = \sigma_{\pi(0)} \oplus \ldots \oplus \sigma_{\pi(p-1)} \tag{B.2}$$

die Komponenten der direkten Summe gemäß π umpermutiert.

Beweis: Für $d := \deg(\sigma_0) + \ldots + \deg(\sigma_{p-1})$ sei

$$U := \begin{pmatrix} U_{0,0} & \ldots & U_{0,p-1} \\ \vdots & \ddots & \vdots \\ U_{p-1,0} & \ldots & U_{p-1,p-1} \end{pmatrix} \in \mathcal{U}(d)$$

die Matrix mit den Blöcken $U_{j,k}$ der Größe $d_{\pi(j)} \times d_k$, wobei $d_j := \deg(\sigma_j)$ der Grad von σ_j ist. Gilt $U_{j,\pi(j)} := I_{d_{\pi(j)}}$ für $j \in \{0, \ldots, p-1\}$ und sind alle anderen Blöcke Nullmatrizen passender Größe, so ist U eine Matrix, die Gl. (B.2) erfüllt. □

Durch Anwendung einer geeigneten Permutationsmatrix kann gezeigt werden, daß die Darstellung, die in Lemma 2.36 ergänzt wird, nicht als letzte Komponente der direkten Summe auftreten muß.

Lemma B.2 (Ergänzung mit Permutation) *Es sei M eine Matrix mit orthonormalen Spalten und der Symmetrie*

$$(\sigma_0 \oplus (I_m \otimes \kappa) \oplus \sigma_1)M = M(\tau_0 \oplus (I_n \otimes \kappa) \oplus \tau_1)\,, \tag{B.3}$$

wobei κ irreduzibel ist und in $\sigma_0 \oplus \sigma_1$ sowie $\tau_0 \oplus \tau_1$ jeweils die Multiplizität null hat. Dann existiert eine Matrix N, so daß die Zusammensetzung $\tilde{M} = (M|N)$ orthonormale Spalten und die Symmetrie

$$(\sigma_0 \oplus (I_m \otimes \kappa) \oplus \sigma_1)\tilde{M} = \tilde{M}(\tau_0 \oplus (I_n \otimes \kappa) \oplus \tau_1 \oplus (I_{m-n} \otimes \kappa))$$

hat, wobei die Darstellung auf der rechten Seite im Vergleich zu Gl. (B.3) um $m-n$ Komponenten κ ergänzt wird.

Beweis: Nach Lemma B.1 gibt es Permutationsmatrizen U und V, für die

$$U(\sigma_0 \oplus \sigma_1 \oplus (I_m \otimes \kappa))U^\dagger M = MV(\tau_0 \oplus \tau_1 \oplus (I_n \otimes \kappa))V^\dagger$$

gilt. Da κ in $\sigma_0 \oplus \sigma_1$ und $\tau_0 \oplus \tau_1$ jeweils die Multiplizität null hat, kann nach Lemma 2.36 die Matrix $U^\dagger MV$ um $p := (m-n)\deg(\kappa)$ orthonormale Spalten zu $M' := (U^\dagger MV|N)$ ergänzt werden, welche die Symmetrie

$$(\sigma_0 \oplus \sigma_1 \oplus (I_m \otimes \kappa))M' = M'(\tau_0 \oplus \tau_1 \oplus (I_n \otimes \kappa) \oplus (I_{m-n} \otimes \kappa))$$

hat. Da $V^\dagger \oplus I_p$ die rechte Darstellung

$$\tau_0 \oplus \tau_1 \oplus (I_n \otimes \kappa) \oplus (I_{m-n} \otimes \kappa) \quad \text{zu} \quad \tau_0 \oplus (I_n \otimes \kappa) \oplus \tau_1 \oplus (I_{m-n} \otimes \kappa)$$

permutiert, folgt die Aussage des Lemmas für die Matrix N aufgrund

$$\tilde{M} = UM'(V^\dagger \oplus I_p) = (M|N)\,.$$

□

Dieses Lemma kann mehrmals angewandt werden, um wie in Kor. 2.38 alle Multiplizitäten n_j auf m_j zu erhöhen.

Beweis von Kor. 2.38: Die Darstellungen $\kappa_0, \kappa_1, \ldots, \kappa_{z-1}$ werden nacheinander ergänzt. Bei der Ergänzung von $m_\ell - n_\ell$ Darstellungen κ_ℓ wird von der Symmetrie aus Gl. (B.3) mit der schon ergänzten Matrix M ausgegangen, wobei

$$\sigma_0 := \bigoplus_{j=0}^{\ell-1}(I_{m_j} \otimes \kappa_j) \quad \text{und} \quad \sigma_1 := \bigoplus_{j=\ell+1}^{z-1}(I_{m_j} \otimes \kappa_j)$$

auf der linken Seite sowie

$$\tau_0 := \bigoplus_{j=0}^{\ell-1}(I_{n_j} \otimes \kappa_j) \quad \text{und} \quad \tau_1 := \bigoplus_{j=\ell+1}^{z-1}(I_{n_j} \otimes \kappa_j) \oplus \bigoplus_{j=0}^{\ell-1}(I_{m_j-n_j} \otimes \kappa_j)$$

auf der rechten Seite stehen. Dabei ist die direkte Summe von $j=0$ bis $j=-1$ die leere Summe. Weiterhin werden $\kappa := \kappa_\ell$, $m := m_\ell$ und $n := n_\ell$ definiert. Da κ in $\sigma_0 \oplus \sigma_1$ und in $\tau_0 \oplus \tau_1$ jeweils die Multiplizität null hat, kann Lemma B.2 angewandt werden, um $m_\ell - n_\ell$ Komponenten κ_ℓ zu ergänzen. □

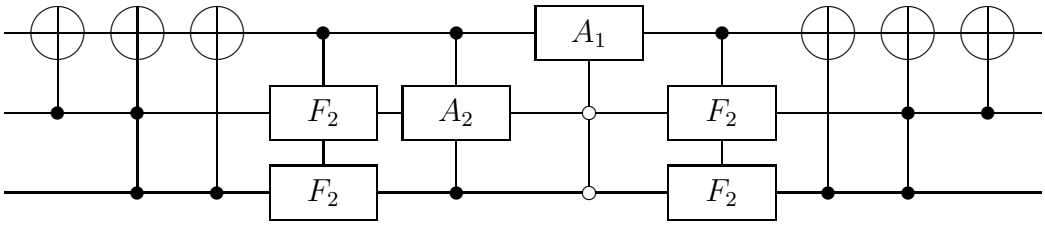

Abbildung B.1: Schaltkreis für $F_5 \oplus I_3$ auf drei Qubits. Das Symbol $\circ$ bedeutet, daß auf der steuernden Leitung vor und nach dem Gatter die Operation σ_x ausgeführt wird.

B.2 Einbettung der Fourier-Transformation

In diesem Abschnitt wird ein Schaltkreis zur Durchführung der Fourier-Transformation F_5 auf drei Qubits konstruiert; hierbei wird die Einbettung $F_5 \oplus I_3$ der DFT-Matrix in den achtdimensionalen Raum zugrunde gelegt, wie sie in Abschnitt 4.4.1 zur Durchführung des Dodekaeder-POVMs genutzt wird. Grundlage einer möglichen Zerlegung in Ein-Qubit- und CNOT-Gatter ist die Gleichung

$$F_5 \oplus I_3 = P^\dagger (I_4 \oplus (F_2 \otimes F_2)) M (I_4 \oplus (F_2 \otimes F_2)) P \tag{B.4}$$

mit den durch

$$M := \begin{pmatrix} a & \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ b & \cdot & \cdot & \cdot & c & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & d & \cdot & e \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & e & \cdot & f \end{pmatrix} \quad \text{und} \quad P := \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

definierten Matrizen für $a := \sqrt{1/5}$, $b := \sqrt{4/5}$, $c := -a$,

$$d := (\sqrt{10} - \sqrt{50})\, g\,, \quad e := \sqrt{40}\, g \quad \text{und} \quad f := -d \quad \text{mit} \quad g := i\, \frac{\sqrt{5+\sqrt{5}}}{20}\,.$$

Die mit $\cdot$ gekennzeichneten Einträge von M und P sind null. Die Zerlegung von $F_5 \oplus I_3$ wird durch das Rader-Verfahren (siehe Abschnitt 4.2 in [CB93]) nahe gelegt und folgt, indem Gl. (B.4) als Ansatz betrachtet wird und unter den 40320 Permutationsmatrizen $P \in U(8)$ diejenige gewählt wird, die in einen einfachen Schaltkreis übersetzt werden kann und darüber hinaus ein möglichst einfaches M zur Folge hat. Ein Schaltkreis, der dem Produkt aus Gl. (B.4) für das gefundene P entspricht, ist in Abb. B.1 dargestellt, wobei die beiden gesteuerten Gatter

$$A_1 := \begin{pmatrix} a & b \\ b & c \end{pmatrix} \quad \text{und} \quad A_2 := \begin{pmatrix} d & e \\ e & f \end{pmatrix}$$

der Matrix M entsprechen. Die Fourier-Transformationen $I_4 \oplus (F_2 \otimes F_2)$ werden mit den F_2-Gattern durchgeführt, die Permutationen P und $P^\dagger$ jeweils mit den drei gesteuerten σ_x-Gatter am Anfang bzw. Ende. Eine obere Schranke des Aufwands folgt, indem alle Transformationen in Ein-Qubit- und CNOT-Gatter zerlegt werden:

Satz B.3 (Aufwand der eingebetteten Transformation) *Die Fourier-Transformation $F_5 \oplus I_3$ kann mit* 44 *Ein-Qubit- und* 32 *CNOT-Gattern auf einem Drei-Qubit-Register durchgeführt werden.*

Beweis: Die $\circ$-Eingänge von A_1 in Abb. B.1 können insgesamt durch vier σ_x in $\bullet$-Eingänge überführt werden. Damit umfaßt der Schaltkreis jeweils vier σ_x, CNOT, einfach gesteuerte F_2 und doppelt gesteuerte Gatter. Die F_2 können nach Lemma 5.5 in [BBC$^+$95] jeweils durch zwei Ein-Qubit- und ein CNOT-Gatter ersetzt werden. Ferner kann jede doppelt gesteuerte Operation nach Kor. 6.2 von [BBC$^+$95] in acht Ein-Qubit- und sechs CNOT-Gatter zerlegt werden. □

Der für $F_5 \oplus I_3$ gefundene Schaltkreis legt nahe, daß durch die Reduktion von F_5 auf $F_2 \otimes F_2$ der Aufwand von $F_5 \oplus I_3$ im Vergleich zu einer Zerlegung, die für beliebige Transformationen genutzt werden kann, verringert wird. In [VMS04] wird beispielsweise eine Methode angegeben, mit der ein beliebiges Drei-Qubit-Gatter in bis zu 72 Ein-Qubit- und 64 CNOT-Gatter zerlegt wird.

B.3 POVMs mit Heisenberg-Weyl-Symmetrie

In Abschnitt 5.5.2 wird die minimal störende Durchführung des Heisenberg-Weyl-POVMs aus Def. 4.25 untersucht. Dabei wird gemäß Satz 5.8 für M aus Gl. (5.12) die Matrix

$$AMB^\dagger = X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger (F_d \otimes F_d \otimes I_d) M \ \in \ \mathrm{Int}(I_d \otimes I_d \otimes \sigma, \sigma)$$

erhalten, wobei A und B Zerlegungsmatrizen der Darstellungen $\sigma_\pi \otimes \sigma$ bzw. σ sind, welche zusammen die Symmetrie $(\sigma_\pi \otimes \sigma)M = M\sigma$ festlegen. Im folgenden wird gezeigt, daß $AMB^\dagger = |\Phi_0\rangle \otimes I_d$ mit dem durch Gl. (5.15) definierten Vektor $|\Phi_0\rangle$ gilt. Hierzu wird

$$\sqrt{\Pi} = \sum_{j=0}^{d-1} X_d^j \Delta_j \in \mathbb{C}^{d\times d}$$

mit passenden Diagonalmatrizen $\Delta_j \in \mathbb{C}^{d\times d}$ geschrieben, womit Gl. (5.12) in

$$\begin{aligned} M &= \sum_{j,k=0}^{d-1} |jd+k\rangle \otimes Z_d^k X_d^j \sqrt{\Pi} X_d^{-j} Z_d^{-k} \\ &= \sum_{j,k=0}^{d-1} |jd+k\rangle \otimes Z_d^k X_d^j \left(\sum_{\ell=0}^{d-1} X_d^\ell \Delta_\ell \right) X_d^{-j} Z_d^{-k} \\ &= \sum_{j,k,\ell=0}^{d-1} |jd+k\rangle \otimes Z_d^k X_d^\ell (X_d^j \Delta_\ell X_d^{-j}) Z_d^{-k} \end{aligned}$$

umgeformt werden kann. Ferner werden die Gleichungen

$$\begin{aligned} M &= \sum_{j,k,\ell=0}^{d-1} |jd+k\rangle \otimes Z_d^k X_d^\ell (X_d^j \Delta_\ell X_d^{-j}) Z_d^{-k} \\ &= \sum_{j,k,\ell=0}^{d-1} |jd+k\rangle \otimes Z_d^k X_d^\ell Z_d^{-k} (X_d^j \Delta_\ell X_d^{-j}) \\ &= \sum_{j,k,\ell=0}^{d-1} \omega_d^{k\ell} |jd+k\rangle \otimes X_d^\ell (X_d^j \Delta_\ell X_d^{-j}) \end{aligned}$$

erhalten, weil $X_d Z_d^{-1} = \omega_d Z_d^{-1} X_d$ gilt und $X_d^j \Delta_\ell X_d^{-j}$ eine Diagonalmatrix ist. Im nächsten Schritt wird M mit der Fourier-Transformation

$$I_d \otimes F_d \otimes I_d = \sqrt{\frac{1}{d}} \sum_{p,q,r=0}^{d-1} \omega_d^{qr} |pd+q\rangle\langle pd+r| \otimes I_d$$

multipliziert, so daß die Matrix

$$\begin{aligned} M_1 &:= (I_d \otimes F_d \otimes I_d) M \\ &= \left(\sqrt{\frac{1}{d}} \sum_{p,q,r=0}^{d-1} \omega_d^{qr} |pd+q\rangle\langle pd+r| \otimes I_d \right) \left(\sum_{j,k,\ell=0}^{d-1} \omega_d^{k\ell} |jd+k\rangle \otimes X_d^\ell (X_d^j \Delta_\ell X_d^{-j}) \right) \\ &= \sqrt{d} \sum_{p,q=0}^{d-1} |pd+q\rangle \otimes X_d^{-q} (X_d^p \Delta_{-q \bmod d} X_d^{-p}) \end{aligned}$$

resultiert. Die anschließende Multiplikation mit

$$F_d \otimes I_d \otimes I_d = \sqrt{\frac{1}{d}} \sum_{j,k,\ell=0}^{d-1} \omega_d^{jk} |jd+\ell\rangle\langle kd+\ell| \otimes I_d$$

hat die Summe

$$M_2 := (F_d \otimes I_d \otimes I_d) M_1 = \sum_{j,k,\ell=0}^{d-1} \omega_d^{jk} |jd+\ell\rangle \otimes X_d^{-\ell} (X_d^k \Delta_{-\ell \bmod d} X_d^{-k})$$

zur Folge. Es wird nun zuerst die Phasenmatrix $Z_{\mathrm{div}}^\dagger$ und danach die zyklische Schiebematrix X_{mod} angewandt. Dies entspricht der Multiplikation mit

$$X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger = \sum_{p,q=0}^{d-1} |pd+q\rangle\langle pd+q| \otimes X_d^q Z_d^{-p} \,,$$

die zu der Matrix

$$M_3 := X_{\mathrm{mod}} Z_{\mathrm{div}}^\dagger M_2 = \sum_{j,k,\ell=0}^{d-1} \omega_d^{j(k+l)} |jd+\ell\rangle \otimes Z_d^{-j} (X_d^k \Delta_{-\ell \bmod d} X_d^{-k})$$

führt. Da $\sum_{j=0}^{d-1} X_d^j D X_d^{-j} = \mathrm{tr}(D) I_d$ für eine diagonale Matrix $D \in \mathbb{C}^{d\times d}$ gilt, kann

$$\begin{aligned}
M_3 &= \sum_{j,k,\ell=0}^{d-1} \omega_d^{j(k+\ell)} |jd+\ell\rangle \otimes Z_d^{-j}(X_d^k \Delta_{-\ell \bmod d} X_d^{-k}) \\
&= \sum_{j,k,\ell=0}^{d-1} \omega_d^{jk}\omega_d^{j\ell} |jd+\ell\rangle \otimes Z_d^{-j} X_d^k \Delta_{-\ell \bmod d} X_d^{-k} \\
&= \sum_{j,k,\ell=0}^{d-1} \omega_d^{j\ell} |jd+\ell\rangle \otimes X_d^k (Z_d^{-j} \Delta_{-\ell \bmod d}) X_d^{-k} \\
&= \sum_{j,\ell=0}^{d-1} \omega_d^{j\ell} |jd+\ell\rangle \otimes \mathrm{tr}(Z_d^{-j}\Delta_{-\ell \bmod d}) I_d \\
&= \sum_{j,\ell=0}^{d-1} \mathrm{tr}(\omega_d^{j\ell} Z_d^{-j}\Delta_{-\ell \bmod d}) |jd+\ell\rangle \otimes I_d = |\Phi_0\rangle \otimes I_d
\end{aligned}$$

geschrieben werden, womit sich der Vektor

$$|\Phi_0\rangle = \sum_{j,\ell=0}^{d-1} \mathrm{tr}(\omega_d^{j\ell} Z_d^{-j}\Delta_{-\ell \bmod d}) |jd+\ell\rangle$$

ergibt. Mit der Fourier-Transformation

$$F_d \otimes I_d = \sqrt{\frac{1}{d}} \sum_{p,q,r=0}^{d-1} \omega_d^{pq} |pd+r\rangle\langle qd+r|$$

wird anschließend der Vektor

$$(F_d \otimes I_d)|\Phi_0\rangle = \sqrt{\frac{1}{d}} \sum_{p,q,r=0}^{d-1} \omega_d^{(p+r)q} \mathrm{tr}(Z_d^{-q}\Delta_{-r \bmod d}) |pd+r\rangle$$

erhalten. Der Koeffizient von $|pd+r\rangle$ kann zu

$$\sqrt{\frac{1}{d}} \sum_{q=0}^{d-1} \omega_d^{(p+r)q} \mathrm{tr}(Z_d^{-q}\Delta_{-r \bmod d}) = \sqrt{\frac{1}{d}}\, \mathrm{tr}\left(\left(\sum_{q=0}^{d-1} \omega_d^{(p+r)q} Z_d^{-q} \right) \Delta_{-r \bmod d} \right)$$

umgeformt werden; es folgt

$$\begin{aligned}
\sum_{q=0}^{d-1} \omega_d^{(p+r)q} Z_d^{-q} &= \sum_{q=0}^{d-1} \omega_d^{(p+r)q} \left(\sum_{j=0}^{d-1} \omega_d^{-jq} |j\rangle\langle j| \right) = \sum_{j=0}^{d-1} \left(\sum_{q=0}^{d-1} \omega_d^{(p+r-j)q} \right) |j\rangle\langle j| \\
&= d\, |(p+r) \bmod d\rangle\langle (p+r) \bmod d|
\end{aligned}$$

und daher gilt

$$(F_d \otimes I_d)|\Phi_0\rangle = \sqrt{d} \sum_{p,r=0}^{d-1} \Delta_{-r \bmod d}^{((p+r) \bmod d)} |pd+r\rangle\,,$$

wobei $D^{(k)}$ der k-te Eintrag in der Diagonalmatrix D ist. Mit $|pd+r\rangle = |p\rangle \otimes |r\rangle$ ist dies die Summe

$$(F_d \otimes I_d)|\Phi_0\rangle = \sqrt{d} \sum_{p,r=0}^{d-1} \langle p|\sqrt{\Pi}|(p+r) \bmod d\rangle |p\rangle \otimes |r\rangle \,, \tag{B.5}$$

da

$$\begin{aligned}
\sqrt{\Pi} &= \sum_{\ell=0}^{d-1} X_d^\ell \Delta_\ell = \sum_{\ell,u=0}^{d-1} |(u+\ell) \bmod d\rangle\langle u|\Delta_\ell \\
&= \sum_{\ell,u,j=0}^{d-1} |(u+\ell) \bmod d\rangle\langle u|\Delta_\ell^{(j)}|j\rangle\langle j| \\
&= \sum_{\ell,u,j=0}^{d-1} \Delta_\ell^{(j)} |(u+\ell) \bmod d\rangle\langle u|j\rangle\langle j| = \sum_{\ell,j=0}^{d-1} \Delta_\ell^{(j)} |(j+\ell) \bmod d\rangle\langle j| \,.
\end{aligned}$$

Demnach ist $\Delta_{-r \bmod d}^{((p+r) \bmod d)}$ der Eintrag von $\sqrt{\Pi}$ zu $|p\rangle\langle(p+r) \bmod d|$. Das bedeutet, daß

$$\langle p|\sqrt{\Pi}|(p+r) \bmod d\rangle = \Delta_{-r \bmod d}^{((p+r) \bmod d)} \,.$$

Die Anwendung der Operation $\sum_{q=0}^{d-1} |q\rangle\langle q| \otimes X_d^q$ auf $(F_d \otimes I_d)|\Phi_0\rangle$ von Gl. (B.5) führt zu

$$\begin{aligned}
|\Phi_0'\rangle &:= \sqrt{d} \left(\sum_{q=0}^{d-1} |q\rangle\langle q| \otimes X_d^q \right) \sum_{p,r=0}^{d-1} \langle p|\sqrt{\Pi}|(p+r) \bmod d\rangle |p\rangle \otimes |r\rangle \\
&= \sqrt{d} \sum_{p,r=0}^{d-1} \langle p|\sqrt{\Pi}|(p+r) \bmod d\rangle |p\rangle \otimes |(p+r) \bmod d\rangle \,.
\end{aligned}$$

Dies zeigt $|\Phi_0'\rangle = \sqrt{d} \sum_{j,k=0}^{d-1} \sqrt{\Pi}_{j,k} |j\rangle \otimes |k\rangle$, wobei $\sqrt{\Pi}_{j,k}$ der Eintrag von $\sqrt{\Pi}$ in der j-ten Zeile und k-ten Spalte ist. Hierbei ist $|\Phi_0'\rangle$ ein normierter Zustandsvektor, denn es gilt

$$\langle \Phi_0'|\Phi_0'\rangle = d \sum_{j,k=0}^{d-1} |\sqrt{\Pi}_{j,k}|^2 = d \operatorname{tr}(\sqrt{\Pi}\sqrt{\Pi}) = d \operatorname{tr}(\Pi) = 1$$

aufgrund $\operatorname{tr}(\Pi) = 1/d$. Bei dieser Umformung wird die Gleichung

$$\begin{aligned}
\operatorname{tr}((a_{j,k})_{j,k}(a_{\ell,m})_{\ell,m}) &= \operatorname{tr}\left(\left(\sum_{\nu=0}^{d-1} a_{j,\nu} a_{\nu,k} \right)_{j,k} \right) \\
&= \sum_{j,\nu=0}^{d-1} a_{j,\nu} a_{\nu,j} = \sum_{j,\nu=0}^{d-1} a_{j,\nu} \overline{a}_{j,\nu} = \sum_{j,\nu=0}^{d-1} |a_{j,\nu}|^2
\end{aligned}$$

für eine hermitesche Matrix mit den Einträgen $a_{j,k}$ genutzt. Insgesamt folgt die Gleichung

$$\left(\sum_{q=0}^{d-1} |q\rangle\langle q| \otimes X_d^q \right) (F_d \otimes I_d)|\Phi_0\rangle = \sqrt{d} \sum_{j,k=0}^{d-1} \sqrt{\Pi}_{j,k} |j\rangle \otimes |k\rangle \,,$$

die unmittelbar zu Gl. (5.15) führt.

Literaturverzeichnis

[Alf71] Alfsen, E. M.: *Compact Convex Sets and Boundary Integrals.* Berlin: Springer, 1971

[AP05] Ahnert, S. E.; Payne, M. C.: General implementation of all possible positive-operator-value measurements of single photon polarization states. *Physical Review A* 71 (2005), pp. 012330

[AP06] Ahnert, S. E.; Payne, M. C.: All possible bipartite positive-operator-value measurements of two-photon polarization states. *Physical Review A* 73 (2006), pp. 022333

[App05] Appleby, D. M.: Symmetric informationally complete-positive operator valued measures and the extended Clifford group. *Journal of Mathematical Physics* 46 (2005), pp. 052107

[ASFL05] Andersen, U. L.; Sabuncu, M.; Filip, R.; Leuchs, G.: *Experimental demonstration of coherent state estimation with minimal disturbance.* 2005. – arXiv.org e-Print archive, quant-ph/0510191

[Aud05] Audretsch, J.: *Verschränkte Systeme.* Weinheim: Wiley, 2005

[Bar98] Barnum, H.: *Quantum Information Theory.* Albuquerque, University of New Mexico, Dissertation, 1998

[Bar00] Barnum, H.: Information-disturbance tradeoff in quantum measurement on the uniform ensemble. Department of Computer Science, University of Bristol. Bristol, 2000 (CSTR-00-013). – Forschungsbericht

[BBC+93] Bennett, C. H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wootters, W. K.: Teleporting an unknown state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters* 70 (1993), pp. 1895–1899

[BBC+95] Barenco, A.; Bennett, C. H.; Cleve, R.; DiVincenzo, D. P.; Margolus, N.; Shor, P. W.; Sleator, T.; Smolin, J. A.; Weinfurter, H.: Elementary gates for quantum computation. *Physical Review A* 52 (1995), pp. 3457–3467

[BBRV02] Bandyopadhyay, S.; Boykin, P. O.; Roychowdhury, V.; Vatan, F.: A new proof for the existence of mutually unbiased bases. *Algorithmica* 34 (2002), pp. 512–528

[BCM91] Braunstein, S. L.; Caves, C. M.; Milburn, G. J.: Interpretation for a positive P representation. *Physical Review A* 43 (1991), pp. 1153–1159

[BCv05] Bacon, D.; Childs, A. M.; van Dam, W.: *Optimal measurements for the dihedral hidden subgroup problem.* 2005. – arXiv.org e-Print archive, quant-ph/0501044

[Bea97] Beals, R.: Quantum computation of Fourier transforms over the symmetric groups. In: *Proceedings of the Symposium on Theory of Computing (STOC).* New York: ACM Press, 1997, pp. 48–53

[Bet84] Beth, T.: *Verfahren der schnellen Fourier-Transformation.* Stuttgart: Teubner, 1984

[BGL95] Busch, P.; Grabowski, M.; Lahti, P. J.: *Operational Quantum Physics.* Berlin: Springer, 1995

[BHS01] Bergou, J. A.; Hillery, M.; Sun, Y.: Optimum discrimination of non-orthogonal quantum states: an optical realization. *Fortschritte der Physik* 49 (2001), pp. 915–925

[BKMH97] Ban, M.; Kurokawa, K.; Momose, R.; Hirota, O.: Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *International Journal of Theoretical Physics* 36 (1997), pp. 1269–1288

[BML97] Brandt, H. E.; Myers, J. M.; Lomonaco, S. J.: Aspects of entangled translucent eavesdropping in quantum cryptography. *Physical Review A* 56 (1997), pp. 4456–4465

[Bos96] Bosch, S.: *Algebra.* Berlin: Springer, 1996

[BR04] Bachor, H.-A.; Ralph, T. C.: *A Guide to Experiments in Quantum Optics.* Weinheim: Wiley, 2004

[Bra99] Brandt, H. E.: Positive operator valued measure in quantum information processing. *American Journal of Physics* 67 (1999), pp. 434–439

[Bru02] Bruss, D.: Characterizing entanglement. *Journal of Mathematical Physics* 43 (2002), pp. 4237–4251

[BYH97] Ban, M.; Yamazaki, K.; Hirota, O.: Accessible information in combined and sequential quantum measurements on a binary-state signal. *Physical Review A* 55 (1997), pp. 22–26

[Cal01] Calsamiglia, J.: *Quantum Information Processing and its Linear Optical Implementation.* Helsinki, University of Helsinki, Dissertation, 2001

[Cal02] Calsamiglia, J.: Generalized measurements by linear elements. *Physical Review A* 65 (2002)

[CB93] Clausen, M.; Baum, U.: *Fast Fourier Transforms*. Mannheim: BI, 1993

[CCBR01] Clarke, R. B. M.; Chefles, A.; Barnett, S. M.; Riis, E.: Experimental demonstration of optimal unambiguous state discrimination. *Physical Review A* 63 (2001), pp. 040305(R)

[CD06] Chiribella, G.; D'Ariano, G. M.: *Extremal covariant measurements*. 2006. – arXiv.org e-Print archive, quant-ph/0603168

[CEMM98] Cleve, R.; Ekert, A.; Macchiavello, C.; Mosca, M.: Quantum algorithms revisited. In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. Band 454. London: The Royal Society, 1998, pp. 339–354

[Che98] Chefles, A.: Unambiguous discrimination between linearly independent quantum states. *Physics Letters A* 239 (1998), pp. 339–347

[Che00] Chefles, A.: Quantum state discrimination. *Contemporary Physics* 41 (2000), pp. 401–424

[CKC+01] Clarke, R. B. M.; Kendon, V. M.; Chefles, A.; Barnett, S. M.; Riis, E.; Sasaki, M.: Experimental realization of optimal detection strategies for overcomplete states. *Physical Review A* 64 (2001), pp. 012303

[CR62] Curtis, C. W.; Reiner, I.: *Representation Theory of Finite Groups and Associative Algebras*. New York: Wiley, 1962

[CT91] Cover, T. M.; Thomas, J. A.: *Elements of Information Theory*. New York: Wiley, 1991

[Cyb01] Cybenko, G.: Reducing quantum computations to elementary unitary operations. *Computing in Science and Engineering* 3 (2001), pp. 27–32

[Dav76] Davies, E. B.: *Quantum Theory of Open Systems*. London: Academic Press, 1976

[Dav78] Davies, E. B.: Information and quantum measurement. *IEEE Transactions on Information Theory* IT-24 (1978), pp. 596–599

[Dec05] Decker, T.: *Symmetric measurements attaining the accessible information*. 2005. – arXiv.org e-Print archive, quant-ph/0509122

[DJB04] Decker, T.; Janzing, D.; Beth, T.: Quantum circuits for single-qubit measurements corresponding to platonic solids. *International Journal of Quantum Information* 2 (2004), pp. 353–377

[DJR05] Decker, T.; Janzing, D.; Rötteler, M.: Implementation of group-covariant positive operator valued measures by orthogonal measurements. *Journal of Mathematical Physics* 46 (2005), pp. 012104

[DLPS02] D'Ariano, G. M.; Lo Presti, P.; Sacchi, M. F.: A quantum measurement of the spin direction. *Physical Letters A* 292 (2002), pp. 233–237

[Dor71] Dornhoff, L.: *Group Representation Theory.* Band A. New York: Dekker, 1971

[EF01] Eldar, Y. C.; Forney, G. D.: On quantum detection and the square-root measurement. *IEEE Transactions on Information Theory* 47 (2001), pp. 858–872

[Egn97] Egner, S.: *Zur algorithmischen Zerlegungstheorie linearer Transformationen mit Symmetrie.* Karlsruhe, Universität Karlsruhe (TH), Dissertation, 1997

[EHK99] Ettinger, M.; Høyer, P.; Knill, E.: *Hidden subgroup states are almost orthogonal.* 1999. – arXiv.org e-Print archive, quant-ph/9901034

[EMGK05] Englert, B.-G.; Ming, T. K.; Guan, G. C.; Khoon, N. H.: Single-loop interferometer for minimal ellipsometry. *Laser Physics* 15 (2005), pp. 7–9

[EMV04] Eldar, Y.; Megretski, A.; Verghese, G. C.: Optimal detection of symmetric mixed quantum states. *IEEE Transactions on Information Theory* 50 (2004), pp. 1198–1207

[FAABS01] Franke-Arnold, S.; Andersson, E.; Barnett, S. M.; Stenholm, S.: Generalized measurements of atomic qubits. *Physical Review A* 63 (2001), pp. 052301

[FH91] Fulton, W.; Harris, J.: *Representation Theory.* New York: Springer, 1991

[FLS89a] Feynman, R. P.; Leighton, R. B.; Sands, M.: *The Feynman Lectures on Physics.* Band 2. Reading: Addison-Wesley, 1989

[FLS89b] Feynman, R. P.; Leighton, R. B.; Sands, M.: *The Feynman Lectures on Physics.* Band 1. Reading: Addison-Wesley, 1989

[FP96] Fuchs, C. A.; Peres, A.: Quantum-state disturbance versus information gain: uncertainty relations for quantum information. *Physical Review A* 53 (1996), pp. 2038–2045

[FS92] Fässler, A.; Stiefel, E.: *Group Theoretical Methods and Their Applications.* Boston: Birkhäuser, 1992

[FSB+98] Furusawa, A.; Sørensen, J. L.; Braunstein, S. L.; Fuchs, C. A.; Kimble, H. J.; Polzik, E. S.: Unconditional quantum teleportation. *Science* 282 (1998), pp. 706–709

[FTMS03] Fujiwara, M.; Takeoka, M.; Mizuno, J.; Sasaki, M.: Exceeding the classical capacity limit in a quantum channel. *Physical Review Letters* 90 (2003), pp. 167906

[GHW04] Gibbons, K. S.; Hoffman, M. J.; Wootters, W. K.: Discrete phase space based on finite fields. *Physical Review A* 70 (2004), pp. 062101

[GJ79] Garey, M. R.; Johnson, D. S.: *Computers and Intractability.* New York: W. H. Freeman and Company, 1979

[GK05] Gerry, C. C.; Knight, P. L.: *Introductory Quantum Optics.* Cambridge: Cambridge University Press, 2005

[GR94] Göpfert, A.; Riedrich, T.: *Funktionalanalysis.* Leipzig: Teubner, 1994

[Gra04] Grassl, M.: On SIC-POVMs and MUBs in dimension 6. In: *Proceedings of ERATO Conference on Quantum Information Science 2004 (EQIS 2004)*, 2004, pp. 60–61. – Siehe auch arXiv.org e-Print archive, quant-ph/0406175

[GRTZ02] Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H.: Quantum cryptography. *Reviews of Modern Physics* 74 (2002), pp. 145–195

[Grü67] Grünbaum, B.: *Convex Polytopes.* New York: Wiley, 1967

[Hei90] Hein, W.: *Struktur- und Darstellungstheorie der klassischen Gruppen.* Berlin: Springer, 1990

[Hel76] Helstrom, C. W.: *Quantum Detection and Estimation Theory.* New York: Academic Press, 1976

[HIKF00] Hofmann, H. F.; Ide, T.; Kobayashi, T.; Furusawa, A.: Fidelity and information in the quantum teleportation of continuous variables. *Physical Review A* 62 (2000), pp. 062304

[HIKF01] Hofmann, H. F.; Ide, T.; Kobayashi, T.; Furusawa, A.: Information losses in continuous-variable quantum teleportation. *Physical Review A* 64 (2001), pp. 040301(R)

[HJS+96] Hausladen, P.; Jozsa, R.; Schumacher, B.; Westmoreland, M.; Wootters, W. K.: Classical information capacity of a quantum channel. *Physical Review A* 54 (1996), pp. 1869–1876

[HMG+96] Huttner, B.; Muller, A.; Gautier, J. D.; Zbinden, H.; Gisin, N.: Unambiguous quantum measurement of nonorthogonal states. *Physical Review A* 54 (1996), pp. 3783–3789

[HMP+97] Huelga, S. F.; Macchiavello, C.; Pellizzari, T.; Ekert, A. K.; Plenio, B.; Cirac, J. I.: On the improvement of frequency standards with quantum entanglement. *Physical Review Letters* 79 (1997)

[Hol73] Holevo, A. S.: Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission* 9 (1973), pp. 177–183

[Hol98] Holevo, A. S.: The capacity of the quantum channel with general states. *IEEE Transactions on Information Theory* 44 (1998), pp. 269–273

[Hun79] Hund, F.: *Grundbegriffe der Physik*. Band 1. Mannheim: BI, 1979

[HW94] Hausladen, P.; Wootters, W. K.: A 'pretty good' measurement for distinguishing quantum states. *Journal of Modern Optics* 41 (1994), pp. 2385–2390

[Isa76] Isaacs, I. M.: *Character Theory of Finite Groups*. New York: Academic Press, 1976

[JB03] Janzing, D.; Beth, D.: Quasi-order of clocks and their synchronism and quantum bounds for copying timing information. *IEEE Transactions on Information Theory* 49 (2003), pp. 230–240

[JD06] Janzing, D.; Decker, T.: Minimally disturbing Heisenberg-Weyl symmetric measurements using hard-core collisions of Schrödinger particles. *Journal of Mathematical Physics* 47 (2006), pp. 082102

[JL01] James, G.; Liebeck, M.: *Representations and Characters of Groups*. Cambridge: Cambridge University Press, 2001

[Koe85] Koecher, M.: *Lineare Algebra und analytische Geometrie*. Berlin: Springer, 1985

[Kro96] Kroschel, K.: *Statistische Nachrichtentheorie*. Berlin: Springer, 1996

[KSV02] Kitaev, A. Y.; Shen, A. H.; Vyalyi, M. N.: *Classical and Quantum Computation*. Providence: American Mathematical Society, 2002

[Lom04] Lomont, C.: *The hidden subgroup problem - review and open problems*. 2004. – arXiv.org e-Print archive, quant-ph/0411037

[Lor96] Lorenz, F.: *Lineare Algebra*. Band 2. Heidelberg: Spektrum Akademischer Verlag, 1996

[LP93] Leonhardt, U.; Paul, H.: Phase measurement and Q function. *Physical Review A* 47 (1993), pp. R2460–2463

[Man82] Mandel, L.: Squeezed states and sub-Poissonian photon statistics. *Physical Review Letters* 49 (1982), pp. 136–138

[MFA+01] Mizuno, J.; Fujiwara, M.; Akiba, M.; Kawanishi, T.; Barnett, S. M.; Sasaki, M.: Optimum detection for extracting maximum information from symmetric qubit sets. *Physical Review A* 65 (2001), pp. 012315

[MRR04] Moore, C.; Rockmore, D.; Russell, A.: Generic quantum Fourier transforms. In: Munro, J. I. (Hrsg.): *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2004)*, 2004, pp. 778–787. – Siehe auch arXiv.org e-Print archive, quant-ph/0304064

[MS83] MacWilliams, F. J.; Sloane, N. J.: *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1983

[MSB04] Mohseni, M.; Steinberg, A. M.; Bergou, J. A.: Optical realization of optimal unambiguous discrimination for pure and mixed quantum states. *Physical Review Letters* 93 (2004), pp. 200403

[Mur90] Murphy, G. J.: *C^*-Algebras and Operator Theory*. San Diego: Academic Press, 1990

[MW95] Mandel, L.; Wolf, E.: *Optical Coherence and Quantum Optics*. Cambridge: Cambridge University Press, 1995

[NC00] Nielsen, M. A.; Chuang, I. L.: *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000

[Per93] Peres, A.: *Quantum Theory: Concepts and Methods*. Dordrecht: Kluwer, 1993

[PS02a] Peres, A.; Scudo, P. F.: Covariant quantum measurements may not be optimal. *Journal of Modern Optics* 49 (2002), pp. 1235–1243

[PS02b] Peres, A.; Scudo, P. F.: Unspeakable quantum information. In: Khrennikov, A. (Hrsg.): *Quantum Theory: Reconsideration of Foundations*. Växjö: Växjö University Press, 2002 (Mathematical Modelling in Physics, Engineering and Cognitive Sciences). – Siehe auch arXiv.org e-Print archive, quant-ph/0201017

[Püs98] Püschel, M.: *Konstruktive Darstellungstheorie und Algorithmengenerierung*. Karlsruhe, Universität Karlsruhe (TH), Dissertation, 1998

[Püs02] Püschel, M.: Decomposing monomial representations of solvable groups. *Journal of Symbolic Computation* 34 (2002), pp. 561–596

[PW91] Peres, A.; Wootters, W. K.: Optimal detection of quantum information. *Physical Review Letters* 66 (1991), pp. 1119–1122

[Ral00a] Ralph, T. C.: Continuous variable quantum cryptography. *Physical Review A* 61 (2000), pp. 010303(R)

[Ral00b] Ralph, T. C.: Security of continuous-variable quantum cryptography. *Physical Review A* 62 (2000), pp. 062306

[RB98] Rötteler, M.; Beth, T.: *Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups*. 1998. – arXiv.org e-Print archive, quant-ph/9812070

[RBKSC04] Renes, J. M.; Blume-Kohout, R.; Scott, A. J.; Caves, C. M.: Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics* 45 (2004), pp. 2171–2180

[ŘEK04] Řeháček, J.; Englert, B.-G.; Kaszlikowski, D.: Minimal qubit tomography. *Physical Review A* 70 (2004), pp. 052321

[Ren04] Renes, J. M.: *Frames, Designs, and Spherical Codes in Quantum Information Theory.* Albuquerque, University of New Mexico, Dissertation, 2004

[Röt01] Rötteler, M.: *Schnelle Signaltransformationen für Quantenrechner.* Karlsruhe, Universität Karlsruhe (TH), Dissertation, 2001

[RRS02] Roa, L.; Retamal, J. C.; Saavedra, C.: Quantum-state discrimination. *Physical Review A* 66 (2002), pp. 012103

[RZBB94] Reck, M.; Zeilinger, A.; Bernstein, H. J.; Bertani, P.: Experimental realization of any discrete unitary operator. *Physical Review Letters* 73 (1994), pp. 58–61

[S+97] Schönert, Martin u. a.: *GAP – Groups, Algorithms, and Programming – version 3 release 4 patchlevel 4.* Aachen: Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, 1997

[SBJ+99] Sasaki, M.; Barnett, S. M.; Jozsa, R.; Osaki, M.; Hirota, O.: Accessible information and optimal strategies for real symmetrical quantum sources. *Physical Review A* 59 (1999), pp. 3325–3335

[Sch01] Schleich, W.: *Quantum Optics in Phase Space.* Berlin: Wiley, 2001

[Ser77] Serre, J.-P.: *Linear Representations of Finite Groups.* New York: Springer, 1977

[Sha48] Shannon, C. E.: A mathematical theory of communication. *Bell System Technical Journal* 27 (1948), pp. 379–423

[Sho01] Shor, P. W.: On the number of elements needed in a POVM attaining the accessible information. In: Hirota, O. (Hrsg.); Tombesi, P. (Hrsg.): *Quantum, Communication, Measurement and Computing.* Band 3. Dortrecht: Kluwer, 2001. – Siehe auch arXiv.org e-Print archive, quant-ph/0009077

[Sho04] Shor, P. W.: The adaptive classical capacity of a quantum channel. *IBM Journal of Research and Development* 48 (2004), pp. 115–138

[SHY+85] Slusher, R. E.; Hollberg, L. W.; Yurke, B.; Mertz, J. C.; Valley, J. F.: Observation of squeezed states generated by four-wave mixing in an optical cavity. *Physical Review Letters* 55 (1985), pp. 2409–2414

[SKIH97] Sasaki, M.; Kato, K.; Izutsu, M.; Hirota, O.: A demonstration of superadditivity in the classical capacity of a quantum channel. *Physics Letters A* 236 (1997), pp. 1–4

[SKIH98] Sasaki, M.; Kato, K.; Izutsu, M.; Hirota, O.: Quantum channels showing superadditivity in capacity. *Physical Review A* 58 (1998), pp. 146–158

[Ste92] Stenholm, S.: Simultaneous measurements of conjugate variables. *Annals of Physics* 218 (1992), pp. 233–254

[Ste94] Sternberg, S.: *Group Theory and Physics.* Cambridge: Cambridge University Press, 1994

[Ter99] Terras, A.: *Fourier Analysis on Finite Groups and Applications.* Cambridge: Cambridge University Press, 1999

[TFMS04] Takeoka, M.; Fujiwara, M.; Mizuno, J.; Sasaki, M.: Implementation of generalized quantum measurements: superadditive quantum coding, accessible information extraction, and classical capacity limit. *Physical Review A* 69 (2004), pp. 052329

[TS04] Tyc, T.; Sanders, B. C.: Operational formulation of homodyne detection. *Journal of Physics A* 37 (2004), pp. 7341–7357

[VMS04] Vartiainen, J. J.; Möttönen, M.; Salomaa, M. M.: Efficient decomposition of quantum gates. *Physical Review Letters* 92 (2004), pp. 177902

[WF89] Wootters, W. K.; Fields, B. D.: Optimal state-determination by mutually unbiased measurements. *Annals of Physics* 191 (1989), pp. 363–381

[WJDB03] Wocjan, P.; Janzing, D.; Decker, T.; Beth, T.: *Measuring 4-local n-qubit observables could probabilistically solve PSPACE.* 2003. – arXiv.org e-Print archive, quant-ph/0308011

[WM95] Walls, D. F.; Milburn, G. J.: *Quantum Optics.* Berlin: Springer, 1995

[Woo05] Wootters, W. K.: *Distinguishing unentangled states with an unentangled measurement.* 2005. – arXiv.org e-Print archive, quant-ph/0506149

[YKL75] Yuen, H. P.; Kennedy, R. S.; Lax, M.: Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Transactions on Information Theory* 21 (1975), pp. 125–134

[Zim72] Ziman, J.: *Principles of the Theory of Solids.* Cambridge: Cambridge University Press, 1972

Eigene Veröffentlichungen

Beiträge in Zeitschriften

- Janzing, D.; Decker, T.; Beth, T.: Performing joint measurements and transformations on several qubits by operating on a single control qubit. *Physical Review A* 67 (2003), pp. 042320

- Decker, T.; Janzing, D.; Beth, T.: Quantum circuits for single-qubit measurements corresponding to platonic solids. *International Journal of Quantum Information* 2 (2004), pp. 353–377

- Decker, T.; Janzing, D.; Rötteler, M.: Implementation of group-covariant positive operator valued measures by orthogonal measurements. *Journal of Mathematical Physics* 46 (2005), pp. 012104

- Decker, T.; Grassl, M.: Implementation of generalized measurements with minimal disturbance on a quantum computer. *Fortschritte der Physik* 54 (2006), pp. 898–916

- Janzing, D.; Decker, T.: Minimally disturbing Heisenberg-Weyl symmetric measurements using hard-core collisions of Schrödinger particles. *Journal of Mathematical Physics* 47 (2006), pp. 082102

Eingereichte Beiträge

- Wocjan, P.; Janzing, D.; Decker, T.; Beth, T.: *Measuring 4-local n-qubit observables could probabilistically solve PSPACE.* 2003. – arXiv.org e-Print archive, quant-ph/0308011

- Decker, T.: *Symmetric measurements attaining the accessible information.* 2005. – arXiv.org e-Print archive, quant-ph/0509122

Studien- und Diplomarbeit

- Decker, T.: *POVM-Messungen zur optimalen Unterscheidung von Quantenzuständen.* Karlsruhe, Universität Karlsruhe (TH), Studienarbeit, 2001

- Decker, T.: *Gruppentheoretischer Entwurf von Meßalgorithmen für kollektive Observable auf Quantenregistern.* Karlsruhe, Universität Karlsruhe (TH), Diplomarbeit, 2002

Stichwortverzeichnis