Einführung in Grundlagen und Protokolle der Quanteninformatik*

Bernd Crell und Armin Uhlmann

Institut für Theoretische Physik
Universität Leipzig

*Zentrum für Höhere Studien, NTZ-Preprint **33** (1998)

Inhaltsverzeichnis

Vorwort

Im Januar 1998 hielten wir vier Seminarvorträge zur Einführung in die Quanten–Informationstheorie ("Quanteninformatik"). Die Frage, wie ein quantenphysikalisches Analogon zur Informationstheorie aussehen könnte und für welche Zwecke ein solches Sinn macht, hat eine längere und sehr verzweigte Geschichte. Viele verschiedene Wissensgebiete trugen bzw. tragen zum Versuch ihrer Beantwortung bei.

Durch die Arbeiten von Brillouin, Jaynes, Ingarden und anderen ergaben sich bedeutende Anwendungen der Shannonschen Informationstheorie in der Physik, namentlich der Thermodynamik und Statistischen Physik. Jedoch sind ihre eigentlichen Grundlagen, wie auch die der Kodierungstheorie, der Theorie der Komplexität, der Programmierung und der Berechenbarkeit, nur marginal physikalischer Natur. Auf einem anderen Blatt steht, daß zur Nutzung ihrer Ergebnisse oft außergewöhnliche physikalische Einsicht und Kunstfertigkeit wie auch bewundernswertes technisches Können erforderlich sind.

Versucht man sich jedoch der Idee der Quanteninformation und ihrer Verarbeitung zu nähern, so findet man sich unvermittelt von subtilen Problemen der Quantenphysik umgeben. Von der experimentellen Realisierung (oder gar technischen Beherrschung) fast aller ihrer Gedankenexperimente ist man freilich noch weit, sehr weit, entfernt. Vielleicht aber ist, was heute als logisch konsistente Phantasie erscheint, der bescheidene Startpunkt einer Hochtechnologie des kommenden Jahrhunderts.

Die ersten Anfänge einer quantenmechanischen Informationstheorie reichen bis in die 50er Jahre zurück. Aber erst in den 60er und 70er Jahren wurden unter dem Einfluß der sich entwickelnden Quanten– und Mikroelektronik die Besonderheiten der Quanten–Informationstheorie deutlicher. Von den Pionieren dieser Entwicklung seien stellvertretend Gabor, Gordon, Liu, Helstrom, Levitin, Holevo, Ingarden, Davies und Ohya genannt. In den 80er Jahren kamen mit den Arbeiten über Computer, die nach quantenmechanischen Prinzipien arbeiten, neue Akzente hinzu (Benioff, Feynman, Deutsch und Peres). Über diese nur angedeutete und sicher unvollständige Historie kann man sich in folgenden Arbeiten einen kleinen Überblick verschaffen: [35, 39, 53, 45, 47, 49, 24, 61, 6, 32, 33, 25, 64].

Aus diesem Problemkreis (und insbesondere aus der Entwicklung der letzten Jahre) haben wir — auch aus Kompetenzgründen — nur eine bescheidene Auswahl treffen können. Für kritische Anmerkungen sind wir dankbar.

Bemerkung zur Notation:

Wir werden Hilberträume stets mit $\mathcal{H}$ (und eventuell mit weiteren Indizes) bezeichnen. Oft bezeichnet $\mathcal{H}$ speziell den zweidimensionalen Hilbertraum (q-Bit–Hilbertraum).

Die Hilbertraumvektoren werden (nach Schrödinger) mit ϕ, ψ, ... bezeichnet. Wir benutzen aber, besonders für die q-Bit–Basisvektoren und ihre Tensorprodukte, auch die Dirac–Schreibweise. Wir schreiben dann wie üblich etwa $|x\rangle$ oder $|\uparrow\rangle$. Dadurch gibt es, auch um Mißverständnisse zu vermeiden, kleine Unterschiede für die Schreibweise der Skalarprodukte: $\langle\, \phi, \psi \,\rangle$ bzw. $\langle\, x|y \,\rangle$.

Auch für die eindimensionalen Projektoren ist die Dirac'sche Notation recht zweckmäßig; z.B. ist $|\phi\rangle\langle\phi|$, $\langle\phi, \phi\rangle = 1$, der Projektor auf den von ϕ erzeugten Unterraum.

Meist verwenden wir für Operatoren Großbuchstaben. Wichtige Ausnahmen sind Dichteoperatoren, die wir ϱ, ω, ... nennen. So kann z. B. der Projektor $|\phi\rangle\langle\phi|$, $\langle\phi, \phi\rangle = 1$, sowohl ein Spektralprojektor P als auch ein Dichteoperator π eines reinen Zustandes sein. Mit Tr bezeichnen wir die Spurbildung.

Um die Terminologie nicht zu schwerfällig zu machen, identifizieren wir Zustände mit ihren Dichteoperatoren. Wir führen also, wenn ϱ einen Dichteoperator bezeichnet, für das lineare, positive und normierte Funktional $A \to \mathrm{Tr}\ \varrho A$ kein eigenes Symbol ein. (Im Endlichdimensionalen und für normale Zustände von Typ-I-Faktoren bedeutet dies keine Beschränkung der Allgemeinheit.)

1 bezeichnet immer den Eins–Operator im entsprechenden Hilbertraum.

1 Die Idee des Quantenrechners

1.1 Quantenbotschaften

Die Informationstheorie bewertet die Antwort auf eine Ja–Nein–Frage mit einem Bit. Um ein unbekanntes Element einer Menge aus N Elementen herauszufinden, benötigt man im Mittel $\log_2 N$ Bits (— oder mehr, wenn man es ungeschickt anstellt). Eine unbekannte Botschaft der Länge L, die aus einem Alphabet mit N Buchstaben (oder Zeichen) gebildet wurde, erfordert daher $L \cdot \log_2 N$ Bits, denn wir können sie als ein unbekanntes Element einer Menge aus N^L verschiedenen Botschaften ansehen. Eine so einfache Abschätzung gilt aber nur unter zwei Annahmen:

- es darf keine Korrelation zwischen den Buchstaben der Botschaft geben;

- in der Botschaft muß jeder Buchstabe des Alphabets im Mittel gleich häufig anzutreffen sein.

Die zweite Annahme läßt sich leicht lockern: Kommt der i-te Buchstabe mit der mittlerer Häufigkeit p_i vor, so wird eine Zufallvariable eingeführt, deren Werte die Buchstaben des Alphabets sind und die dem i-ten Buchstaben die Wahrscheinlichkeit p_i zuordnet. Wir nennen diese Zufallsvariable λ. Die Information I, die zur Identifizierung der Botschaft in der Menge aller Botschaften der Länge L erforderlich ist, wird durch das L-fache der *Entropie H_λ von λ* von unten abgeschätzt:

$$I \geq L \cdot H_\lambda$$

mit

$$H_\lambda := -\sum p_i \log_2 p_i. \qquad (*)$$

(Der Logarithmus wird — anders als bei der Boltzmann–Gibbs'schen Entropie — zur Basis 2 genommen, und die Boltzmannsche Konstante wird weggelassen. Die so definierte dimensionslose Entropie wird in Bit/Buchstabe angegeben.)

Angenommen, besagte Botschaft soll mit Hilfe eines anderen Alphabets umgeschrieben werden. Die Zufallsvariable λ' definiere die Wahrscheinlichkeiten $p'_1, p'_2, \ldots$ für seine Buchstaben. Dann gilt für die erwartete Länge L' der neuen Botschaft die Ungleichung

$$L \cdot H_\lambda \leq L' \cdot H_{\lambda'} \quad \text{mit} \quad H_{\lambda'} = -\sum p'_i \log_2 p'_i.$$

Man weiß, daß es Übersetzungen gibt, für die die Differenz

$$\frac{L'}{L} - \frac{\sum p_i \log_2 p_i}{\sum p'_i \log_2 p'_i}$$

für "typische" Botschaften größer werdender Länge gegen Null geht.

Unter Bit–Folgen verstehen wird Botschaften, die mit einem Alphabet geschrieben sind, das nur aus zwei Buchstaben besteht, etwa den Zahlen 0 und 1. Für die Länge

einer Bitfolge, die eine optimale Übersetzung unserer eingangs betrachteten Botschaft ist, darf man die Zahl $L \cdot H_\lambda$ erwarten. Die Zeichen 0 und 1 müssen dann mit gleicher Wahrscheinlichkeit auftreten, d.h. jeweils mit der Wahrscheinlichkeit 1/2.

Nach dieser skizzenhaften Erinnerung an ein paar Begriffe der Shannonschen Informationstheorie wenden wir uns den *Quantenalphabeten* zu. Hierzu ist die Vorstellung sinnvoll, ein klassisches Alphabet mit N Buchstaben sei durch ein physikalisches System realisiert, das genau N verschiedener Zustände fähig ist. Denken wir etwa an ein "Schalter", der in genau N Stellungen einrasten kann. Ist ein solcher "Schalter" quantenphysikalischer Natur, so erzwingt das Überlagerungsprinzip, daß die Gesamtheit der (reinen) Zustände durch die Vektoren eines komplexen Hilbertraumes der Dimension N beschrieben werden muß.

Sei also $\mathcal{H}$ ein Hilbertraum der Dimension N über den komplexen Zahlen. Zwei Vektoren charaktersieren genau dann den gleichen Zustand, wenn sie linear abhängig sind. Der Null entspricht kein Zustand. Ein (reiner) Zustand entspricht daher einem eindimensionalen Unterraum oder dem Projektionsoperator auf diesen Unterraum.

Jetzt können wir bereits einige *Quantenbotschaften* untersuchen. Nehmen wir hierzu an, eine solche sei in einem *Quantenalphabet* abgefaßt, das aus endlich vielen reinen Zuständen $\pi_1, \pi_2, \dots$,

$$\pi_j = |\varphi_j\rangle\langle\varphi_j|, \quad \langle\varphi_j, \varphi_j\rangle = 1, \quad \varphi_j \in \mathcal{H}$$

besteht. Die Quantenbotschaft, der "Quantentext ",

$$\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \dots$$

sei eine aus diesem Quantenalphabet gebildete Folge, in der der *Quantenbuchstabe* π_j mit der Wahrscheinlichkeit $p_j > 0$ auftritt.

Die Quantenphysik verbietet die Herstellung solcher Botschaften nicht[1]. Man kann ja zunächst den "Quantentext"$\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \dots$ als eine klassische Botschaft mit der Entropie $(*)$ ansehen, deren Buchstaben nur etwas unüblich geschrieben sind. Die Aufgabe des Herstellers besteht darin, nach Maßgabe dieser klassischen Botschaft durch die Erzeugung der ihnen entsprechenden Zustände in $\mathcal{H}$ die Quantenbotschaft nacheinander zu gewinnen und eventuell abzusenden. Da als bekannt angenommen wird, welcher Quantenbuchstabe dem Symbol "π_j"entsprechen soll, benötigt man genau die Information, die in der klassischen Botschaft enthalten ist, also die Entropie

$$H^{\text{in}}(\text{Quantenbotschaft}) = -L \cdot \sum p_i \log_2 p_i.$$

Mit Ausnahme des trivialen 1-dimensionalen Hilbertraums kann man daher *in jedem Hilbertraum ein Quantenalphabet beliebiger Länge einrichten.*

In der Literatur werden Herstellung und Absenden einer (Quanten)botschaft oft einer Person namens *Alice* anvertraut. Der Empfänger, der sie lesen oder weiterverarbeiten soll, wird *Bob* genannt. Die Personifizierung vereinfacht die Sprechweise, darf aber nicht zu wörtlich genommen werden.

[1] Ihre experimentelle Realisierung ist gegenwärtig aber nur in sehr engem Rahmen möglich.

Nehmen wir nun an, Bob erhalte eine Quantenbotschaft und diese sei gerade $\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \ldots$. Im Allgemeinen kann Bob, der die Quantenbotschaft zu lesen versucht, diese nicht vollständig interpretieren: Was er auch tut, er kann ihr nicht die Information entnehmen, die er brauchte, um seinerseits die gleiche Quantenbotschaft herzustellen. Zur Illustration diskutieren wir im Folgenden, was bei einer vollständigen v.Neumann'schen Messung [86] geschieht. Generell aber gilt:

Jeder Versuch, eine hinreichend allgemeine Quantenbotschaft - einen "Quantentext"- in klassische Information zu verwandeln, ist mit einem irreversiblen Verlust an Information verbunden.

Alice ihrerseits kann über einen "klassischen" Kanal zusätzliche Information an Bob liefern, die den Verlust kompensiert. Vermutlich wird sie dabei versuchen, mit möglichst wenig Bits auszukommen.

Wir untersuchen, wieviele Bit klassischer Information aus der Quantenbotschaft $\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \ldots$ mit Hilfe einer vollständigen Messung[2] à la von Neumann gewonnen werden können. Hierzu benötigen wir den Operator

$$D := \sum p_i \pi_i,$$

aus dem die Größe

$$H^{\text{out}}(\text{Quantenbotschaft}) := L \cdot \text{Tr}(-D \log_2 D)$$

gewonnen wird. Als erstes kann man zeigen, daß

$$H^{\text{out}}(\text{Quantenbotschaft}) \leq H^{\text{in}}(\text{Quantenbotschaft})$$

und *Gleichheit dann und nur dann eintritt, wenn das Quantenalphabet orthogonal ist*, also $\pi_i \pi_k = 0$ für $i \neq k$ ([82]).

Nach dieser Vorbereitung lassen wir Bob eine vollständige orthonormale Basis $\psi_1, \psi_2, \ldots$ von $\mathcal{H}$ auswählen. Seien $P_k = |\psi_k\rangle\langle\psi_k|$ die mit ihr gebildeten Projektionsoperatoren.[3] Bob wählt eine Observable

$$A = \sum \lambda_k P_k$$

mit lauter verschiedenen Eigenwerten. Eine Apparatur, die A zu messen gestattet, zeigt die Werte $\lambda_1, \lambda_2, \ldots$ an. Diese Werte bilden ein "klassisches" Alphabet und unser Meßapparat transformiert (oder dekodiert) die Quantenbotschaft in eine Botschaft:

$$\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \ldots \Longrightarrow \lambda_{i_1}, \lambda_{i_2}, \lambda_{i_3}, \ldots.$$

[2] Etwas genauer wird der Meßprozeß im zweiten Kapitel behandelt.

[3] Sowohl die π_j also auch die P_k sind minimale Projektoren. Die Verschiedenheit der Bezeichnung soll auf ihre unterschiedliche Rolle hinweisen, die sie entweder als Zustände oder als Observable spielen.

Wie groß ist die Entropie der neuen Botschaft ?

Die Wahrscheinlichkeit p_{jk} für die Anzeige des Wertes λ_k im Zustand π_j gibt die Quantentheorie mit

$$p_{jk} = \mathrm{Tr}\, \pi_j P_k = |\langle \varphi_j, \psi_k \rangle|^2$$

an. Die Wahrscheinlichkeit p'_k, den Meßwert λ_k zu erhalten, beträgt demnach

$$p'_k = \sum_j p_j \mathrm{Tr}\, \pi_j P_k = \mathrm{Tr}\, P_k D.$$

Die erwartete Entropie der neuen Botschaft ist somit

$$L \cdot H_\lambda = -L \cdot \sum p'_j \log_2 p'_j = -L \cdot \sum \langle \psi_j, D\psi_j \rangle \ln_2 \langle \psi_j, D\psi_j \rangle.$$

Um eine möglichst gute Dekodierung zu erhalten, muß die mittlere Information pro Buchstabe maximiert werden.

Aus der strengen Konkavität von $-x \ln x$ folgt:

H_λ erreicht seinen maximalen Wert genau dann, wenn $\psi_1, \psi_2, \ldots$ Eigenvektoren von D sind. Damit ist die bestmögliche Übersetzung einer Quantenbotschaft der oben beschriebenen Art in ein Botschaft mit Hilfe einer vollständigen von Neumann'schen Messung gefunden.

Obiges Beispiel stützt folgende Regeln:

a) Der Informationsgehalt einer Quantenbotschaft bleibt ungeändert, wenn man sie unitären (oder antiunitären) Transformationen unterwirft. Die Werte von H^{out}(Quantenbotschaft) und H^{in}(Quantenbotschaft) bleiben erhalten.

b) Nur Quantenbotschaften mit orthogonalem Quantenalphabet können ohne Verlust in klassische Botschaften transformiert werden. Hierzu muß aber eine adäquate Orthonormalbasis bekannt sein. Daher benötigt man oft einen *Hilbertraum mit ausgezeichneter Basis*. Sie wird *Referenz*basis oder *Berechnungs*basis (engl. compuational basis) genannt.

c) Generisch führt jede Operation, die eine klassische Botschaft über die Lage eines Vektors im Hilbertraum (oder eines Zustandes im Zustandsraum) abzulesen gestattet, zu zufälligen Veränderungen der Quantenbotschaft.

1.2 q-Bits und Multi-q–Bits

Ein *q-Bit*[4] π, englisch: qubit [72], ist ein reiner Zustand eines 2-dimensionalen Hilbertraumes $\mathcal{H}$. Jedes quantenphysikalische 2-Niveau-System wird durch einen sol-

[4] In Anlehnung an Dirac's q-Zahlen [28].

chen Hilbertraum beschrieben. Für die Zwecke des Transports und der Verarbeitung (Transformation) von Quanteninformation ist jedoch seine konkrete physikalische Realisierung nicht von primärem Interesse. Man spricht daher auch vom *q-Bit–Hilbertraum*.

Die q-Bits korrespondieren also vermöge

$$\pi = |\varphi\rangle\langle\varphi| \tag{1}$$

modulo Phasenfaktoren zu den Einheitsvektoren des 2-dimensionalen Hilbertraumes:

$$\varphi \in \mathcal{H}, \quad \dim \mathcal{H} = 2, \quad \langle\varphi, \varphi\rangle = 1. \tag{2}$$

Wir nehmen an, daß in $\mathcal{H}$ eine normierte, orthogonale Basis $|0\rangle$, $|1\rangle$ als Referenzbasis ausgezeichnet ist. Wir nennen sie *q-Bit–Basis* und benutzen für sie gleichberechtigt die Matrix–, die Spin– und die logische Notation:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\uparrow\rangle = |0\rangle$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\downarrow\rangle = |1\rangle.$$

Die Referenzbasis legt die Pauli–Matrizen σ_j, $j = 1, 2, 3$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

wie üblich fest. Ist $x = 0, 1$ und rechnen wir modulo 2, so gilt

$$\sigma_3|x\rangle = (-1)^x|x\rangle, \quad \sigma_1|x\rangle = |x+1\rangle \tag{3}$$

$$\sigma_2|0\rangle = i|1\rangle, \quad \sigma_2|1\rangle = -i|0\rangle.$$

Neben den q-Bits, die durch reine Zustände repräsentiert sind, müssen wir auch die *gemischten* q-Bits betrachten. In der Quanteninformatik werden sie *verrauschte* q-Bits (noisy qubits) genannt. Eine Quantenbotschaft $\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \ldots$ kann aus verrauschten q-Bits (oder allgemeiner aus gemischten Zuständen eines Hilbertraumes) bestehen.

In der Klassischen Physik sind Mischungen als Wahrscheinlichkeitsverteilungen über dem Zustandsraum (also dem Phasenraum) definiert. Sie sind nicht selbst Zustände. Aber in der Quantenphysik gehören die gemischten Zustände zum Zustandsraum. Hier ist der Unterschied zwischen "rein" und "gemischt" kein absoluter. Er hängt von den Observablen ab, die man zur Beschreibung des Quantensystems zuläßt: Schließt man Observable aus, so kann ein reiner Zustand gemischt werden. Fügt man Observable hinzu, betrachtet also das fragliche System als ein Teilsystem eines größeren, so kann ein gemischter Zustand im letzteren ein reiner Zustand sein.

Zustände über endlich–dimensionalen Hilberträumen identifiziert man oft mit Dichteoperatoren. Die Dichteoperatoren über einem q-Bit–Hilbertraum sind von besonders einfacher Form, denn die Positivitätsbedingung ist leicht zu überprüfen. Bezüglich unserer Referenzbasis haben sie die Gestalt

$$\begin{pmatrix} s & \bar{z} \\ z & 1-s \end{pmatrix}, \quad 0 \leq s \leq 1, \quad s(1-s) \geq z\bar{z}.$$

Der Dichteoperator $\frac{1}{2}\mathbf{1}$ charakerisiert den Spurzustand.. Mit Ausnahme des Spurzustandes kann man einem verrauschten q-Bit ein q-Bit zuordnen. Das erreicht man durch Angabe der Zerlegung

$$\begin{pmatrix} s & \bar{z} \\ z & 1-s \end{pmatrix} = p\,\pi + (1-p)\frac{1}{2}\mathbf{1}, \quad p > 0,$$

wobei π einen reinen Zustand (1) bezeichnet. Diese Zerlegung existiert und ist eindeutig.

Zum Beweis transformiert man den Dichteoperator unitär auf Diagonalform. Dann entsteht aus obiger Gleichung

$$\begin{pmatrix} t & 0 \\ 0 & 1-t \end{pmatrix} = p \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + (1-p) \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}, \quad p = 2t-1,$$

wobei die Transformation so geführt wurde, daß $t > 1-t$ ist. Dies geht genau dann, wenn es sich nicht um den Spurzustand handelt.

Je kleiner p ist, umso schwieriger ist es, das q-Bit π zu identifizieren. Eine v.Neumannsche Messung, die π und das zu π orthogonale q-Bit π' unterscheidet, zeigt π mit der Wahscheinlichkeit $(1+p)/2$. Die Wahrscheinlichkeit, daß das verrauschte q-Bit mit π' identifiziert wird, ist folglich $(1-p)/2$. Der Spurzustand, bei dem $p = 0$ ist, enthält keinerlei Information. Er ist "logisch leer".

Eine weitere, oft benutzte Beschreibung unseres verrauschten Bits ist

$$\begin{pmatrix} s & \bar{z} \\ z & 1-s \end{pmatrix} = \frac{1}{2}(\mathbf{1} + x_1\sigma_1 + x_2\sigma_2 + x_3\sigma_3), \quad 2s = 1 + x_3, \quad z = x_1 + ix_2.$$

Wir erhalten genau dann einen Dichteoperator, wenn für den reellen Vektor (x_1, x_2, x_3) die Bedingung $x_1^2 + x_2^2 + x_3^2 \leq 1$ erfüllt ist. Die Oberfläche dieser Kugel heißt *Blochsphäre*. Die Bloch–Sphäre, $x_1^2 + x_2^2 + x_3^2 = 1$, parametrisiert die reinen q-Bits.

Die zur Referenzbasis $|0\rangle, |1\rangle$ gehörenden Projektoren bilden den Nord– bzw. Südpol der Bloch–Sphäre. Die Referenzbasis zeichnet somit eine Achse im q-Bit–Zustandsraum aus.

Damit beenden wir den kurzen Exkurs über verrauschte q-Bits.

Aus Bits werden Wörter zusammengesetzt, z.B. Bytes. Diese bilden selbst ein Alphabet, das jedoch über eine zusätzliche Struktur verfügt: seine lexikographische Ordnung. Analog werden aus q-Bits *Multi–q-Bits*.

Die (reinen oder unverrauschten) Multi–q-Bits der Länge n sind, bis auf Phasenfaktoren, die Einheitsvektoren des n-fachen Tensorprodukts des q-Bit–Hilbertraumes,

$$\mathcal{H}^{\otimes n} = \mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}, \quad \dim \mathcal{H}^{\otimes n} = 2^n. \tag{4}$$

Auch hier werden wir annehmen, daß in jedem der Faktoren eine orthonormierte q-Bit–Basis $|0\rangle, |1\rangle$ ausgezeichnet ist. Damit ist auch eine orthonormierte Wort– oder Produkt–Basis in $\mathcal{H}^{\otimes n}$ gegeben, die aus den Vektoren

$$|x_1 x_2 \dots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle, \quad x_i = 0, 1 \tag{5}$$

besteht. Diese *Produktvektoren* bilden im Folgenden die Referenzbasis ("computational basis") der Multi–q-bits.

Beispielsweise ist die Referenzbasis der 2-q-Bits:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |\uparrow\uparrow\rangle, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |\uparrow\downarrow\rangle,$$

$$|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |\downarrow\uparrow\rangle, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |\downarrow\downarrow\rangle.$$

Der Multi–q-Bit–Raum ist somit ein Hilbertraum mit folgender zusätzlicher Struktur:

Er besitzt eine ausgezeichnete Faktorzerlegung (4).

Er besitzt eine ausgezeichnete Basis (5), die mit der Zerlegung (4) verträglich ist.

Bemerkungen:

Die Wahl der Basisvektoren für die einzelnen Faktoren in (4) bedarf einer Konvention, ist aber ansonsten willkürlich möglich. Hierzu werden nichtentartete Observable in den einzelnen q-Bit–Räumen ausgezeichnet, aus deren Eigenvektoren die Referenzbasis (5) des Multi–q-Bit–Raumes zusammengesetzt wird. Die Eigenvektoren werden so bis auf Phasenfaktoren bestimmt. Eine oft verwendete Konvention besteht darin, Observable auszuwählen, die den Einfluß eines äußeren Feldes beschreiben, das als Referenz zur Verfügung steht. Es ist ein keineswegs triviales Problem, die Wahl der Referenzbasis stabil und zeitlich kontrolliert zu halten. Die Synchronisation ist besonders delikat, wenn die physikalische Realisierung des Multi–q-Bit–Raumes makroskopische räumliche Ausdehnung besitzt.
Wir schließen noch eine allgemeine Bemerkung zum Tensorprodukt an. Haben wir ein aus mehreren (sagen wir: n) Teilsystemen zusammengesetztes Quantensytem vorliegen, dann ist der Gesamt-Hilbertraum das Tensorprodukt der Hilberträume der Teilsysteme:

$$\mathcal{H}_{ges} = \mathcal{H}_1 \otimes \dots \mathcal{H}_n.$$

Werden Operationen (Messungen und Präparationen, unitäre Transformationen) nur an Teilsystemen durchgeführt, so sprechen wir von *lokalen Operationen*. Damit ist nicht automatisch ein räumlicher Aspekt verbunden, obwohl er in manchen Anwendungen, wenn die Einwirkung auf die Teilsysteme mit Experimenten verbunden ist, die untereinander räumlich mehr oder weniger weit getrennt sind, natürlich von besonderer Bedeutung ist (und Anlaß leidenschaftlicher Debatten war und ist). Wir kommen im Zusammenhang mit dem EPR-Kanal darauf zurück. Ein zu einer lokalen Operation im Hilbertraum $\mathcal{H}_i$ korrespondierender Operator ist im Gesamt-Hilbertraum $\mathcal{H}_{ges}$ gegeben durch

$$\mathbf{1} \otimes \ldots \mathbf{1} \otimes A \otimes \mathbf{1} \ldots \mathbf{1},$$

wobei A an der i-ten Stelle steht und der entsprechende Operator aus $\mathcal{H}_i$ ist, der die gewünschte Operation induziert. □

1.3 Logische q-Bit Operationen

Ein klassischer Rechner verarbeitet Bit–Folgen

$$xyz \ldots, \quad \text{z.B. } 011000101 \tag{6}$$

endlicher Länge durch Anwendung elementarer logischer Operationen (oder logischer Befehle, die Kombinationen elementarer Operationen sind):

$$xyz \ldots \longrightarrow x'y'z' \ldots. \tag{7}$$

Dabei werden 1-Bit, 2-Bit, 3-Bit,..., –Operationen ausgeführt.

Man sagt dann, daß bei einer (einfachen oder zusammengesetzten) Operation die Bit–Folge durch ein *Gate* läuft, das die Tranformation der Folge vornimmt. Ein klassische Rechner kann als ein Netzwerk solcher n-Bit–Operationen oder Gates aufgefaßt werden.

Ein *Quantenrechner* verarbeitet Multi–q-Bits durch Ausführung von 1-q-Bit–, 2-q-Bit–, 3-q-Bit–, ... Operationen. Analog zum klassischen Rechner sprechen wir von Quanten–Gates, die die Transformationen der Multi–q-Bits vornehmen. Ein Quantenrechner ist daher ein Netzwerk von Quanten–Gates.[5]

Quanten–Gates repräsentieren unitäre Transformationen in einem Multi–q-Bit Raum.[6]

[5] Quanten–Gate–Netzwerke gehen auf Deutsch [26] zurück und sind im wesentlichen auch dem Quanten-Analogon der Turing-Maschine äquivalent.

[6] Durch die Arbeiten von Lecerf, Petri und Bennett (siehe z.B. die historischen Übersichten in [7] und Kap.9.5 in [42])ist bekannt, daß jeder klassische Rechenprozeß auf reversible Weise (und sogar ohne größeren Mehraufwand an Rechenzeit und Speicher) ausgeführt werden kann.

Die Quantentheorie erlaubt die Anwendung beliebiger unitärer Operatoren.

Diese wichtige Feststellung ist eine Kompatibilitätsaussage: Mit ihr kommen wir nicht zu Widersprüchen mit den Grundlagen der Quantentheorie. Denn die Quantentheorie erlaubt die Annahme, daß die Einbettung eines Quantensystems als Untersystem in ein (sehr viel) größeres grundsätzlich so erfolgen kann, daß die zeitliche Evolution eine definierte Folge unitärer Transformationen im Untersystem bewirkt.

Betrachten wir einige Beispiele.

Logische Verneinung NOT

Das klassische NOT verwandelt 0 in 1 und 1 in 0,

$$x \longrightarrow x' = \mathrm{NOT}(x) = x + 1 \mod 2. \tag{8}$$

Das NOT als Quanten–Gate bezieht sich auf die Referenzbasis $|0\rangle$, $|1\rangle$ und kann als unitäre Operation mit der Pauli-Matrix σ_1 ausgeführt werden:

$$\sigma_1|0\rangle = |1\rangle, \quad \sigma_1|1\rangle = |0\rangle.$$

Die Wirkung von NOT ist aber nur dann so einfach wie im klassischen Fall, wenn es auf ein Element der Referenzbasis wirkt. Ansonsten haben wir

$$\mathrm{Not}(a_0|0\rangle + a_1|1\rangle) = (a_0|1\rangle + a_1|0\rangle).$$

Insbesondere führt der Fall $a_0 = \pm a_1$ auf zwei reine Zustände, die durch die Anwendung von NOT nicht geändert werden. Offensichtlich wirkt NOT nur auf die Elemente der Referenzbasis als logische Verneinung.

In der Sprache der Gates ist NOT eine Operation NOT_k, die auf das k-te q-Bit in $\mathcal{H}^{\otimes n}$ wirkt und durch die unitäre Transformation

$$\mathbf{1} \otimes \ldots \mathbf{1} \otimes \sigma_1 \otimes \mathbf{1} \cdots \otimes \mathbf{1}$$

gegeben ist, wobei σ_1 an der k-ten Stelle steht.

Lassen wir beispielsweise die logische Verneinung auf das erste q-Bit eines 2-q-Bit Vektors wirken. Wir erhalten dann

$$\mathrm{NOT}_1\,(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) = (c|00\rangle + d|01\rangle + a|10\rangle + b|11\rangle)$$

oder, äquivalent,

$$\mathrm{NOT}_1 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} c \\ d \\ a \\ b \end{pmatrix}.$$

Dementsprechend führt NOT_1 n voneinander unabhängige Transpositionen der Koeffizienten eines allgemeinen n-q-Bit Vektors aus, obwohl nur auf eines der q-Bits eingewirkt wurde. Das ist eine wichtige Beobachtung, die auch für andere Quantenoperationen sinngemäß gilt.

Beobachtungen solcher Art haben die Idee aufkommen lassen, daß Quantenrechner klassischen Rechnern möglicherweise überlegen sind, wenn man Resultate dieser eigenartigen "Parallelverarbeitung" durch geeignete Wahl der Observablen aus dem Endzustand ablesen könnte, siehe z.B. [32, 77].

Mit den Worten von R. Jozsa [51] ausgedrückt:
"The physical act of doing nothing on part of an entangled composite system is a highly nontrivial operation. It leads to an exponential information processing benefit if used in conjunction with performing an operation on another (small) part of the system."
Einige Quanten–Algorithmen, die diese Erwartung (theoretisch) erfüllen, werden noch beschrieben werden. Offenbar sind aber nur für gewisse Problemklassen Quanten–Algorithmen effektiver als klassische (siehe [63, 31]).

Phasenschieber

Diese auf ein q-Bit wirkenden Operationen multipizieren die Vektoren der Referenzbasis mit einem Phasenfaktor. Sie lassen also die diesen Vektoren entsprechenden Zustände invariant. Phasenschieber sind Drehungen um die durch $|0\rangle$ und $|1\rangle$ festgelegte Achse des q-Bit–Zustandsraumes (also der Bloch–Sphäre) und können $\exp i\vartheta\,\sigma_3$ geschrieben werden. Auf dem Gebiet des Quantenrechnens ist aber eine andere Normierung üblich, nämlich

$$\begin{pmatrix} 1 & 0 \\ 0 & \epsilon \end{pmatrix}, \quad |\epsilon| = 1$$

Dadurch bleibt $|0\rangle$, das Analogon zum klassisch nicht gesetzten Bit, ungeändert; ein Umstand, der der Denkweise klassischen Programmierens offensichtlich entgegenkommt. Auch das NOT wurde ja der U(2), nicht aber der SU(2) entnommen[7].

σ_3, die Verschiebung der Phase um π, und σ_1, das logische NOT, sind unitär äquivalent. Wir sehen, daß ohne Auszeichung einer Referenzbasis den unitären Operationen keine (quanten)logische Bedeutung zugeschrieben werden kann.

Hadamard – (Walsh) – Transformation H

Sie ist definiert durch

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{9}$$

$$\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{\sigma_1 + \sigma_3}{\sqrt{2}}.$$

[7] Es wäre aber ohne Einschränkung der Allgemeinheit möglich, die Standards der logischen Grundoperationen als spezielle unitäre Transformationen zu definieren.

Eine kompaktere Schreibweise ist:

$$\mathrm{H}|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle), \quad x = 0, 1.$$

Die Hadamard–Transformation ist involutiv: $\mathrm{H}^2 = \mathbf{1}$.

Interessant ist auch die n-fache Hadamard Transformation

$$\begin{aligned} \mathrm{H}^{\otimes n}|x_1 x_2 \ldots x_n\rangle &= \mathrm{H} \otimes \mathrm{H} \otimes \cdots \otimes \mathrm{H}|x_1 x_2 \ldots x_n\rangle \\ &= 2^{-n/2} \sum (-1)^{x_1 y_1 + x_2 y_2 + \cdots} |y_1 y_2 \ldots y_n\rangle \end{aligned} \tag{10}$$

wobei sich die Summation über alle n-Bit-Strings erstreckt.
Eleganter ausgedrückt: $x = \{x_1, \ldots, x_n\}$ sei ein Wort aus n Bits, und wir schreiben für das entsprechende n-fache q-Bit $|x\rangle$. B_n sei die Menge aller Worte aus n Bits. Verwenden wir nun für die bitweise Addition und Multiplikation zweier Worte x und y die Regeln der Boolschen Algebra, dann erhalten wir

$$\mathrm{H}^{\otimes n}|x\rangle = 2^{-n/2} \sum_{y \in B_n} (-1)^{xy} |y\rangle.$$

Speziell sieht man, daß $\mathrm{H}^{\otimes n}$ angewandt auf $|0, 0, ...0\rangle$ eine Superposition aller Basisvektoren mit gleichen Koeffizienten ergibt

$$\mathrm{H}^{\otimes n}|0, 0, ...0\rangle = 2^{-n/2} \sum_{y \in B_n} |y\rangle.$$

Bemerkung:
Die Matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ ist die (im wesentlichen eindeutige) reelle 2x2-*Hadamard–Matrix*. Reelle Hadamard-Matrizen haben nur die Matrixelemente 1 oder -1. Ihre Zeilenvektoren stehen senkrecht aufeinander. $\mathrm{H}^{\otimes n}$ ist (bis auf den Faktor $\frac{1}{\sqrt{2^n}}$) durch das n-fache Tensorprodukt der Matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ gegeben und führt auf eine 2^nx2^n-Hadamard-Matrix (Hadamard-Matrizen dieser Ordnung heißen Sylvester- oder Walsh-Matrizen). Im Zusammenhang mit den EPR-Zuständen werden wir auf diese Matrizen noch zurückkommen. □

Fourier–Transformation

Die endliche Fourier–Transformation in $\mathcal{H}^{\otimes n}$ ist ebenfalls das direkte Produkt von 1-q-Bit–Operationen. Allerdings hängen letztere von der Länge n des Multi–q-Bits ab. Mit der bei der Hadamard–Transformation eingeführten Konvention, $x = \{x_1, \ldots, x_n\}$, wird sie definiert durch

$$F^{\otimes n}|x\rangle = 2^{-n/2} \sum e^{2\pi i (xy)/m} |y\rangle, \quad m = 2^n. \tag{11}$$

Kontrollierte NOT–**Operation** (**controlled** NOT, CNOT, ^{C}NOT)

Klassisch ist CNOT eine umkehrbare 2-Bit–Operation:

$$xy \longrightarrow x'y' = \mathrm{CNOT}(xy) = x(x+y) \mod 2. \tag{12}$$

Ist das erste Bit nicht gesetzt, so bleibt das zweite ungeändert. Ist das erste Bit gesetzt, so wird das zweite der Operation NOT unterworfen.

Die CNOT–Operation ergibt für den Fall $x = 1$, wenn sie auf die Abbildung $y \longrightarrow y'$ eingeschränkt wird, gerade die NOT–Operation. Betrachten wir hingegen y' als Funktion der Eingänge x, y , dann erhalten wir eine Modifikation der ODER–Operation, das sogenannte exclusive–OR[8].

Eine analoge Konstruktion erfolgt im Quantenfall, wobei die Vektoren der Referenzbasis die klassische Bit–Situation ersetzen. Die allgemeine Definition einer kontrollierten Operation ist daher wie folgt:

Sei $U \in \mathrm{U}(2)$ eine 1-q-Bit–Operation. Das *kontrollierte* U läßt $|00\rangle$ und $|01\rangle$ unverändert. Aber für $x = 0, 1$ geht $|1x\rangle$ in $|1\rangle \otimes U|x\rangle$ über.

Speziell ist die unitäre Transformation CNOT (oder ^{C}NOT) durch

$$|00\rangle \longrightarrow |00\rangle \quad |01\rangle \longrightarrow |01\rangle$$

$$|10\rangle \longrightarrow |11\rangle \quad |11\rangle \longrightarrow |10\rangle$$

im 2-q-Bit–Hilberraum definiert. In Matrixdarstellung wäre das

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Petri–Toffoli–Gate (controlled–controlled NOT)

Das klassische Petri–Toffoli–Gate ist das *doppelt kontrollierte* NOT. Diese 3-Bit–Operation wendet NOT genau dann auf das dritte Bit an, wenn die ersten beiden Bits gesetzt sind, d.h. den Wert 1 haben. In jedem anderen Fall bleibt der 3-Bit–String ungeändert. Modulo 2 ist daher

$$xyz \longrightarrow xy(z + x \cdot y). \tag{13}$$

Petri [65] und Toffoli [81] zeigten die Universalität dieser Operation: Jede invertierbare Operation kann durch Kombination von Petri–Toffoli–Gates erreicht werden.

Die Umsetzung auf den 3-q-Bit–Hilbertraum ist offensichtlich: Bezogen auf die Referenzbasis der 3-q–Bits haben wir Molulo 2 den unitären Operator

$$|xyz\rangle \longrightarrow |xyz'\rangle, \quad z' = z + x \cdot y$$

[8] CNOT wird deshalb mitunter auch als XOR–Operation bezeichnet.

zu setzen.

Aus gruppentheoretischer Sicht ist es nicht verwunderlich, daß es verschiedene Mengen universeller Gates gibt, aus denen im Prinzip mit beliebiger Genaugkeit alle unitären Transformationen aufgebaut werden können. Beispiele findet man in [2] oder [79] (und der dort angegebenen Literatur). Es gilt beispielsweise ein gewisses Analogon zum klassischen Resultat von Petri und Toffoli: das Hadamard-Gate und CCNOT (das Petri–Toffoli– Gate) bilden solch eine Menge universeller Gates [73, 1].

Wir wollen noch darauf aufmerksam machen, daß es für die Realisierung von Quantencomputern (und natürlich auch für andere Quantenkanäle) wichtig ist, zu erreichen, daß ein gewisses Maß an "äußeren Rauscheinflüssen" (so führen z.B. Dekohärenz–Effekte zu einer Umwandlung von Multi-q-Bits in verrauschte Multi–q-Bits (Dichtematrizen)) und Ungenauigkeiten der Gates "toleriert" wird. Mit ihrem Konzept der "fault–tolerant quantum computation" haben Steane [78] und Shor [75] mit Hilfe fehlerkorrigierender Quantencodes einen ersten Schritt aufgezeigt (siehe auch den Überblick in [67, 68]).

2 Quanten–Algorithmen

2.1 Die Berechnung einer Funktion

Wir wollen die Berechnung einer Funktion

$$f : \{0,1\}^n \quad \longrightarrow \quad \{0,1\}^m$$

mit

$$\{0,1\}^n = \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{n} \quad \text{und} \quad \{0,1\}^m = \underbrace{\{0,1\} \times \cdots \times \{0,1\}}_{m}$$

als unitäre Operation darstellen. Den beiden kartesischen Produkten, d.h. den Bitfolgen der Länge n bzw. den Bitfolgen der Länge m, ordnen wir eineindeutig eine Multi–q-Bit–Basis der Hilberträume

$$\mathcal{H}_1 = \underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n} \quad \text{bzw.} \quad \mathcal{H}_2 = \underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{m}$$

zu. $\mathcal{H}$ bezeichnet auch in diesem Kapitel wieder den zweidimensionalen q-Bit–Hilbertraum, und eine Multi–q-Bit–Basis von $\mathcal{H}_1$ bzw. $\mathcal{H}_2$ bauen wir aus den Tensorprodukten einer q-Bit–Basis von $\mathcal{H}$ auf:

$$x = (x_1, \ldots, x_n) \in \{0,1\}^n$$

ordnen wir dem Basisvektor

$$|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \in \mathcal{H}_1$$

zu, wobei die Vektoren $|x_i\rangle\,(x_i = 0, 1)$ für alle i eine (synchronisierte) q-Bit–Basis von $\mathcal{H}$ bilden (entsprechend für $y = (y_1, \ldots y_m) \in \{0,1\}^m$).
Die "Resultat–Zustandsvektoren " $|f(x)\rangle \in \mathcal{H}_2$ für $x \in \mathcal{H}_1$ bilden damit eine orthogonale Familie. Durch Messung einer Observablen aus $\mathcal{H}_2$ (die die Eigenvektoren $\{|f(x)\rangle\}$ und zugehörige nichtentartete Eigenwerte hat) lassen sie sich — wie natürlich auch gewünscht — problemlos unterscheiden und signalisieren den jeweiligen Wert von f.
Unter der *Berechnung von f* verstehen wir dann die unitäre Transformation

$$U_f : \quad \mathcal{H}_1 \otimes \mathcal{H}_2 \longrightarrow \mathcal{H}_1 \otimes \mathcal{H}_2$$

mit der folgenden Wirkung auf den Basis–Vektoren

$$U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |f(x) + y\rangle.$$

Die Addition ist komponentenweise und modulo 2 zu verstehen. Speziell erhalten wir

$$U_f|x\rangle \otimes |0, ...0\rangle = |x\rangle \otimes |f(x)\rangle.$$

Bemerkung: Die Reversibilität der Berechnung von f, also der Unitarität von U_f, wird durch diese Darstellung im "Rechner–Hilbertraum" $\mathcal{H}_1 \otimes \mathcal{H}_2$, die die Eingangsdaten speichert, gesichert. Eventuell muß $\mathcal{H}_1 \otimes \mathcal{H}_2$ noch "weiter vergrößert" werden, um die tatsächliche Berechnung, die unter Umständen nur durch einen Folge von Gates ("Zwischenrechnungen") erreicht wird, zu ermöglichen.□

2.2 Das Problem von Deutsch und seine Verallgemeinerung

Wir wollen die früher geäußerte Vermutung, daß Quantenrechner klassischen Rechnern möglicherweise (zumindest für gewisse Problemklassen) überlegen sein könnten, etwas untermauern.
Dazu betrachten wir das *Problem von Deutsch* [25]:

Für eine Funktion $f : \{0,1\} \longrightarrow \{0,1\}$ soll entschieden werden, ob die Funktion f konstant ist ($f(0) = f(1)$) oder nicht ($f(0) \neq f(1)$) ?
Klassisch würde man $f(0)$ und $f(1)$ berechnen, um die Frage zu entscheiden. Quantenmechanisch erzeugen wir zuerst eine Superposition aller Zustandsvektoren, die zu den Argumenten, die für eine Berechnung in Frage kommen, gehören. Daran schließt sich die "simultane" Berechnung von f an, die zu einer Superposition aller Berechnungsergebnisse führt. Da wir uns aber nicht für die tatsächlichen Werte von f interessieren, sondern nur für die "globale" Eigenschaft, ob f konstant ist oder nicht, versuchen wir eine Observable zu finden, deren *einmalige* Messung schon ausreicht, um diese Eigenschaft zu bestimmen.

Im Rechner–Hilbertraum $\mathcal{H} \otimes \mathcal{H}$ starten wir mit dem Zustand $|0\rangle \otimes |1\rangle$. Die Anwendung der 2-fachen Hadamard–Transformation $H \otimes H$ (Erzeugung der Ausgangssuperposition) und der anschließenden Wirkung von U_f (Berechnung von f) führt auf die folgende Endsuperposition:

$$|0\rangle \otimes |1\rangle \xrightarrow{H\otimes H} \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle - |1\rangle \otimes |1\rangle)$$

$$\xrightarrow{U_f} \frac{1}{2}(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle - |0\rangle \otimes |f(0)+1\rangle - |1\rangle \otimes |f(1)+1\rangle) =$$

$$\frac{1}{4}(|0\rangle + |1\rangle) \otimes (|f(0)\rangle + |f(1)\rangle - |f(0)+1\rangle - |f(1)+1\rangle) +$$

$$\frac{1}{4}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle - |f(0)+1\rangle + |f(1)+1\rangle).$$

Wir benutzen jetzt für die Messung des ersten q-Bits eine nichtentartete Observable A, die die orthogonalen Eigenvektoren

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{und} \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

hat. Wie man am zweiten q-Bit des Tensorprodukts sieht, erlaubt nun die Messung von A, zweifelsfrei zu bestimmen, ob f konstant ist oder nicht:

- $f(0) = f(1) = f$ führt zu

$$\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|f\rangle - |f+1\rangle),$$

  korresponiert also zum Eigenvektor $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ des ersten q-Bits

- $f \neq$ const. (und damit $f(0) = f(1) + 1$ bzw. $f(1) = f(0) + 1$) liefert

$$\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

  und führt somit zum Eigenvektor $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ des ersten q-Bits.

Bemerkung:

Es bietet sich auch an, eine weitere Hadamard–Transformation auszuführen, um als Eigenbasis der zu messenden Observablen wieder die q-Bit–Basis $|0\rangle, |1\rangle$ zu erhalten (denn $H = H^{-1}$). Ein solcher Algorithmus zur Lösung des Problems von Deutsch ist mit NMR–Techniken realisiert worden (siehe [23, 50]).□

Eine leichte Verallgemeinerung des Problems von Deutsch , das sogenannte *Deutsch–Jozsa–Problem*, zeigt, daß dieser Algorithmus zu einem exponentiell verringertem Rechenaufwand im Vergleich zum klassischen Algorithmus führt. Es sollte allerdings betont werden, daß bei diesen Betrachtungen stets der Aufwand für die Berechnung der Funktion f *nicht* in Rechnung gestellt wird. Die Berechnung von f wird als eine klassische bzw. quantenmechanische Black–Box-Routine, als *Orakel* betrachtet, die unmittelbar das Resultat liefert. Den Aufwand messen wir daran, wie oft das klassische bzw. Quanten–Orakel befragt werden muß.

Gegeben sei eine Funktion

$$f : \{0,1\}^n \quad \longrightarrow \quad \{0,1\},$$

von der bekannt sei, daß sie entweder konstant oder ausgeglichen ist (d.h. den Wert 0 bzw. 1 für jeweils genau die Hälfte der Argumente annimmt). Das Deutsch–Jozsa–Problem besteht darin, zu bestimmen, welche dieser Eigenschaften die Funktion f hat. Wir übertragen jetzt den früheren Algorithmus.

Dazu starten wir mit dem Zustandsvektor

$$\underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n} \otimes |1\rangle \in \quad \mathcal{H}^{\otimes n} \otimes \mathcal{H}.$$

Werden nun die (n+1)–fache Hadamard–Transformation und die Berechnung von f ausgeführt, so erhalten wir (jeweils bis auf einen Faktor):

- für f =const. den Zustandsvektor

$$(\sum_{x\in\{0,1\}^n} |x\rangle) \otimes (|0\rangle - |1\rangle)$$

- für f ausgeglichen

$$(\sum_{f(y)=0} |y\rangle - \sum_{f(z)=1} |z\rangle) \otimes (|0\rangle - |1\rangle),\ y, z \in \{0,1\}^n.$$

Die Messung einer Observablen, die die beiden orthogonalen Zustandsvektoren der n q-Bits

$$\sum_{x\in\{0,1\}^n} |x\rangle \quad \text{und} \quad \sum_{f(y)=0} |y\rangle - \sum_{f(z)=1} |z\rangle \quad y, z \in \{0,1\}^n$$

unterscheidet, bestimmt wieder zweifelsfrei, welche Eigenschaft von f vorliegt.

Mit einer einmaligen quantenmechanischen Berechnung der Funktion f läßt sich also das Problem entscheiden, während im klassischen Fall die Funktion f mindestens $(2^{n-1}+1)$ –mal berechnet werden muß, um die Konstanz oder Ausgeglichenheit zu ermitteln.

2.3 Der Suchalgorithmus von Grover

Wir wollen noch kurz auf einen weiteren Algorithmus für ein sehr aufwendiges Problem eingehen. Es soll eine nicht strukturierte Datenbank mit $N = 2^n$ Einträgen nach einem bestimmten Eintrag durchsucht werden (man denke an das Problem, mit Hilfe des Telefonbuches zu einer bekannten Telefonnummer die zugehörige Person ausfindig zu machen). Würde man systemtisch oder probabilistisch die Datenbank durchsuchen, wird man im Mittel einen zeitlichen Aufwand in der Größenordnung von N (d.h. exponentiell in n, der Bitgröße der Einträge) einkalkulieren müssen. Der *Quantenalgorithmus von Grover* [40] reduziert zwar den zeitlichen Aufwand, um mit hoher Wahrscheinlichkeit den richtigen Eintrag zu finden, nur auf die Größenordnung $\sqrt{N}$, ist aber sicher für große N trotzdem noch interessant:

> "Quantum mechanics helps in searching for a needle in a haystack"[41].

Die Menge der Datenbankeinträge beschreiben wir durch $\{0,1\}^n$ (oder eine ihrer Teilmengen). Im Hilbertraum $\mathcal{H}^{\otimes n}$ repräsentieren wir die Datenbankeinträge natürlich wieder durch die oben eingeführten Basisvektoren $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$ mit $x = (x_1, \ldots, x_n) \in \{0,1\}^n$. Durch Messung einer nichtentarteten Observablen A, die diese Basisvektoren als Eigenvektoren besitzt, kann man folglich die Einträge unterscheiden. Der gesuchte Eintrag sei $x_0 \in \{0,1\}^n$ bzw. der ihm zugeordnete Vektor $|x_0\rangle \in \mathcal{H}^{\otimes n}$.

Das Heraussuchen des richtigen Eintrages betrachten wir als Funktionsberechnung. Wir starten mit dem Zustandsvektor

$$\underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n} \otimes |1\rangle \in \quad \mathcal{H}^{\otimes n} \otimes \mathcal{H}.$$

Die Hadamard–Transformation $H^{\otimes n} \otimes H$ führt dann auf

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes (|0\rangle - |1\rangle).$$

Berechnet wird nun die Funktion

$$g: \quad \{0,1\}^n \longrightarrow \{0,1\} \quad \text{mit}$$

$$g(x) = 0 \quad \text{für } x \neq x_0 \quad \text{und} \quad g(x_0) = 1.$$

Die zugeordnete unitäre Transformation U_g liefert

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes (|0\rangle - |1\rangle) \quad \xrightarrow{U_g}$$

$$\frac{1}{\sqrt{2^{n+1}}} (\sum_x |x\rangle) \otimes (|g(x)\rangle - |g(x)+1\rangle) =$$

$$\frac{1}{\sqrt{2^{n+1}}} (\sum_{x \neq x_0} |x\rangle - |x_0\rangle) \otimes (|0\rangle - |1\rangle).$$

Betrachten wir nun, welche Wirkung U_g auf die ersten n q-Bits hatte, so sehen wir, daß die unitäre Transformation $\mathbf{1} - 2\,|x_0\rangle\langle x_0|$ (Spiegelung an Ebene senkrecht zu $|x_0\rangle$) ausgeführt wurde:

$$|x\rangle \longrightarrow |x\rangle, x \neq x_0, \quad \text{und} \quad |x_0\rangle \longrightarrow -|x_0\rangle.$$

Wir benötigen noch eine weitere Operation auf den ersten n q-Bits, die Spiegelung

$$2\,|s\rangle\langle s| - \mathbf{1}.$$

$|s\rangle$ ist die Abkürzung für den (nach der anfänglichen) Hadamard–Transformation in $\mathcal{H}^{\otimes n}$ entstandenen "Startvektor"

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$$

Diese unitäre Operation bewirkt

$$|s\rangle \longrightarrow |s\rangle \quad \text{und} \quad |y\rangle \longrightarrow -|y\rangle \quad \text{für alle} \quad |y\rangle \,\text{senkrecht zu}\, |s\rangle.$$

Die Hintereinanderausführung dieser beiden Spiegelungen

$$(2\,|s\rangle\langle s| - \mathbf{1})(\mathbf{1} - 2\,|x_0\rangle\langle x_0|)$$

führt (als Produkt einer geraden Zahl von Spiegelungen) zu einer Drehung in der Ebene, die durch die Vektoren $|x_0\rangle$ und $|s\rangle$ bestimmt wird. Der Startvektor $|s\rangle$ wird dadurch in Richtung unseres gesuchten Zustandsvektors $|x_0\rangle$ gedreht:

$$|s\rangle \longrightarrow (2\,|s\rangle\langle s| - \mathbf{1})(\mathbf{1} - 2\,|x_0\rangle\langle x_0|)\,|s\rangle =$$

$$(1 - 4\,|\langle x_0|s\rangle|^2)\,|s\rangle + 2\,\langle x_0|s\rangle\,|x_0\rangle.$$

Wenn wir beachten, daß $\langle x_0|s\rangle = \frac{1}{\sqrt{N}}$ [9], dann bemerken wir, daß für großes N die Vektoren $|x_0\rangle$ und $|s\rangle$ fast senkrecht aufeinander stehen und der Drehwinkel von der Größenordnung $\frac{2}{\sqrt{N}}$ ist.

Der Grover–Algorithmus besteht nun darin, diese Drehung so lange zu wiederholen bis der resultierende Zustandsvektor "genügend weit an $|x_0\rangle$ herangerückt"ist, so daß infolge der großen Übergangswahrscheinlichkeit eine Messung unserer Datenbank-Observablen A mit großer Wahrscheinlichkeit tatsächlich den gesuchten Eintrag x_0 ergibt. Die Zahl der Wiederholungen sollte dabei in der Größenordnung $\frac{\pi/2}{2/\sqrt{N}} = \frac{\pi}{4}\sqrt{N}$ liegen. Um nicht an x_0 "vorbeizudrehen"und eine möglichst hohe Erfolgswahrscheinlichkeit zu erreichen, ist es wichtig, die optimale Zahl der Wiederholungen genau zu kennen (siehe [16]).

Bemerkungen:

Der besonders einfache Fall $N = 4$, bei dem (wie man sich schnell überzeugt) nach einer einzigen Drehung sogar mit Sicherheit der gesuchte Zustand erreicht wird, ist mit NMR–Methoden realisiert worden (siehe [22]).
Der zeitliche Aufwand[10], einen Eintrag in einer Datenbank der Größe N zu finden, liegt für den Grover-Algorithmus in der Größenordnung $\sqrt{N}$. Diese Größenordnung wird von keinem anderen Quanten-Algorithmis unterboten([16] und insbesondere [91]).□

2.4 Der Faktorisierungsalgorithmus von Shor

Etwas ausführlicher soll nun auf einen Algorithmus eingegangen werden, der ebenfalls probabilistisch ist und seit 1994 das Interesse an Quantencomputern ganz

[9] Der Startvektor $|s\rangle$ hat zu jedem Datenbankeintrag $|x\rangle$ die Übergangswahrscheinlichkeit $|\langle x|s\rangle|^2 = \frac{1}{N}$.

[10] Der zeitliche Aufwand wird daran gemessen, wie oft die Funktion g berechnet werden muß (Anzahl der Orakel–Anfragen) — mit anderen Worten: wie oft die beschriebene Drehung wiederholt werden muß.

wesentlich stimuliert hat — der *Faktorisierungsalgorithmus von Shor* [74],[76]. Shor konnte zeigen, daß mit einem Quantencomputer der zeitliche Aufwand für die Faktorisierung einer natürlichen Zahl n in ihre Primfaktoren nur wie ein Polynom in $\log_2 n$ (der Bitgröße von n) wächst. Die bekannten klassischen Algorithmen ermöglichen (wenn auch mit großen Unterschieden) letzlich doch nur eine Faktorisierung mit exponentiell steigendem Aufwand[11] in $\log_2 n$. Allerdings gibt es keinen Beweis, daß klassische Algorithmen prinzipiell derart beschränkt sind (siehe [69])[12].
Wir wollen das Verfahren von Shor beschreiben[13], aber darauf verzichten, explizite Gates für die Realisierung der Teiloperationen anzugeben (siehe z.B. [5]). Auch für die Abschätzung der zeitliche Effizienz der Teiloperationen (insbesondere der modularen Operationen und der Fouriertransformation), die zusammengefügt letztlich nur zu einem in $\log_2 n$ polynomialen Aufwand führen, sei auf Shor's Arbeit [76] verwiesen.

Gegeben sei eine ungerade Zahl n. Wir wollen auch annehmen, daß n keine Potenz einer ungeraden Primzahl sei. Um letztere Eigenschaft zu testen, gibt es effiziente Verfahren (siehe [69]). Die Aufgabe besteht nun darin, von dieser Zahl n einen (nichttrivialen) Faktor zu ermitteln, so daß wir n als Produkt darstellen können. Sukzessive Fortsetzung des Verfahrens mit den gefundenen Faktoren würde dann letztendlich zur Primzahlzerlegung von n führen.

Als nächsten Schritt wollen wir uns davon überzeugen, daß ein Faktor von n mit einer gewissen Wahrscheinlichkeit (nach dem von Shor benutzten Verfahren von G.L. Miller) gefunden werden kann, wenn die Periode der Funktion

$$f(x) = a^x \bmod n$$

bekannt wäre, wobei a eine *zufällig* gewählte natürliche Zahl mit $a < n$ und $\mathrm{ggT}(a, n) = 1$[14] ist. Als Periode von f bezeichnen wir die kleinste natürliche Zahl r mit $f(x+r) = f(x)$ und damit auch die kleinste natürliche Zahl r mit $a^r = 1 \bmod n$.

[11] Ein naiver Divisionsalgorithmus erfordert eine Größenordnung von $\sqrt{n}$ Divisionen, um zwei Faktoren von n zu finden. Das ergibt einen exponentiellen Aufwand in $\log_2 n$, da $\sqrt{n} = (2^{\log_2 n})^{\frac{1}{2}} = 2^{\frac{1}{2}\log_2 n}$.

[12] Auf den Schwierigkeiten, die klassische Rechner mit der Faktorisierung großer Zahlen (und mit ähnlich gelagerten Problemen) haben, basiert die Sicherheit weitverbreiteter kryptographischer Verfahren (Public–Key–Kryptographie à la RSA u.a. — siehe z.B. [52] oder etwas unterhaltsamer [4]).

[13] Neben den Originalarbeiten [74, 76] findet man in [30] eine gute Darstellung dieses Algorithmus. Eine Übersicht findet man auch in vielen einführenden Arbeiten zur Quanten–Informatik, von denen stellvertretend nur [85, 80, 68] genannt seien.

[14] $\mathrm{ggT}(a, n)$ = größter gemeinsamer Teiler von a und n. Die Berechnung des größten gemeinsamen Teilers zweier Zahlen ist mit dem Euklidschen Algorithmus in polynomialer Zeit möglich.

Bemerkungen:

Für die Erfolgswahrscheinlichkeit des Verfahrens ist es wichtig, daß a zufällig gewählt wurde (siehe unten). Würde dabei zufällig ein a gewählt, für das $\mathrm{ggT}(a,n) \neq 1$, dann hätten wir bereits einen Faktor gefunden und wären fertig.
Die Forderung $\mathrm{ggT}(a,n) = 1$ sichert die Existenz der Periode r, denn nach dem Satz von Euler–Fermat ([43],Theorem 72) gilt für jedes a mit $\mathrm{ggT}(a,n) = 1$ stets $a^{\Phi(n)} = 1 \bmod n$ mit der Eulerschen Funktion Φ[15].
Aus der Beziehung $a^r = 1 \bmod n$ wird auch deutlich, daß die Forderung $a < n$ keine Einschränkung ist, da a ohnehin nur modulo n die Periode r bestimmt. Mit anderen Worten: r können wir auch als die Ordnung von a in der multiplikativen Gruppe der natürlichen Zahlen modulo n ansehen. □

Nehmen wir also vorläufig an, daß die Periode r bereits bestimmt werden konnte. Nun bedeutet $a^r = 1 \bmod n$, daß $a^r - 1 = (a^{r/2}+1)(a^{r/2}-1) = 0 \bmod n$. Da r schon die kleinste Zahl mit dieser Eigenschaft ist, muß $a^{r/2} - 1 \neq 0 \bmod n$ sein.

Als Resultat erhalten wir:

Ist r gerade und $(a^{r/2}+1)$ nicht bereits durch n teilbar ($(a^{r/2}+1) \neq 0 \bmod n$), dann haben wir mit $\mathrm{ggT}(a^{r/2}+1,n)$ und $\mathrm{ggT}(a^{r/2}-1,n)$ nichttriviale Faktoren von n gefunden.[16]

Wie erfolgreich ist das Verfahren ? Dem Erfolg des Verfahrens steht nur im Wege, daß unser gewähltes a zu ungeradem r und/oder zu $(a^{r/2}+1) = 0 \bmod n$ führt. Wird — wie gefordert — a zufällig gewählt, dann ist die Wahrscheinlichkeit dafür aber höchstens 1/2.
Die Erfolgswahrscheinlichkeit, auf die beschriebene Weise Faktoren zu finden, beträgt somit mindestens 1/2.[17]

Nun setzt der "Quantenteil" des Shor'schen Verfahrens ein und zeigt, wie man auf einem Quantenrechner die noch ausstehende Berechnung der Periode r tatsächlich realisieren kann.

Wir beginnen damit, den Rechner–Hilbertraum zu wählen. Er wird in der Form $\mathcal{H}_1 \otimes \mathcal{H}_2$ so gewählt, daß die Berechnung der Funktion

$$f(x) = a^x \bmod n$$

mit den oben gewählten a und n als unitäre Transformation U_f realisiert werden kann. Wir werden aber wegen der nachfolgenden Operationen zweckmäßigerweise

[15] $\Phi(n)$ = Anzahl der natürlichen Zahlen k mit $k \leq n$ und $\mathrm{ggT}(k,n) = 1$.

[16] Ist $(a^{r/2}+1) = 0 \bmod n$, erhielten wir lediglich die triviale Faktorisierung $n = 1 \cdot n$. Das würde immer eintreten, wenn (was wir von vornherein ausgeschlossen haben) n Potenz einer ungeraden Primzahl wäre.

[17] Um nicht vom Hauptanliegen abzulenken, sei für diese Abschätzung auf [76] oder den (noch ausführlicheren) Anhang von [30] verwiesen.

nicht die Dualdarstellung der Argumente und Funktionswerte verwenden, sondern deren Dezimaldarstellung bevorzugen.

Der "Argument–Hilbertraum" $\mathcal{H}_1$ soll die Dimension $q = 2^m$ haben, wobei $n^2 \leq 2^m < 2n^2$ und die Vektoren $|x\rangle$ mit $0 \leq x \leq q-1$ eine orthonormierte Basis von $\mathcal{H}_1$ bilden. Diese Wahl der Dimension hat zahlentheoretische Gründe, die wir vorläufig übergehen. Für den "Werte–Hilbertraum" $\mathcal{H}_2$ nehmen wir an, daß die Vektoren $|a^x \bmod n\rangle$ (wegen der Periodizität sind das lediglich r voneinander verschiedene Vektoren) eine orthonormale Familie bilden. Die Dimension von $\mathcal{H}_2$ müßte demnach eigentlich nur r betragen. Da wir die Periode r aber nicht kennen, wählen wir die Dimension einfach "groß" genug. Die Dimension von $\mathcal{H}_2$ sei n[18].

Gestartet wird mit dem Zustandsvektor

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle \otimes |0\rangle$$

des Rechner–Hilbertraums (der vielleicht mit Hilfe der Hadamard–Transformation aus einem Basisvektor $|x\rangle \otimes |y\rangle$ erzeugt wurde). Die zu f gehörende unitäre Transformation U_f (definiert wie im Abschnitt 2.1) soll die folgende Operation ausführen

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle \otimes |0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle \otimes |a^x \bmod n\rangle.$$

Daran schließen wir die Fouriertransformation $F^{\otimes m} \otimes \mathbf{1}$ an und erhalten

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle \otimes |a^x \bmod n\rangle \longrightarrow \frac{1}{q} \sum_{c=0}^{q-1} \sum_{x=0}^{q-1} e^{\frac{2\pi i x c}{q}} |c\rangle \otimes |a^x \bmod n\rangle.$$

Berücksichtigen wir jetzt, daß

$$|a^x \bmod n\rangle = |a^k \bmod n\rangle,$$

wenn $a^x = a^k \bmod n$, wobei wir wegen der Periode r auch noch $0 \leq k < r$ wählen können, dann ergibt das die folgende Superposition der orthonormalen Vektoren $|c\rangle \otimes |a^k \bmod n\rangle$ ($c = 0, .., q-1$ und $k = 0, ...r-1$):

$$\frac{1}{q} \sum_{c=0}^{q-1} \sum_{k=0}^{r-1} \Big(\sum_{x : a^x = a^k \bmod n} e^{\frac{2\pi i x c}{q}} \Big) |c\rangle \otimes |a^k \bmod n\rangle.$$

Dieser Zustandsvektor aus $\mathcal{H}_1 \otimes \mathcal{H}_2$ bestimmt nun einen Zustand in $\mathcal{H}_1$ (reduzierte Dichtematrix), der die Wahrscheinlichkeiten für die Resultate von Messungen in $\mathcal{H}_1$ beschreibt. Wir wollen die entstandenen Interferenzeffekte nun nutzen, um mit Hilfe

[18] Das schon früher angeschnittene Problem, "weitere Dimensionen für Zwischenrechnungen vorzusehen ", bereitet keine Schwierigkeiten und wird übergangen.

einer Messung von c - sprich: einer Observablen aus $\mathcal{H}_1$, die die Eigenvektoren $|c\rangle$ hat - die Periode r zu bestimmen. Die Wahrscheinlichkeit für c ergibt sich zu

$$\sum_{k=0}^{r-1} |\frac{1}{q} \sum_{x:a^x=a^k \bmod n} e^{\frac{2\pi i x c}{q}}|^2.$$

Wir verwenden jetzt, daß $a^x = a^k \bmod n$ der Beziehung $x = k \bmod r$ äquivalent ist, d.h. $x = br + k$ und b läuft für festes k (wegen $x = 0, \ldots q-1$) von 0 bis $[\frac{q-1-k}{r}]$[19]. Der Ausdruck für die Wahrscheinlichkeit von c läßt sich damit umformen in

$$\sum_{k=0}^{r-1} |\frac{1}{q} \sum_{b=0}^{[\frac{q-1-k}{r}]} e^{\frac{2\pi i(br+k)c}{q}}|^2 = \sum_{k=0}^{r-1} |\frac{1}{q} \sum_{b=0}^{[\frac{q-1-k}{r}]} e^{\frac{2\pi i b r c}{q}}|^2.$$

Maximale Wahrscheinlichkeit haben damit alle Werte c, für die das Produkt $r \cdot c$ durch q teilbar ist: es müßte dann

$$\frac{r \cdot c}{q} = d \quad \text{oder} \quad \frac{c}{q} - \frac{d}{r} = 0$$

für eine gewisse ganze Zahl d sein.

Besonders einfach wäre der Fall, daß r Teiler von q und damit auch eine Potenz von 2 ist. Dann ergäbe jede Messung sogar mit Sicherheit einen Wert c, der ein Vielfaches von $\frac{q}{r}$ ist. Wären auch noch d und r teilerfremd, so hätten wir $\frac{c}{q}$ nur noch zu kürzen bis Zähler und Nenner teilerfremd sind, und r ließe sich — wegen $\frac{c}{q} = \frac{d}{r}$ — ablesen.
Wie wahrscheinlich es ist, daß bei zufälligem d, d und r teilerfremd sind, läßt sich leicht bestimmen. Mit der Eulerschen Funktion $\Phi(r)$, die gerade die Anzahl der zu r teilerfremden Zahlen, die kleiner oder gleich r sind, angibt, wäre diese Wahrscheinlichkeit $\frac{\Phi(r)}{r}$. Wir müssen deshalb im Mittel das ganze Verfahren (von der Präparation des Startvektors bis zur Messung von c) hinreichend oft, nämlich in der Größenordnung $\frac{r}{\Phi(r)}$, wiederholen, um die richtige Periode r herauszufinden. Nach jeder Wiederholung würden wir überprüfen[20], ob der durch Kürzung von $\frac{c}{q}$ bestimmte Wert von r tatsächlich bereits die gesuchte Periode ist.
Damit der Gesamtaufwand tatsächlich aber nur polynomial ist, sollte die mittlere Zahl der Wiederholungen natürlich (asymptotisch) höchstens in der Größenordnung von $\log_2 n$ (oder einer Potenz davon) liegen. Wenn wir uns jetzt erinnern, daß $r \leq \Phi(n) < n$ für $n > 1$, dann ersehen wir schon aus der groben Abschätzung:
$\pi(r) \equiv \{\text{Anzahl der Primzahlen} \leq r\} \leq \Phi(r)$ und dem fundamentalen Primzahlverteilungsgesetz $\pi(r) \sim \frac{r}{\ln r}$ [43], daß die mittlere Zahl der Wiederholungen

$$\frac{r}{\Phi(r)} \leq \frac{r}{\pi(r)} \sim \ln r \leq \ln n$$

[19] $[x]$ = ganzer Teil von x.
[20] Das erfordert nur polynomialen Aufwand (siehe [74, 76].

die Größenordnung von $\log_2 n$ nicht übersteigen wird[21].

Im allgemeinen Fall, wenn r kein Teiler von q ist, würden wir trotzdem erwarten, daß die Wahrscheinlichkeitsverteilung bei jenen c konzentriert ist, für die rc "fast" durch q teilbar ist, d.h. ein d mit $\frac{c}{q} - \frac{d}{r} \approx 0$ existiert .
In Anlehnung an die Argumente von Shor [74, 76, 30] wollen wir noch kurz zeigen, wie man in diesem Fall mit einem "verfeinerten " Verfahren die Periode bestimmen kann. Dabei wird auch verständlich werden, warum eingangs die Dimension q des "Argument"–Hilbertraumes $\mathcal{H}_1$ in der Größenordnung n^2 gewählt worden war.

Aus obigem Ausdruck für die Wahrscheinlichkeit des Wertes c ersehen wir, daß das Produkt rc nur modulo q eingeht. Wir können es deshalb immer auf einen Wert im Intervall $[-q/2, q/2]$ reduzieren. Weiterhin wird diese Wahrscheinlichkeit wegen $k < r < n << q \sim n^2$ zuverlässig durch

$$r|\frac{1}{q}\sum_{b=0}^{[\frac{q}{r}]-1} e^{\frac{2\pi i b r c}{q}}|^2$$

approximiert, wobei $k = r - 1$ gesetzt wurde. rc nennen wir "fast durch q teilbar", wenn $-r/2 \leq rc \mod q \leq r/2$. Anders ausgedrückt: es existiert eine ganze Zahl d mit

$$|rc - dq| \leq \frac{r}{2} \text{ oder } |\frac{c}{q} - \frac{d}{r}| \leq \frac{1}{2q}.$$

Wie groß ist die Wahrscheinlichkeit, bei einer Messung den Wert c, so daß rc fast durch q teilbar ist, zu finden ? Eine untere Grenze für diese Wahrscheinlichkeit erhalten wir durch Aufsummation der obigen geometrischen Reihe für den Grenzfall $|rc \mod q| = r/2$ und Berücksichtigung von $r < n << q \sim n^2$:

$$\{\text{Wahrscheinlichkeit für c mit } -r/2 \leq rc \bmod q \leq r/2\}$$

$$\leq \frac{r}{q^2}\frac{1}{\sin^2 \frac{\pi r}{2q}} \sim \frac{r}{q^2}\frac{1}{(\frac{\pi r}{2q})^2} = \frac{4}{\pi^2 r}.$$

Da die Anzahl der Werte c, für die rc fast durch q teilbar ist, offenbar gerade r beträgt, ist die Gesamtwahrscheinlichkeit, bei der Messung derartige c zu finden, mindestens

$$r\frac{4}{\pi^2 r} = \frac{4}{\pi^2}.$$

Nehmen wir nun an, unsere Messung habe tatsächlich ein c ergeben, für das

$$|\frac{c}{q} - \frac{d}{r}| \leq \frac{1}{2q}$$

[21] Diese Abschätzung wird unter Verwendung der Asymptotik der Eulerschen Funktion (z.B. [43]) noch wesentlich günstiger.

mit einem gewissen d. Da $r \leq n$ und $n^2 \leq q \leq 2n^2$, kann es nur *eine* rationale Zahl $\frac{d}{r}$ geben, die die uns bereits durch die Messung bekannte rationale Zahl $\frac{c}{q}$ mit dem Fehler $\frac{1}{2q}$ approximiert. Mit einem effizienten (d.h. nur polynomial aufwendigen) Verfahren — der Kettenbruchzerlegung[22] — läßt sich diese Approximation, d.h. $\frac{d}{r}$, bestimmen. Nehmen wir nun weiterhin an, daß d und r auch noch teilerfremd sind, dann ist damit die Periode r ablesbar.
Die Wahrscheinlichkeit, daß d und r teilerfremd sind, ist (bei näherungsweiser Gleichwahrscheinlichkeit der Werte) wieder $\frac{\Phi(r)}{r}$, so daß wir ein probabilistisches Verfahren gefunden haben, daß mindestens mit der Wahrscheinlickeit $\frac{4\Phi(r)}{\pi^2 r}$ zum Erfolg führt.

Die "Zusammenschaltung" aller Verfahren und Operationen liefert damit einen probabilistischen Faktorisierungsalgorithmus, der nur mit polynomialen Aufwand arbeitet.

[22]Wir wollen nur anmerken, daß sich jede rationale Zahl x eindeutig durch einen endlichen Kettenbruch der Form $[a_0; a_1, \ldots, a_N] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$ mit der ganzen Zahl a_0 und den natürlichen Zahlen $a_1, \ldots, a_N$ darstellen läßt. Die Approximationen von x — gegeben durch die Kettenbruchnäherungen $\frac{s_k}{t_k} = [a_0; a_1, \ldots, a_k]$ mit $k < N$ — haben genau einen Fehler $\frac{1}{t_k^2}$, wie wir ihn oben angetroffen haben . Informationen zu Kettenbrüchen findet man in Zahlentheorie–Texten, z.B. [43].

3 Messung und Präparation

3.1 Präparation reiner Zustände

Ehe man Quanteninformation verarbeiten und übermitteln kann, muß man sie herstellen und lesen können. Um zu sehen, wie dies bewerkstelligt wird, wollen wir in diesem Abschnitt an einige wohlbekannte quantenphysikalische Grundkenntnisse erinnern.

Die reinen Zustände eines quantenphysikalischen Systems denken wir uns durch (normierte) Vektoren eines Hilbertraumes $\mathcal{H}$ gegeben, der beliebig gewählt werden kann, aber im Hinblick auf unsere Anwendungen in der Regel endlichdimensional ist. Wie üblich wird die Algebra aller beschränkten Operatoren, die in $\mathcal{H}$ wirken, mit $\mathcal{B} := \mathcal{B}(\mathcal{H})$ bezeichnet.
Grundsätzlich kann jeder hermitische[23] Operator dieser Algebra eine Observable sein[24]. Allerdings sind nur solche Observable einer *apparativen* Messung zugänglich, die einen *endlichen Wertevorrat* besitzen. Nicht nur, daß keine Meßapparatur unendlich viele Meßwerte unterscheiden kann, ein solches Gerät würde ein Quantenalphabet definieren, das pro Buchstabe eine unendlich große Information zu tragen erlaubt.
Eine allgemeine Observable kann daher nur approximativ ausgemessen werden. Es gehört zu ihr eine kommutative Familie von Operatoren mit endlichem Wertevorrat, also von Meßapparaturen, welche sich der fraglichen Observablen jeweils innerhalb eines Meßbereichs und mit einer gewissen Meßgenauigkeit annähern. Mathematisch gesehen erzeugt eine Observable eine unitale kommutative von Neumann Algebra, in der die Operatoren mit endlichem Spektrum dicht liegen.

Das Erzeugen und das Lesen von Quanteninformation basiert auf observablen Größen, die im obigen Sinne durch eine Meßapparatur repräsentiert werden können. Sei also $A = A^*$ ein Operator mit endlichem Wertevorrat. Seine verschiedenen Eigenwerte seien $\lambda_1, \lambda_2, \ldots, \lambda_m$. Die Menge der Eigenvektoren zum Eigenwert λ_k ist ein linearer Unterraum von $\mathcal{H}$. Der Projektionsoperator P_k bilde unseren Hilbertraum $\mathcal{H}$ auf diesen Unterraum, nämlich auf $P_k\mathcal{H}$, ab. Damit gilt

$$A = \lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_m P_m. \tag{14}$$

Angenommen, der Zustand unseres Systems sei durch den Einheitsvektor ("Zustandsvektor") ψ gegeben. Bei der Messung der physikalischen Größe, die vom Operator A repräsentiert wird, wird die Meßapparatur einen der Eigenwerte von A anzeigen.
Welcher Eigenwert wird angezeigt? Ist ψ nicht ein Eigenvektor von A, so können

[23] In der Tat sind auch normale Operatoren observabel.

[24] Superauswahlregeln und andere grundsätzlichen Einschränkungen werden der Einfachheit halber nicht betrachtet.

wir das *nicht* im voraus wissen; das Erscheinen der möglichen Eigenwerte ist absolut zufällig. Wir kennen nur die *Wahrscheinlichkeit* ihres Auftretens: Die Wahrscheinlichkeit p_k, daß der Eigenwert λ_k angezeigt wird, ist der Erwartungswert des Projektors P_k im Zustand vor der Messung:

$$p_k = \langle \psi, P_k \psi \rangle. \tag{15}$$

Hier setzt nun eine weitere Grundregel ein, die die Präparation beherrscht:
WENN das Meßinstrument λ_k anzeigt, *DANN* befindet sich das System in einem Eigenzustand des Operators A mit diesem Eigenwert.
p_k ist daher die Wahrscheinlichkeit für den Übergang des Zustandes ψ in einen solchen Eigenzustand. Die Auswahl seines Eigenvektors ist wie folgt geregelt:

$$\psi \longrightarrow \psi_k := \frac{1}{\sqrt{p_k}} P_k \, \psi. \tag{16}$$

Manchmal ist es geschickter, auf die Normierung des Eigenvektors zu verzichten und zu sagen, $P_k\psi$ sei präpariert worden. Physikalisch ist das äquivalent.
Hierzu noch einige Anmerkungen:
a) Es ist einleuchtend, daß eine Wahrscheinlichkeit, wenn sie nicht extrem nahe bei 0 oder 1 liegt, *nichts* für eine Einzelmessung bedeutet. Bei *einem* Ereignis verlieren Wahrscheinlichkeiten völlig ihre Kraft. Nur wenn wir Zugang zu hinreichend vielen Systemen haben, die sich alle (hinreichend genau) im Zustand ψ befinden, werden sich die Übergangswahrscheinlichkeiten zeigen. ("Man braucht eine Menge Photonen, um ein Interferenzmuster zu sehen.")

b) Wir wissen, daß linear abhängige Zustandsvektoren den gleichen Zustand beschreiben. Haben wir jedoch zwei Zustandsvektoren, so ist ihre relative Phase physikalisch bedeutsam. Dies ist hier der Fall, da (16) festlegt, daß die Übergangsamplitude $\langle \psi, \psi_k \rangle$ reell und positiv zu sein hat.

c) Es sollte angemerkt werden, daß oben nur die Grundform des apparativen Meßprozeßes dargestellt wurde, die oft mit anderen kombiniert auftritt. Zum Beispiel entsteht aus A ein *Filter*, wenn für einige Eigenwerte die präparierten Zustände vom Meßinstrument aufgenommen werden. (Man denke an ein Polarisationsfilter, dessen Material idealerweise nur Photonen einer Polarisationsrichtung absorbiert, die zu ihr senkrecht polarisierten Photonen aber durchläßt; oder an einen Stern–Gerlach Versuch, bei dem der unerwünschte Strahl auf ein Target geleitet wird.) Wesentlich raffiniertere Anordnungen entstehen durch Kombination von Meßprozeß und Interferometrie.

d) Die Quantentheorie erlaubt die Existenz von Meßgeräten zu Observablen mit endlichem Spektrum. Sie sagt aber fast nichts, wie diese herzustellen sind.

e)J. v. Neumann [86] betrachtete in erster Linie die Präparation bei vollständigen Messungen. Für Messungen bei entartetem Eigenwert λ_k nahm er an, daß der resultierende Zustand durch eine vom Meßgerät getroffene Auswahl der Basis im Unterrraum $P_k\mathcal{H}$ des entarteten Eigenwertes bestimmt wird und damit i.a. nicht unabhängig vom konkreten Meßgerät ist (s. Kap. V.1 in [86]). Die oben angegebene

Regel, daß lediglich in den zum Eigenwert gehörenden Unterraum projiziert wird, ist eine Abänderung, die auf Lüders zurückgeht [56]. Sie beseitigt diese Abhängigkeit von der konkreten Meßanordnung und ist dadurch ausgezeichnet, daß sie in einem gewissen Sinne zur minimalsten Zustandsänderung führt, weil sie nicht in den Unterraum $P_k\mathcal{H}$ "eingreift".Die Wahrscheinlichkeit, den entarteten Eigenwert λ_k im Zustand $P = |\psi\rangle\langle\psi|$ zu messen, ist in jedem Fall $\mathrm{Tr}PP_k = \langle\psi, P_k\psi\rangle$.

Wir wollen unsere Aufmerksamkeit noch auf einen interessanten Aspekt des oben Gesagten lenken. Ein Blick auf den output–Zustandsvektor (16) zeigt eine erstaunliche Unabhängigkeit von der Observablen A und ihren Eigenwerten. Wir können die gleiche Präparation mit jeder geeigneten, die Projektoren P_k unterscheidenden Funktion

$$f(A) = \sum_{j=1}^{m} f(\lambda_j)\, P_j \tag{17}$$

von A erreichen. Mit anderen Worten, die genaue physikalische Natur von A (— es mag sich um Energie, Ort, Spin oder eine andere wichtige physikalische Größe handeln) spielt für die Präparation *keine* Rolle:
Für das Protokoll der Präparation ist es gleichgültig, ob der Meßapparat A oder $f(A)$ zu bestimmen gestattet. Es ist nur wichtig, daß die möglichen out–Zustände durch die Meßdaten unterschieden werden können.[25] Diese Einsicht wollen wir ein wenig formalisieren.

Wir erlauben in (17) beliebige komplexe Funktionen von A, deren Eigenwerte z.B. als Punkte auf einem Bildschirm angezeigt werden könnten. Die Menge aller $f(A)$ bildet dann eine Unteralgebra $\mathcal{C}_A$ von $\mathcal{B}$.

Wir benötigen den *Kommutanten* $\mathcal{C}'_A$ von $\mathcal{C}_A$ in $\mathcal{B}$. Ein Operator B kommutiert mit allen Funktionen $f(A)$ von A genau dann, wenn er mit A kommutiert:

$$B \in \mathcal{C}'_A \quad \Longleftrightarrow \quad [A, B] = AB - BA = 0. \tag{18}$$

Die Zerlegung von $\mathcal{H}$ in irreduzible Darstellungen von $\mathcal{C}'_A$ ist nun nichts anderes als die Zerlegung

$$\mathcal{H} = P_1\mathcal{H} \oplus P_2\mathcal{H} \oplus \cdots \oplus P_m\mathcal{H} \tag{19}$$

Wir können daher die Information, die in einer einzelnen Messung erhalten wird, wie folgt beschreiben:

(a) Der output–Vektor gehört zu einer irreduziblen Darstellung von $\mathcal{C}'_A$.

(b) Der Meßwert λ_k wird dann und nur dann angezeigt, wenn der output–Vektor zum Darstellungsraum $P_k\mathcal{H}$ gehört, d. h. der Meßwert *informiert uns, zu welcher* irreduziblen Darstellung von $\mathcal{C}'_A$ der neue Zustandsvektor gehört.

(c) Kennen wir *durch zusätzliche Informationen* (!) den input–Vektor ψ, so können wir schließen, daß der output–Vektor bis auf einen positiven Normierungsfaktor gleich $P_k\psi$ ist.

[25] Dies gestattet die Definition entropieartiger Maße für die Information. Aber Begriffe wie "Gleichgewicht" und "Temperatur" sind informationstheoretisch irrelevant.

Um einen Zustand mit Zustandsvektor φ zu erzeugen, wird eine Observable ausgewählt, die φ als Eigenvektor mit nicht–entartetem Eigenwert besitzt. Wird dieser Eigenwert gemessen, so ist klar, daß der durch φ charakterisierte Zustand vorliegt.

Die einfachste Observable, die dies erfüllt, ist der Projektor $|\varphi\rangle\langle\varphi|$. Wird der Eigenwert "1" angezeigt, so ist die Präparation gelungen. Erscheint der Eigenwert "0", so wird uns lediglich die Orthogonalität des erzeugten Zustandes zu φ angezeigt. Wird so mitgeteilt, daß die Präparation mißlungen ist, können wir den Zustand verwerfen und einen neuen Versuch zur Präparation des gewünschten Zustands unternehmen. Das Verwerfen kann durch einen Filter geschehen.

Je geringer die Entartung von Eigenwerten ist, umso mehr erfahren wir über den präparierten Zustand. Ideal ist daher, wenn keiner der Eigenwerte der Observablen entartet ist. Observable, die diese Bedingung erfüllen, führen *vollständige Messungen* aus. Genau dann leistet A vollständige Messungen, wenn (der Abschluß von) $\mathcal{C}_A$ eine maximale kommutative Algebra ist.
Sei nun λ der Eigenwert von A zum Eigenvektor φ, und A erzeuge eine maximal kommutative Algebra. Ergibt die Messung den Wert λ, so ist die Aufgabe erledigt. Wird allerdings ein von λ verschiedener Meßwert angezeigt, so wissen wir doch, um welchen Zustand es sich handelt: Es muß noch eine unitäre Transformation ausgeführt werden, die den falsch präparierten Zustandsvektor in den gewünschten transformiert.
Wird zusätzlich eine Verabredung darüber getroffen, welche unitären Transformationen falsch präparierte Zustandsvektoren in den gewünschten Zustand φ transformieren, so sprechen wir von einem *Protokoll zur Präparation von* φ.

Es ist wichtig, zu vermerken, daß dieses Protokoll *lokal* ist: Seine Durchführung kann im System des Hilbertraumes erfolgen, in dem der Zustand präpariert wird. (Gehört dieser Hilbertraum Alice, so benötigt sie keine Hilfe von Bob oder anderen Personen.) Auch die von Lüders erweiterte Regel, die Messungen an gemischten Zuständen beschreibt und auf die wir zurückkommen werden, ändert nichts am lokalen Charakter des Protokolls.

Nach der erfolgreichen Durchführung des Protokolls sind wir im Besitz einer Information vom Maß $I = \log_2 \dim \mathcal{H}$. Daher wird mit steigender Dimension die Präparation immer aufwendiger. Ist $\mathcal{H}$ nicht von endlicher Dimension, so ist das Protokoll undurchführbar: Wir müßten ein Meßgerät besitzen, das unendlich viele Meßwerte zu unterscheiden gestattet (und zusätzlich experimentellen Zugriff auf unendlich viele unitäre Operationen haben).
Können wir nur $m < \dim \mathcal{H}$ reine Zustände mit Hilfe der Messung unterscheiden und ebensoviele unitäre Operationen ausführen, so sind die Forderungen des Protokolls nur teilweise befriedigt: Die erfolgreiche Präparation kann nur mit einer gewissen Wahrscheinlichkeit (bzw. mit einer gewissenn Fehlerrate) durchgeführt werden. Diese Wahrscheinlichkeit hängt aber vom Ausgangszustand ab, ist also im ungünstigsten Fall dem Präparator unbekannt.

3.2 Die Lüders'sche Regel

Was geschieht bei einer Messung mit der Observablen (14), wenn kein reiner, durch einen Vektor definierter input–Zustand vorliegt? Der Zustand (oder das positive lineare Funktional) $\omega(\cdot)$ wird dann durch einen (nicht notwendig normierten) Dichteoperator ω beschrieben. Gemischter ("verrauschter") Zustand und Dichteoperator sind durch

$$B \longrightarrow \omega(B) = \mathrm{Tr}\, B\, \omega, \quad B \in \mathcal{B} \tag{20}$$

verknüpft. $\omega(B)$ ist der *Erwartungswert* des Operators B, wenn sich das System im Zustand ω befindet.[26] Gesucht wird die Ausdehnung der Regel (16) auf gemischte Zustände.

Die Antwort erhält man über eine *Purifizierung* von ω: ω wird als Reduktion eines reinen Zustandes (eines größeren Systems) angesehen. Auf diesen reinen Zustand wird dann Regel (16) angewendet. Das Ergebnis erweist sich als unabhängig von der Wahl der Purifikation.

Sei n_ω der Rang des Dichteoperators ω, also die Dimension des Unterraums von $\mathcal{H}$, der durch die Eigenvektoren zu nichtverschwindenden Eigenwerten von ω erzeugt wird. Wir betrachten dann einen erweiterten Hilbertraum

$$\mathcal{H} \otimes \mathcal{H}' \quad \text{mit} \quad \dim \mathcal{H}' \geq n_\omega$$

Ein Vektor ψ des Produktraumes *purifiziert* ω genau dann, wenn

$$\omega(B) = \langle \psi, (B \otimes \mathbf{1})\, \psi \rangle, \quad \forall\, B \in \mathcal{B}(\mathcal{H}).$$

Die Gesamtheit aller möglichen purifizierenden ψ wird mit Hilfe ihrer Gram–Schmidt– Zerlegung angegeben. Seien $p_1, p_2, \ldots$ die n_ω positiven Eigenwerte von ω und sei $\phi_1, \phi_2, \ldots$ ein zu ihnen gehörendes Orthonormalsystem

$$\omega\phi_j = p_j\phi_j, \quad p_j > 0.$$

Dann gibt es genau ein Orthonormalsystem der Länge n_ω in $\mathcal{H}'$ derart, daß

$$\psi = \sum \sqrt{p_j}\, \phi_j \otimes \phi'_j$$

ist. Der Purifizierung von ω im betrachteten Produktraum entsprechen somit eineindeutig die Orthonormalsysteme der Länge n_ω in $\mathcal{H}'$.

Die Regel (16) für einen der Projektoren $P_k \otimes 1$ aus der Zerlegung

$$A \otimes \mathbf{1} = \sum_j \lambda_j P_j \otimes \mathbf{1}$$

besagt jetzt, daß

$$\psi \longrightarrow \varphi_k := (P_k \otimes \mathbf{1})\psi = \sum \sqrt{p_j}\, P_k\phi_j \otimes \phi'_j$$

[26] Wir erinnern nochmals daran, daß wir in der Notation nicht zwischen einem Zustand und dem zugehörigen Dichteoperator unterscheiden werden.

mit der Wahrscheinlichkeit

$$\langle \psi, (P_k \otimes \mathbf{1})\psi \rangle = \omega(P_k).$$

präpariert wird.

Daher entsteht der (noch nicht normierte) Zustand

$$\begin{aligned} \omega_k(B) &:= \langle \varphi_k, (B \otimes \mathbf{1})\varphi_k \rangle \\ &= \langle \psi, (P \otimes \mathbf{1})(B \otimes \mathbf{1})(P \otimes \mathbf{1})\psi \rangle \\ &= \langle \psi, (PBP \otimes \mathbf{1})\psi \rangle \\ &= \omega(PBP) \end{aligned}$$

und wir erhalten als Resultat die *Lüders–Regel* [56]:

> Ist
>
> $$A = \lambda_1 P_1 + \lambda_2 P_2 + \cdots + \lambda_m P_m$$
>
> eine Observable mit den voneinander verschiedenen Eigenwerten λ_k, dann ergibt die Messung von A beim Vorliegen des Zustandes ω mit Wahrscheinlichkeit $\omega(P_k)$ den Zustand ω_k,
>
> $$\omega_k(B) = \omega(P_k)^{-1}\omega(P_k B P_k), \quad B \in \mathcal{B}(\mathcal{H}), \tag{21}$$
>
> oder — für unsere Zwecke gleichbedeutend — den (noch nicht normierten) Dichteoperator $P_k \omega P_k$.

Ist ψ eine Purifizierung von ω, so ist umgekehrt ω die *Reduktion* von $|\psi\rangle\langle\psi|$ nach $\mathcal{H}$. Allgemeiner heißt ω Reduktion eines über $\mathcal{H} \otimes \mathcal{H}'$ gegebenen Zustandes $\tilde{\omega}$, wenn

$$\omega(B) = \tilde{\omega}(B \otimes \mathbf{1}), \quad \text{für alle } B \in \mathcal{B} \tag{22}$$

gilt. Auch von der Dichtematrix ω sagt man dann, sie sei die Reduktion der Dichtematrix $\tilde{\omega}$. Die Abbildung, die die Dichteoperatoren von $\mathcal{H} \otimes \mathcal{H}'$ auf die von $\mathcal{H}$ reduziert, ist die *partielle Spur* über $\mathcal{H}'$ (bezeichnet mit $\mathrm{Tr}_{\mathcal{H}'}$).

3.3 Das Problem, Quantenzustände zu kopieren

Um den Zustand eines Systems bestimmen zu können, benötigen wir von ihm viele (fast) identische Exemplare. Wir können durch kein Experiment erkennen, in welchem Zustand sich ein individuelles Quantensystem befindet.
Die Chance, Kenntnisse über einen individuellen Zustand zu erfahren, eröffnet sich erst, wenn wir bereits etwas über seine Lage im Zustandsraum wissen. Der Idealfall ist, wenn bereits erwiesen ist, daß unser unbekannter Zustandsvektor Eigenvektor einer Observablen mit nichtentartetem Spektrum ist.

Gibt es einen "Quantenkopierer", der uns einen unbekannten Zustand exakt dupliziert, so daß wir uns durch wiederholte Betätigung dieses Vorganges so viele identische Kopien herbeischaffen könnten, wie wir zu einer Ausmessung des Zustandes mit vorgegebener Genauigkeit benötigen? Die Antwort lautet:
Ein solches Gerät *widerspricht* den Grundannahmen der Quantenphysik.

Dieks [27], Wooters und Zurek [90] haben für reine Zustände diese sehr einfache Antwort gefunden, und letztere haben sie in die Worte gekleidet:

> *"quantum states cannot be cloned".*

Ein einfaches Argument geht folgendermaßen: Wir interessieren uns für universelle Kopierer, die jeden beliebigen reinen Zustand kopieren. Für jeden input–Zustandsvektor $\psi \in \mathcal{H}$ unseres Systems muß der Kopierer notwendigerweise $\psi \otimes \psi$ als output liefern.

Angenommen, der Kopierer sei vor seiner Aktion im Zustand $\chi \in \mathcal{H}_c$, danach im Zustand χ'. $\mathcal{H}_c$ ist der Hilbertraum, der den Kopierer zu beschreiben gestattet. Weiter sei $\mathcal{H}'$ der Hilbertraum, in dem die Kopie erstellt werden soll (und den wir mit $\mathcal{H}$ identifizieren werden). Anfangs liege hier ein beliebiger Zustand φ vor, der aber nicht von dem zu kopierenden Zustand abhängen darf. Gesucht ist ein unitärer Operator U, der für alle ψ die Transformation

$$U\,\chi \otimes \psi \otimes \varphi = \chi' \otimes \psi \otimes \psi$$

bewirkt (alle Vektoren seien normiert). Da die unitäre Transformation U die Skalarprodukte der Vektoren in $H_c \otimes \mathcal{H} \otimes \mathcal{H}'$ unverändert läßt, folgt für zwei beliebige Zustandsvektoren $\psi_1, \psi_2 \in \mathcal{H}$

$$\langle \psi_1, \psi_2 \rangle = \langle \psi_1, \psi_2 \rangle^2$$

Es ist klar, daß das nur richtig sein kann, wenn das Skalarprodukt $\langle \psi_1, \psi_2 \rangle$ entweder 0 oder 1 ist. Somit kann es kein von ψ unabhängiges U geben, das ψ in $\psi \otimes \psi$ überführt.

Mit dieser Art des Schließens sehen wir leicht, daß
eine Menge reiner Zustände genau dann exakt kopiert werden kann, wenn sie paarweise orthogonal sind.
Um ein Orthonormalsystem zu kopieren, muß allerdings seine Lage im Hilbertraum bekannt sein, z.B. als die nicht–entarteten Eigenvektoren einer gegebenen Observablen. Übrigens weist auch dieser Gesichtpunkt auf die Bedeutung von Referenzbasen für das Funktionieren von Quantenrechnern hin. Wir wollen daran erinnern, daß die Wahl der Referenzbasen in den Faktoren des Tensorprodukts willkürlich, also nur bis auf eine durch Konvention zu wählende unitäre Transformation bestimmt ist. Mit dem obigen Argument (und den dort verwendeten Bezeichnungen) ist aber auch die folgende unitäre Transformation ausgeschlossen:
$\chi \otimes \psi \otimes \varphi \longrightarrow \chi' \otimes \psi \otimes W\psi$ für alle ψ mit einer "universellen" (d.h. ψ–unabhängigen)

unitären Transformation W. Damit gibt es auch keinen Vorgang, der so klont,daß die "Kopie" im "Kopie–Hilbertraum" $\mathcal{H}'$ exakt diesselbe Basiszerlegung hat, wie das Original im "Original–Hilbertraum" $\mathcal{H}$. Ein Kopieren "relativ zur Basis" ist nicht möglich.

Das Problem des exakten Kopierens verrauschter (d. h. gemischter) Zustände ist wesentlich komplizierter. Es wurde von H. Barnum, C. Caves, C. Fuchs, R. Josza und B. Schumacher [3] gelöst. Ihre Resultate lassen sich folgendermaßen formulieren:

Sei $\mathcal{H}$ der endlich–dimensionale Hilbertraum, auf dem die zu kopierenden Zustände als normierte Dichteoperatoren ω^1 und ω^2 gegeben seien. Als Kopiermechanismus wird eine Abbildung κ

$$\kappa(D) = \sum A_j D\, A_j^*, \quad \sum A_j^* A_j = \mathbf{1}_{\mathcal{H}}$$

von $\mathcal{B}(\mathcal{H})$ in $\mathcal{B}(\mathcal{H} \otimes \mathcal{H})$ angenommen. Dabei sind die A_k Abbildungen von $\mathcal{H}$ in $\mathcal{H} \otimes \mathcal{H}$. A_k^* bezeichnet die zu A_k hermitisch konjugierte Abbildung, die $\mathcal{H} \otimes \mathcal{H}$ in $\mathcal{H}$ abbildet. Diese *vollständig positiven stochastischen Abbildungen* gelten als die allgemeinsten quantenphysikalisch erlaubten ("ausführbaren") linearen Operationen (vgl. [84, 54]). Es sei nun

$$\kappa(\omega^1) = \tilde{\omega}^1, \quad \kappa(\omega^2) = \tilde{\omega}^2.$$

Die Bedingung für exaktes Kopieren (Klonen) entspricht der für reine Zustände:

$$\{\, \tilde{\omega}^i = \omega^i \otimes \omega^i,\ i = 1, 2 \,\} \implies \omega^1 \omega^2 = 0.$$

Nach [3] kann die Forderung nach Klonung durch die nach "Weiterverbreitung" (broadcasting) ersetzt werden, eine schwächere Form des exakten Kopierens. Beim Weiterverbreiten der Quantennachricht wird nur gefordert, daß die Reduktion von $\tilde{\omega}^i$ gemäß (22) auf jeden der beiden Faktoren in $\mathcal{H} \otimes \mathcal{H}$ gleich ω^i ist ($i = 1, 2$). Also wird

$$\mathrm{Tr}_{\mathcal{H}} \omega^i X = \mathrm{Tr}_{\mathcal{H}\otimes\mathcal{H}} \tilde{\omega}^i (X \otimes \mathbf{1}), \quad \forall\, X \in \mathcal{B}$$

und das Analoge für den zweiten Faktor verlangt. Unter den genannten Voraussetzungen führen diese Forderungen zur *Vertauschbarkeit der beiden Dichteoperatoren*: Es muß $\omega^1 \omega^2 = \omega^2 \omega^1$ sein. Ist umgekehrt die Vertauschbarkeit gegeben, so gibt es ein κ, das die Weiterverbreitung garantiert.

3.4 Quantenkopierer

Wenn es auch kein exaktes Kopieren ("Klonen") gibt, so kann man doch nach *optimalen Kopierern* fragen, die mit einer möglichst kleinen Ungenauigkeit arbeiten. Die Antwort hängt von Eigenschaften ab, die beim Kopieren optimiert werden sollen. Als ein typisches Beispiel wollen wir die von Bužek und Hillery [20] gefundene "universal quantum copying machine" (UQCM) vorstellen, die ein beliebiges q-Bit

in zwei gleich stark verrauschte q-Bits wandelt. Essentiell ist für diesen Kopierer eine unitäre Abbildung

$$V \; : \quad \mathcal{H} \mapsto \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}, \quad \dim \mathcal{H} = 2, \tag{23}$$

des 2-dimensionalen q-Bit–Raumes in den 8-dimensionalen Bildraum. Letzter besteht aus zwei Replika des ersteren und einem Hilfsraum, der den Kopierer symbolisiert[27], in diesem Fall aber ebenfalls durch den q-Bit–Hilbertraum $\mathcal{H}$ gegeben ist. Als Kopien gelten die Reduktionen des Bildvektors auf die ersten beiden Faktoren in (23).

Die UQCM entsteht dadurch, daß man V so wählt, daß die beiden identischen Kopien so wenig wie möglich verrauscht sind und der "Grad der Verrauschung"auch noch unabhängig vom input-Zustand, dem Original, ist. Dieses optimale und universelle Kopieren bedeutet: die Übergangswahrscheinlichkeit[28] zwischen Kopie und Original soll maximal und unabhängig vom Original sein.

Nach Wahl von Referenzbasen können wir die von Bužek und Hillery gefundene Abbildung durch ihre Wirkung auf eine Basis des *in*- Hilbertraumes kennzeichnen:

$$\phi = a|0\rangle + b|1\rangle, \quad V\phi = \psi = a\psi_0 + b\psi_1 \quad \text{und} \quad a\bar{a} + b\bar{b} = 1 \tag{24}$$

$$\begin{aligned} \psi_0 &= \sqrt{\frac{2}{3}}|000\rangle + \sqrt{\frac{1}{6}}(|101\rangle + |011\rangle) \\ \psi_1 &= \sqrt{\frac{2}{3}}|111\rangle + \sqrt{\frac{1}{6}}(|010\rangle + |100\rangle). \end{aligned} \tag{25}$$

Zuerst werde die partielle Spur über den dritten Faktor ausgeführt, und dann jeweils nach einem der anderen beiden. Dazu zerlegen wir ψ gemäß

$$\psi = \varphi_{**0} \otimes |0\rangle + \varphi_{**1} \otimes |1\rangle \tag{26}$$

$$\begin{aligned} \varphi_{**0} &= a\sqrt{\frac{2}{3}}|00\rangle + b\sqrt{\frac{1}{6}}(|01\rangle + |10\rangle) \\ \varphi_{**1} &= b\sqrt{\frac{2}{3}}|11\rangle + a\sqrt{\frac{1}{6}}(|10\rangle + |01\rangle). \end{aligned} \tag{27}$$

[27] In [20] ist diese Abbildung in einen unitären Operator des 8-dimensionalen Hilbertraums so eingebettet, daß die von Dieks, Wooters und Zurek benutzte Terminologie zur Anwendung kommen kann.

[28] Die Übergangswahrscheinlichkeit zwischen beliebigen — nicht notwendig reinen — Quantenzuständen wurde in [83] definiert. In einem Teil der jüngeren Literatur wird sie auch als "fidelity" bezeichnet.

Diese Vektoren stehen senkrecht aufeinander. Daher entsteht durch Reduktion nach dem letzten Faktor der Dichteoperator

$$\varrho^{12} = |\varphi_{**0}\rangle\langle\varphi_{**0}| + |\varphi_{**1}\rangle\langle\varphi_{**1}|. \tag{28}$$

Um einen expliziteren Ausdruck zu erhalten, gehen wir zur Matrixschreibweise über. Dabei nehmen wir, wie im ersten Kapitel beschrieben, die Indices in lexikographischer Reihenfolge an. Zunächst ergibt sich für die beiden reinen Zustände (27)

$$|\varphi_{**0}\rangle\langle\varphi_{**0}| = \begin{pmatrix} \frac{2}{3}a\bar{a} & \frac{1}{3}a\bar{b} & \frac{1}{3}a\bar{b} & 0 \\ \frac{1}{3}b\bar{a} & \frac{1}{6}b\bar{b} & \frac{1}{6}b\bar{b} & 0 \\ \frac{1}{3}b\bar{a} & \frac{1}{6}b\bar{b} & \frac{1}{6}b\bar{b} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{29}$$

$$|\varphi_{**1}\rangle\langle\varphi_{**1}| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{6}a\bar{a} & \frac{1}{6}a\bar{a} & \frac{1}{3}a\bar{b} \\ 0 & \frac{1}{6}a\bar{a} & \frac{1}{6}a\bar{a} & \frac{1}{3}a\bar{b} \\ 0 & \frac{1}{3}b\bar{a} & \frac{1}{3}b\bar{a} & \frac{2}{3}b\bar{b} \end{pmatrix}. \tag{30}$$

Addieren wir beide Matrizen, so entsteht nach (28)

$$\varrho^{12} = \begin{pmatrix} \frac{2}{3}a\bar{a} & \frac{1}{3}a\bar{b} & \frac{1}{3}a\bar{b} & 0 \\ \frac{1}{3}b\bar{a} & \frac{1}{6} & \frac{1}{6} & \frac{1}{3}a\bar{b} \\ \frac{1}{3}b\bar{a} & \frac{1}{6} & \frac{1}{6} & \frac{1}{3}a\bar{b} \\ 0 & \frac{1}{3}b\bar{a} & \frac{1}{3}b\bar{a} & \frac{2}{3}b\bar{b} \end{pmatrix}. \tag{31}$$

Die partielle Spur über den zweiten Faktor, $\varrho^1 = \mathrm{Tr}_2\varrho^{12}$, ist die Summe der Diagonalblöcke, falls die Matrix (31) als 2×2–Blockmatrix aufgefaßt wird. Daher ist

$$\varrho^1 = \begin{pmatrix} \frac{2}{3}a\bar{a} & \frac{1}{3}a\bar{b} \\ \frac{1}{3}b\bar{a} & \frac{1}{6} \end{pmatrix} + \begin{pmatrix} \frac{1}{6} & \frac{1}{3}a\bar{b} \\ \frac{1}{3}b\bar{a} & \frac{2}{3}b\bar{b} \end{pmatrix} \tag{32}$$

und somit

$$\varrho^1 = \frac{2}{3}\begin{pmatrix} a\bar{a} & a\bar{b} \\ b\bar{a} & b\bar{b} \end{pmatrix} + \frac{1}{6}\mathbf{1}. \tag{33}$$

Die gleiche Darstellung besitzt auch ϱ^2, die partielle Spur $\mathrm{Tr}_1\varrho^{12}$. Sie entsteht aus der Blockmatrix (31), wenn die vier 2×2 Blöcke durch ihre Spuren ersetzt werden. Insbesondere ist $\varrho^1 = \varrho^2$ bei der korrekten Identifizierung der jeweiligen Referenzbasen.

Nach (33) sind die Kopien verrauschte q-Bits.

Wir berechnen noch die Übergangswahrscheinlichkeit zwischen Original und Kopie (vgl. [83]). In unserem Fall ist das Original der eindimensionale Projektor

$$|\phi\rangle\langle\phi| = \begin{pmatrix} a\bar{a} & a\bar{b} \\ b\bar{a} & b\bar{b} \end{pmatrix}.$$

Daher ist die Übergangswahrscheinlichkeit zwischen Kopie und Original gerade durch den Erwartungswert von ϱ^1 bzw. ϱ^2 im Zustand $|\phi\rangle\langle\phi|$ gegeben:

$$\langle\phi, \varrho^1\,\phi\rangle = \mathrm{Tr}\begin{pmatrix} a\bar{a} & a\bar{b} \\ b\bar{a} & b\bar{b}\end{pmatrix}[\frac{2}{3}\begin{pmatrix} a\bar{a} & a\bar{b} \\ b\bar{a} & b\bar{b}\end{pmatrix} + \frac{1}{6}\,\mathbf{1}] = \frac{5}{6}.$$

Die Verrauschung ist tatsächlich vom Ausgangszustand unabhängig, und sie ist sogar optimal,d.h. sie kann, wenn man die Universalität beibehalten möchte, auch nicht weiter verringert werden (siehe z.B. [18]). Bis auf unitäre Äquivalenz wird V durch diese Anforderung eindeutig bestimmt.

Das Problem des approximativen Kopierens gab Anlaß zu einer ganzen Reihe von Arbeiten, die die obige Untersuchung in verschiedene Richtungen weiterverfolgten, und ist auch weiterhin in der Diskussion (siehe dazu z.B. [18, 37, 88, 92, 21, 60]).

Bemerkung:

Eine Verallgemeinerung der UQCM, die von Werner [88] stammt, sei noch angegeben. Es geht dabei um das Kopieren von N Exemplaren eines reinen Zustandes, gegeben durch einen Einheitsvektor φ in einem beliebigen endlich–dimensionalen Hilbertraum $\mathcal{H}$, auf M $(N < M)$ identische Zustände (im Sinne des Weiterverbreitens):

$$\psi = \varphi \otimes \varphi \otimes \cdots \otimes \varphi \in \mathcal{H}^{\otimes N} \mapsto \mathcal{H}^{\otimes M}. \qquad (W1)$$

Wegen der Symmetrie der in–Zustände ist es ausreichend, die definierende Abbildung auf den bosonischen Sektor zu beschränken. Dessen Dichteoperatoren werden in den Zielraum mit einer Abbildung T_0 eingebettet:

$$T_0 \;:\quad |\psi\rangle\langle\psi| \mapsto |\psi\rangle\langle\psi| \otimes \mathbf{1}_{M-N}. \qquad (W2)$$

Die Symmetrisierung der erhaltenen Zustände, also die Projektion T_1 auf den bosonischen Sektor des Zielraumes, ist eine vollständig positive, bistochastische Abbildung. (Sie ist das arithmetische Mittel der Permutationen der Faktoren.) Wird die Transformation T_1T_0 auf einen bosonischen Dichteoperator des in–Raumes angewendet, so entsteht ein Dichteoperator mit Träger im bosonischen Sektor des Zielraumes. Die Reduktion auf die Faktoren von $\mathcal{H}^{\otimes M}$ ergibt deshalb gleiche Dichteoperatoren. Für den Nachweis der Optimalität des Verfahrens für die Produktzustände (W1) sei auf die Originalarbeit verwiesen.□

3.5 Quantenkryptographie

Wir wollen abschließend noch andeuten, wie man die besprochenen Besonderheiten quantenmechanischer Systeme dazu nutzen kann, die Übertragung klassischer Information vor unbefugten Personen zu schützen. Auf die Vielfalt dieses Problemkreises[29] wollen wir allerdings nicht näher eingehen. Wir werden uns auf das Problem

[29]Eine Einführung in die (klassische) Kryptologie findet man in [4]; eine Einführung in die Quantenkryptographie wird in [10] geboten. Weitere historische quantenkryptographische Details kann man [17] entnehmen.

des Schlüsselaustausches für eine gewisse Klasse von Chiffrierverfahren beschränken. Nach der Behandlung des Einstein–Podolsky–Rosen–Kanals werden wir eine weiteres Schlüsselaustausch-Protokoll kennenlernen.

Unser Demonstrationsbeispiel besteht darin, daß Alice und Bob eine Nachricht austauschen wollen und dazu ein symmetrisches Chiffrierverfahren, die Vernam–Chiffre (oder "one–time pad"), benutzen. Wir werden annehmen, daß die Nachricht bereits digital als (0,1)–Folge der Länge n vorliegt.
Das Verfahren arbeitet nun folgendermaßen. Alice und Bob haben sich auf eine (0,1)–Zufallsfolge der Länge n, die sie auf sicherem Wege ausgetauscht haben und natürlich geheim halten, geeinigt. Zur Verschlüsselung addiert Alice (oder Bob) diese (0,1)–Zufallsfolge gliedweise (d.h. bitweise) mod 2 zur Nachricht. Die Entschlüsselung wird erreicht, indem Bob (oder Alice) diese (0,1)–Zufallsfolge nochmals zur verschlüsselten Nachricht gliedeweise mod 2 addiert. Die modularen Operationen $x+0+0 = x+0 = x$ und $x+1+1 = x+0 = x$ sichern offenbar, daß man auf diesem Wege die ursprüngliche Nachricht rekonstruieren kann. Dieses Verfahren führt zu einer perfekten Chiffrierung im Sinne von Shannon, weil dadurch der verschlüsselte Text vom ursprünglichen Text unabhängig wird und damit keine Rückschlüsse zuläßt. Durch dieses Verfahren ist man vor ungewollten Lauschern sicher, solange die Zufallsfolge (der Schlüssel) geheim bleibt und auch nur einmal benutzt wird. Sehen wir vom Problem ab, Zufallsfolgen zu erzeugen, so bleibt auf alle Fälle das Problem, daß ein ständiger Nachrichtenaustausch natürlich auch einen ständigen Schlüsselaustausch erforderlich macht.

An dieser Stelle setzen einige quantenkryptographische Verfahren ein. Es existieren mittlerweile verschiedene Protokolle, die den Austausch einer Zufallsfolge zwischen Alice und Bob ermöglichen. Die Abhörsicherheit ist allerdings noch nicht völlig geklärt. Angemerkt werden soll auch noch, daß es bereits einige erfolgreich arbeitende Teststrecken gibt (z.B. [66, 48, 19]).
Wir wollen auf ein vereinfachtes Verfahren, das Protokoll B92 [8] von Bennett, eingehen (siehe auch [48]).
Alice und Bob besitzen (0,1)–Zufallsfolgen, die sie sich unabhängig voneinander beschafft haben. Der Schlüssel wird dadurch erzeugt, daß aus diesen beiden Folgen eine in beiden enthaltene Unterfolge durch "abhörsicheren" Informationsautausch ausgewählt wird. Bevor das Verfahren beginnt, müssen Alice und Bob jedoch — worauf bereits oben hingewiesen wurde — die Referenzbasen in ihren q-Bit–Hilberträumen[30] aufeinander abstimmen ("synchronisieren"). Eine Möglichkeit wäre, daß Alice zwei zueinander orthogonale Polarisationszustände von Photonen als Referenzbasis wählt und daraufhin eine Folge von Photonen, die sich jeweils in einem dieser beiden Zuständen befinden, präpariert und an Bob sendet. Sie teilt ihm außerdem auf herkömmliche Weise ("Telefon") mit, welche Polarisation die gesendeten Photonen haben. Bob justiert daraufhin solange seine Polarisationsfilter, bis er möglichst ex-

[30] Wir werden der Einfachheit halber immer von Photonen und ihren Polarisationszuständen sprechen. Die momentan experimentell realisierten quantenkryptographischen Protokolle arbeiten mit Photonen. Für die Polarisationszustände benutzen wir die Spin-Notation aus dem Abschnitt über die q-Bits.

akt Alice's Mitteilung reproduzieren kann. Schwierig wird es natürlich, wenn das Medium nicht optisch stabil ist. Sie könnten natürlich auch, wenn die Möglichkeit besteht, ein Zusammentreffen zu einer Basisjustierung nutzen und versuchen, bei der räumlichen Trennung die Basen "parallel" zu transportieren.
Nun zum eigentlichen Verfahren:
Alice habe die Referenzbasis $|\uparrow\rangle, |\downarrow\rangle$ in ihrem q-Bit–Hilbertraum gewählt. Sie kodiert nun die Zahlen 0 und 1 in zwei nichtorthogonale Zustände:

0 wird in $\pi_0 = \{$ Projektor auf $|\uparrow\rangle \}$ kodiert;

1 wird in $\pi_1 = \{$ Projektor auf $|\rightarrow\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle + |\downarrow\rangle] \}$ kodiert.

Unter Benutzung dieser Kodierung sendet sie an Bob die Quantenbotschaft (also eine Folge von Polarisationszuständen), die ihrer Zufallsfolge entspricht. Wäre Alice Zufallsfolge : $0, 1, 1, 1, 0 \ldots$, dann würde sie folgende Quantenbotschaft senden: $\pi_0, \pi_1, \pi_1, \pi_1, \pi_0 \ldots$.
Denken wir an den vorangegangenen Abschnitt über den Quantenkopierer, dann verhindert die Wahl eines nichtorthogonalen Quantenalphabets, daß ein Lauscher, mitunter "Eva" genannt, sich eine Kopie der Quantenbotschaft verschaffen kann (in der engl. Fassung ist "Eve" lautmäßig abgeleitet von eavesdropper = jemand, der heimlich ein Gespräch mithört). Um diese Quantenbotschaft zu lesen, stehen Bob zwei Meßgeräte (Polarisationsfilter) zur Verfügung, die die beiden zueinander nichtorthogonalen Polarisationszustände $|\downarrow\rangle$ und $|\leftarrow\rangle = \frac{\mathbf{1}}{\sqrt{2}}[|\uparrow\rangle - |\downarrow\rangle]$ herausfiltern. Mit welchem Meßgerät Bob das jeweils eintreffende Photon (den Quantenbuchstaben) mißt, bestimmt er an Hand seiner Zufallsfolge nach folgendem Schema:

0 fordert Herausfiltern von $|\leftarrow\rangle$

1 fordert Herausfiltern von $|\downarrow\rangle$.

Die Projektoren, die zu diesen Messungen gehören, seien

$$P_0 = \quad \text{Projektor auf} \quad |\leftarrow\rangle$$

und

$$P_1 = \quad \text{Projektor auf} \quad |\downarrow\rangle.$$

Wäre Bob's Zufallsfolge: $1, 0, 1, 0, 0 \ldots$, dann würde er folgende Polarisationsmessungen ausführen: $P_1, P_0, P_1, P_0, P_0 \ldots$.
Nach jeder erfolgreichen Messung, d.h. das Alice'sche Photon hat den Filter passiert, markiert Bob diese Stelle seiner Zufallsfolge. Wie man bemerkt, ist wegen der Orthogonalität der Vektoren $P_0\pi_1 = 0$ und $P_1\pi_0 = 0$. Damit wird gesichert, daß Bob niemals eine 0 in seiner Folge kennzeichnet, wenn an derselben Stelle bei Alice eine 1 steht und umgekehrt. Allerdings wird er damit nicht die beiden gemeinsame maximale Teilfolge kennzeichnen können, da die Übergangswahrscheinlichkeit nur $\frac{1}{2}$ beträgt, wenn er den Quantenbuchstaben π_0 mit dem Filter P_0 oder π_1 mit dem

Filter P_1 mißt : $\mathrm{Tr}\,\pi_0 P_0 = \mathrm{Tr}\,\pi_1 P_1 = \frac{1}{2}$.
Bob wird abschließend Alice über einen herkömmlichen (nicht notwendig geschützten) Kanal informieren, welche Stellen er markiert hat (ohne natürlich den Wert zu nennen). Damit verfügen beide über eine gemeinsame Zufallsfolge, die im Mittel aber nur noch aus 25% der ursprünglichen Folge besteht.

Wir haben bisher natürlich stillschweigend ideale Empfangsbedingungen zwischen Alice und Bob angenommen. Falls das — wie in der Praxis — nicht der Fall ist, hätte man noch diverse klassische und/oder quantenmechanische Fehlerkorrekturverfahren einzusetzen. Auf das wichtige Kapitel fehlerkorrigierender Kodes bei der Quantenkommunikation wollen wir in dieser Einführung allerdings gänzlich verzichten (siehe z.B. [78],[75] oder [67]).
Wie sicher ist das geschilderte Verfahren ? Hingewiesen wurde schon auf den Umstand, daß dem exakten Kopieren der Quantenbotschaft ein Riegel vorgeschoben wurde. Wir können an dieser Stelle nicht näher auf das sehr komplizierte Sicherheitsproblem eingehen, sondern wollen nur anmerken, daß einfache Attacken, bei denen Eva die Quantenbotschaft abfängt und sie erst weiterleitet, nachdem sie Polarisationsmessungen ausgeführt hat, erkennbar sind. Eva's Messungen würden die Quantenbuchstaben π_0 bzw. π_1 in Abhänigkeit von den Messungen ändern. Dadurch wird Bob hin und wieder fehlerhaft markieren. Alice und Bob könnten nun öffentlich einen (zufällig ausgewählten) Teil der vermeintlich gemeinsamen Folge vergleichen und auf diese Weise — unter Berücksichtigung der natürlichen Rauschfehlerrate — eventuell auf eine lauschende Eva schließen.

4 Der Einstein–Podolsky–Rosen–Kanal

4.1 Quantenkanäle

Wir kommen nun zu einem weiteren Grundbegriff der Quanten–Informationstheorie, dem *Quanten–Kanal*. Seine Aufgabe ist es, eine Quantenbotschaft von einem "Sender" zu einem "Empfänger" zu transportieren. Da Quantenbotschaften aus Quantenzuständen bestehen, bildet ein Quantenkanal Zustände des Input–Systems auf solche des Output–Systems ab. Diese Abbildung wird *Kanalabbildung* genannt. Die Quantenbotschaft, die eine Folge von Quantenzuständen ist, wird durch die Kanalabbildung Zustand für Zustand in eine neue Folge von Zuständen umgewandelt.

Um nützlich zu sein, müssen Quantenkanäle oft von klassischem Informationsaustausch (klassische Ein– oder Zweiweg–Kommunikation) begleitet werden.

Im Fall des Quantencomputers werden die eingegebenen Multi–q-Bits durch Folgen der früher beschriebenen Operationen auf neue Multi–q-Bits abgebildet. Die resultierende unitäre Transformation aller Operationen, aber auch jedes einzelne Quantengate, repräsentiert einen Quanten–Kanal. Diese Kanalabbildungen sind unitäre Transformationen.

Ein weiteres Beispiel für einen Quantenkanal ist der obige, mit der von Neumann–Lüders–Regel beschriebene Meßprozeß ("Meß– oder Beobachtungskanal"). Die einlaufende Quantenbotschaft wird auf die Eigenzustände einer Observablen (14) abgebildet. Zu jedem Eigenwert mit Projektor P gehört eine Abbildung $\omega \to P\,\omega\,P$, die zufällig angesteuert wird, wenn ein Zustand mit Dichteoperator ω einläuft.

Schließlich sei als drittes Beispiel der *depolarisierende* Kanal [12] genannt, der im 2–dimensionalen q-Bit–Raum operiert. Er ist durch die Abbildung

$$\omega \quad \longrightarrow \quad \kappa(\omega) = \frac{(1-p)}{2}\mathbf{1} + p\omega$$

mit $0 \leq p \leq 1$ bestimmt. Dieser Kanal "rückt " jeden partiell polarisierten Zustand näher zum völlig unpolarisierten Zustand, der durch die Dichtematrix $\frac{1}{2}\mathbf{1}$ gegeben ist. Setzt man mit Hilfe der Pauli-Matrizen

$$A_1 = \sqrt{p}\mathbf{1}, \quad A_2 = \sqrt{\frac{1}{2}(1-p)}\sigma_1, \quad A_3 = \sqrt{\frac{1}{2}(1-p)}\sigma_2,$$

so überzeugt man sich von der Darstellung

$$\kappa(\omega) = A_1\omega A_1 + A_2\omega A_2 + A_3\omega A_3.$$

des depolarisierenden Kanals.

Der allgemeine Quanten–Kanal soll durch eine Familie von Abbildungen, den Kanalabbildungen, des Input–Quanten–Zustandsraumes in den Output–Quanten–Zustandsraum gegeben sein. Von den Kanalabbildungen wird zunächst gefordert,

daß sie affin, also mit der konvexen Struktur des Zustandsraumes verträglich sind, und die Gewichte in "Gibbsschen Mischungen" nicht verändern. Für die Dichteoperatoren über endlich–dimensionalen Hilberträumen folgt, daß man eine solche Abbildung zu einer linearen[31] Abbildung κ fortsetzen kann, die die Positivität von Operatoren erhält.

Der Begriff "Quanten–Kanal" wird aber in der Regel (nach Holevo [47, 62]) in einem eingeschränkteren Sinn benutzt:

> Die Kanal–Abbildungen sollen sogar vollständig positiv sein.

Das ist eine sinnvolle quantenmechanische Zusatzforderung [84], die bei den obigen Beispielen gegeben ist. Wir können sie wie folgt formulieren: Bildet κ die Operatoren[32] von $\mathcal{H}_1$ in die von $\mathcal{H}_2$ ab und sind $\phi_1^{(1)}, \phi_2^{(1)}, \ldots$ beziehungsweise $\phi_1^{(2)}, \phi_2^{(2)}, \ldots$ Vektoren aus diesen Hilberträumen, so gelte

$$\sum_{jk} \langle \phi_j^{(2)},\, \kappa(\, |\phi_j^{(1)}\rangle\langle\phi_k^{(1)}|\,)\, \phi_k^{(2)}\rangle \;\geq\; 0. \tag{vp1}$$

Um diese Bedingung formulieren zu können, mußte die ursprünglich nur für die Abbildung von Dichteoperatoren gedachte Kanalabbildung zu einer Abbildung erweitert werden, die auf allen Operatoren der Form $|\phi\rangle\langle\phi'|$ definiert ist. Ist diese Erweiterung, wie oben angenommen, linear (bzgl. der komplexen Zahlen) und gilt (vp1), so heißt κ *vollständig positiv*.

Ist dann $\mathcal{H}$ ein weiterer Hilbertraum und $\mathbf{1}$ sein Einsoperator, so ist $\kappa \otimes \mathbf{1}$ eine vollständig positive Abbildung, die die Dichteoperatoren von $\mathcal{H}_1 \otimes \mathcal{H}$ in solche über $\mathcal{H}_2 \otimes \mathcal{H}$ überführt. Etwas allgemeiner gesagt: Das direkte Produkt vollständig positiver Abbildungen ist wieder vollständig positiv. Hierin liegt die quantenphysikalische Bedeutung der vollständigen Positivität. Jede zulässige Abbildung zwischen den Operatoren oder den Zuständen von Teilsystemen $\mathcal{H}_i$ muß Einschränkung von Abbildungen zwischen beliebigen größeren Systemen $\mathcal{H}_i \otimes \mathcal{H}$ sein.

Seien $A_1, A_2, \ldots$ lineare Abbildungen von $\mathcal{H}_1$ in $\mathcal{H}_2$. Die zu A_j hermitisch konjugierte Abbildung von $\mathcal{H}_2$ in $\mathcal{H}_1$ werde wie üblich mit A_j^* bezeichnet. Dann ist

$$\kappa(D) = \sum A_j D\, A_j^*,\; D \in \mathcal{B}_1 \tag{vp2}$$

eine vollständig positive Abbildung. Umgekehrt gilt: im Endlichdimensionalen läßt sich jede vollständig positive Abbildung (auf vielerlei Weise) in der Form (vp2) schreiben.

[31] oder zu einer antilinearen

[32] Operatoren der Spurenklasse, falls die Hilberträume unendlich-dimensional sind.

Was aber geschieht, wenn sich die Kanalabbildung *antilinear* zu einer Abbildung κ fortsetzen läßt, die die Ungleichungen (vp1) erfüllt? Mit Hilfe eines antiunitären Operators J (z. B. von $\mathcal{H}_2$) können wir an Stelle von κ die Abbildung $D \to J\kappa(D)J^*$ betrachten, die offenbar linear ist und weiterhin (vp1) erfüllt. Hieraus sehen wir, daß für κ Darstellungen (vp2) gelten, bei denen die Abbildungen A_j antilinear sind. Wir nennen eine antilineare Abbildung, die (vp1) erfüllt, vollständig **ko–positiv*. (Woronowicz hat die Bezeichnung "ko–positiv" für Abbildungen benutzt, die linear und bis auf das Transponieren einer Matrix vollständig positiv sind. Für Hermitesche Operatoren, insbesondere Dichteoperatoren, bewirkt Transponieren eine komplexe Konjugation.)

Eine antilineare Abbildung kann nicht mit einer linearen Abbildung tensoriert werden: "Die imaginäre Einheit weiß dann nicht, mit welchem Vorzeichen sie auftreten soll." Das direkte Produkt zweier antilinearer Abbildungen ist jedoch korrekt definiert. Man findet dann ganz analog, daß die vollständige *Ko–Positivität bei der Bildung von direkten Produkten nicht verloren geht.

Aus physikalischer Sicht sind die vielleicht wichtigsten antilinearen Operationen die Zeitumkehr und ihre Kombination mit Parität und Teilchen–Antiteilchen– Austausch (die CPT–Operation). Sei T die Zeitumkehr in $\mathcal{H}$ und setzen wir für einen Moment $\kappa_T(D) = TDT^{-1}$. Eine vollständig *ko–positive Abbildung κ von $\mathcal{H}_1$ nach $\mathcal{H}_2$ kann dann als $\kappa \otimes \kappa_T$ fortgesetzt werden, analog wie oben bei den linearen vollständig positiven Abbildungen besprochen. Insbesondere verbieten die Axiome der Quantenphysik eine lediglich lokale Zeitumkehr, erlauben aber die globale Zeitumkehr.

Sehen wir uns noch, um etwas konkreter zu werden, die fermionische Zeitumkehr für den 2–dimensionalen q-Bit–Raum an:

$$T(a|0\rangle + b|1\rangle) = i(\bar{b}|0\rangle - \bar{a}|1\rangle),$$

für die $T^* = T^{-1} = -T$ gilt. (Der Faktor i ist lediglich konventionelle Phasenfestlegung.) Die wohl einfachste vollständig *ko–positive Kanalabbildung ist daher

$$\kappa_T(z_0\mathbf{1} + z_1\sigma_1 + z_2\sigma_2 + z_3\sigma_3) = \bar{z}_0\mathbf{1} - \bar{z}_1\sigma_1 - \bar{z}_2\sigma_2 - \bar{z}_3\sigma_3.$$

Ist ω ein normierter Dichteoperator, so ist $\kappa_T(\omega) = \mathbf{1} - \omega$.

4.2 Der EPR–Kanal

Als wichtiges und lehrreiches Beispiel für einen Quantenkanal betrachten wir nun den *EPR–Kanal* (EPR nach **E**instein, **P**odolsky und **R**osen[29]).

Die Ausgangssituation wird durch zwei Quantensysteme gegeben, die durch die Hilbert–Räume $\mathcal{H}_1$ und $\mathcal{H}_2$ beschrieben werden und die durch einen auf dem Produktraum

$$\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2 \tag{34}$$

gegebenen Zustand ω_{12} untereinander korreliert oder "verschränkt"[33] sind. Wir bezeichnen die Algebren der beschränkten Operatoren mit

$$\mathcal{B}_j = \mathcal{B}(\mathcal{H}_j), \quad \mathcal{B}_{12} = \mathcal{B}_1 \otimes \mathcal{B}_2 = \mathcal{B}(\mathcal{H}_{12}). \tag{35}$$

Auch hier werden wir Quantenoperationen, Präparation oder Anwendung unitärer Operationen, die in einem der beiden Systeme durchgeführt werden können, als *lokale Operationen* bezeichnen.

Bemerkung:

Dieser Lokalitätsbegriff ist *allgemeiner* als der in der Relativitätstheorie und der relativistischen Quantenphysik benutzte. Die beiden Systeme können raumartig getrennt sein, müssen es aber nicht. (Man denke an die Verschränkung des Elektron–Spins mit dem Proton–Spin im H–Atom.) Der offenbar unwiderstehliche Reiz, eine räumliche Trennung beider Systeme anzunehmen, veranlaßt gelegentlich Autoren zu einer (oft stillschweigenden) Gleichsetzung. Das ist aber nicht sachgemäß. □

Ähnlich wie im Abschnitt "Quantenbotschaften" werden lokale Operationen oft "personifiziert" : Eine Person namens "Alice" ist im Besitz des Systems $\mathcal{H}_1$, eine zweite mit Namen "Bob" besitzt das System $\mathcal{H}_2$. Alice versucht, Bob etwas mitzuteilen, und benützt dazu, wenigstens in diesem Abschnitt, einen EPR– und einen klassischen Kanal.

Der Kanal wird in Gang gesetzt durch eine Messung im ersten System, einer lokalen Operation von Alice. Wir wissen aber, daß jede Messung in einem System als Messung in jedem größeren angesehen werden kann. Es wird also nicht nur im ersten, sondern auch im Gesamtsystem ein neuer Zustand präpariert. Das aber heißt, auch in Bob's Teilsystem wird der Zustand verändert. Alice teilt das Resultat ihrer Messung Bob über einen "klassischen" Informationskanal[34] mit. Mit dieser Kenntnis kann die Zustandsänderung im zweiten System ganz oder teilweise ermittelt werden.

Sei also ω_{12} ein Zustand über $\mathcal{B}_{12}$. Wir haben dann in den beiden Teilsystemen die reduzierten Zustände

$$\omega_1(B) = \omega_{12}(B \otimes \mathbf{1}), \quad \forall\, B \in \mathcal{B}_1 \tag{36}$$

$$\omega_2(B) = \omega_{12}(\mathbf{1} \otimes B), \quad \forall\, B \in \mathcal{B}_2. \tag{37}$$

Wird nun im ersten System eine Messung der Observablen A durchgeführt, so wird ein bestimmter, durch einen Meßwert λ identifizierbarer Zustand hergestellt (präpariert). Sei nun P der Projektor, der zum Meßwert λ von A gehört. Dann wissen wir bereits, daß Alice nach der Lüders–Regel (21) den Zustand

$$\omega_1'(B) = \omega_1(P)^{-1}\omega_1(PBP), B \in \mathcal{B}_1$$

[33] Der Begriff "Verschränkung" (engl. entanglement [71]) wurde im Gefolge der Arbeit von Einstein, Podolsky und Rosen von Schrödinger [70] eingeführt.

[34] Letzterer unterliegt, falls Alice und Bob räumlich getrennt agieren, der Einsteinschen Kausalitätsforderung.

erhält.

Vom Gesamtsystem aus betrachtet haben wir aber eine Messung mit $A \otimes \mathbf{1}$ durchgeführt. Hier zeigt der Meßwert auf den Projektionsoperator $P \otimes \mathbf{1}$. Durch die Messung wird also auch über $\mathcal{B}_{12}$ ein neuer Zustand präpariert:

$$\omega_{12} \longrightarrow \omega'_{12}, \quad \omega'_{12}(C) := \omega_1(P)^{-1}\omega_{12}((P \otimes \mathbf{1})C(P \otimes \mathbf{1})) \tag{38}$$

mit $C \in \mathcal{B}_{12}$.

Welcher Zustand liegt nun in Bob's System vor ? Um den reduzierten Zustand zu ermitteln haben wir C zu beschränken auf Operatoren der Gestalt $1 \otimes B$. Also ist

$$\begin{aligned} \omega_2 \longrightarrow \omega'_2, \quad \omega'_2(B) &:= \omega_1(P)^{-1}\omega_{12}((P \otimes \mathbf{1})(\mathbf{1} \otimes B(P \otimes \mathbf{1})) \\ &= \omega_1(P)^{-1}\omega_{12}(P \otimes B), \end{aligned} \tag{39}$$

was i.a. verschieden von (37) ist und somit zu einer Zustandsänderung führt.

Angenommen, Bob kennt den ursprünglichen Zustand ϱ_{12} des Gesamtsystems. Wenn er dann von Alice (z. B. telefonisch) benachrichtigt wird, sie habe λ gemessen, so kann Bob erkennen, in welchem Zustand sich sein System befindet. (Genau genommen setzt Alice einen neuen Anfangszustand für die zeitliche Entwicklung in allen beteiligten Systemen. Zeitverzögerungen durch den klassischen Kanal muß Bob gesondert berücksichtigten.)

Wir wollen unsere bisherigen Kenntnisse nutzen, um nach denjenigen Zuständen zu fragen, bei denen der EPR–Kanal trivial wird, bei denen also *keine* Messung von Alice eine Veränderung im Bobschen System nach sich zieht. In diesem Fall würde der EPR–Kanal zum Informationsaustausch nutzlos sein. Beide Systeme wären vollkommen unkorreliert.

Damit dies eintritt, muß offenbar nach (37) und (39) gelten, daß

$$\omega_1(P)\,\omega_2(B) = \omega_{12}(P \otimes B)$$

für alle $B \in \mathcal{B}_2$ und alle Projektoren $P \in \mathcal{B}_1$ ist. Da die Zustände lineare Funktionale sind und jeder Operator des ersten Systems als komplexe Linearkombination von Projektoren geschrieben werden kann, folgt

$$\omega_1(A)\,\omega_2(B) = \omega_{12}(A \otimes B)$$

für alle $A \in \mathcal{B}_1$ und $B \in \mathcal{B}_2$. Das Resultat lautet somit:

Genau dann kann keine Messung im ersten System einen Zustand im zweiten System verändern, wenn ω_{12} ein Produktzustand $\omega_1 \otimes \omega_2$ ist. Solche Zustände korrelieren die beiden Teilsysteme nicht.

Allerdings gibt es auch hier quantenphysikalische Besonderheiten: Alice kann nicht erkennen, ob eine Messung in ihrem System den Bobschen Zustand verändert, selbst

wenn sie ω_1 kennt. Zu dieser Regel gibt es aber eine Ausnahme: Ist der Zustand ω_1 rein, so ist ω_{12} notwendigerweise ein Produktzustand.

Besitzt also Alice einen reinen Zustand, so kann sie auf keine lokale Weise Bobs Zustand verändern. Aber auch umgekehrt! Sie weiß, daß eine lokale Operation im Bobschen System auch ihren Zustand nicht ändern kann.

Die Korrelationen in einem aus zwei (oder auch mehreren) Teilsystemen bestehenden Gesamtsystem sind schwierig zu klassifizieren. Das Problem besteht darin, den Anteil, der erst durch das Überlagerungsprinzip möglich wird, von dem in der Klassischen Physik und der Wahrscheinlichkeitstheorie bekannten zu trennen oder abzugrenzen. So sagt man, ω_{12} sei *unverschränkt*, wenn eine Darstellung

$$\omega_{12} = \sum r_j \omega_1^j \otimes \omega_2^j, \quad r_j > 0, \tag{40}$$

mit Zuständen ω_k^j der beiden Untersysteme ($k = 1, 2$) existiert. Ist ϱ_{12} unverschränkt, aber kein Produktzustand, so spricht man gelegentlich auch von *klassischer Korrelation*. Konsequenterweise heißt ein Zustand *verschränkt*, wenn er keine Darstellung (40) besitzt.

Bis auf wenige Ausnahmen ist es schwierig, einem Zustand anzusehen ob er verschränkt ist oder nicht. Für höhere Dimensionen steht kein handhabbarer Algorithmus zur Entscheidung dieser Frage zur Verfügung. Eine sehr wichtige Ausnahme bilden wiederum die reinen Zustände. Sie stellen niemals klassische Korrelationen her: Ist ω_{12} ein reiner Zustand, so ist er entweder ein Produktzustand, daher unkorreliert, oder er ist verschränkt. Dieser Umstand bedingt eine besonders wichtige und gut zu behandelnde Klasse von EPR–Kanälen, der wir uns jetzt zuwenden.

4.3 Der EPR-Kanal mit Vektorzuständen

Nehmen wir also an, daß

$$\omega_{12}(C) = \langle \psi, C\psi \rangle, \quad \psi \in \mathcal{H}_{12}, \quad \langle \psi, \psi \rangle = 1. \tag{41}$$

Der Dichteoperator von ω_{12} ist daher $|\psi\rangle\langle\psi|$. Die Dichteoperatoren der reduzierten Zustände, (36) und (37), seien ω_1 und ω_2.

ψ besitzt eine (nicht eindeutige) Darstellung

$$\psi = \sum \sqrt{p_j}\, \phi_j^1 \otimes \phi_j^2, \tag{42}$$

wobei die ϕ_j^1 bzw. die ϕ_j^2 Orthonormalsysteme sind, die aus Eigenvektoren von ω_1 bzw. ω_2 bestehen. $p_1, p_2, \ldots$ sind die zu diesen Eigenvektoren gehörenden gemeinsamen Eigenwerte der reduzierten Dichteoperatoren ω_1 und ω_2. Die Darstellung (42) wird *Gram–Schmidt–Darstellung*, oft auch nur *Schmidt–Darstellung*, von ψ genannt.

Wir erhalten

$$\omega_{12}(B_1 \otimes B_2) = \sum \sqrt{p_i p_j}\langle \phi_i^1, B_1 \phi_j^1\rangle \langle \phi_i^2, B_2 \phi_j^2\rangle. \tag{43}$$

Wird nun bei einer Messung von Alice angezeigt, daß der Projektor

$$P = |\phi\rangle\langle\phi|, \quad P \in \mathcal{B}_1$$

zur Präparation benutzt werden muß, so erhalten wir nach (16) den neuen, noch nicht normierten Zustandsvektor des Gesamtsystems durch

$$(|\phi\rangle\langle\phi| \otimes \mathbf{1})\,\psi = \sum \sqrt{p_j}\langle \phi, \phi_j^1\rangle \phi \otimes \phi_j^2 \tag{44}$$

Wir definieren eine Abbildung s^{21} von $\mathcal{H}_1$ nach $\mathcal{H}_2$,

$$s^{21}\phi := \sum \sqrt{p_j}\langle \phi, \phi_j^1\rangle \phi_j^2, \quad \phi \in \mathcal{H}_1. \tag{45}$$

Damit erhalten wir

$$(|\phi\rangle\langle\phi| \otimes \mathbf{1})\,\psi = \phi \otimes s^{21}\phi. \tag{46}$$

Wie wir sehen, wird wegen (46) die Abbildung s^{21} eindeutig durch den Zustandsvektor ψ bestimmt. Es kann zu ihrer Konstruktion eine beliebige Gram – Schmidt – Entwicklung (42) von ψ verwendet werden.

Die EPR–Kanalabbildung ist somit folgendermaßen bestimmt: Ergibt eine Messung im ersten System den Zustandsvektor ϕ, so entsteht im zweiten System der (normierte) Zustandsvektor

$$w^{-1}s^{21}\phi, \quad w = \langle s^{21}\phi, s^{21}\phi\rangle^{\frac{1}{2}} = \langle \phi, \omega_1 \phi\rangle^{\frac{1}{2}}. \tag{47}$$

w ist die Wahrscheinlichkeit für das Eintreffen dieses Ereignisses.

Die Kanalabbildung wird durch ihre Wirkung auf die zu Alice gehörenden reinen Zustände bestimmt und ergibt

$$\kappa_\psi(|\phi\rangle\langle\phi|) = s^{21}(|\phi\rangle\langle\phi|)s^{12}, \quad s^{12} = (s^{21})^* \tag{48}$$

Nach der Definition (45) ist s^{21} offensichtlich antilinear. Bei κ_ψ handelt es sich somit um eine vollständig *ko-positive Kanalabbildung.

Durch Rückgriff auf (46) können diese Erörterungen noch wie folgt etwas abgerundet werden:
Ist ψ irgendwie als Summe von Produktvektoren dargestellt

$$\psi = \sum \tilde{\phi}_j^1 \otimes \tilde{\phi}_j^2, \tag{49}$$

so entsteht durch

$$s^{21}\phi = \sum \langle \phi, \tilde{\phi}_j^1\rangle \tilde{\phi}_j^2, \quad \phi \in \mathcal{H}_1, \tag{50}$$

trotzdem immer wieder diesselbe Abbildung. Ihre hermitisch Adjungierte s^{12} ergibt sich hieraus unmittelbar zu

$$s^{12}\phi' = \sum \langle \phi', \tilde{\phi}_j^2 \rangle \tilde{\phi}_j^1, \quad \phi' \in \mathcal{H}_2. \tag{51}$$

Bemerkung:

Im Endlichdimensionalen kann man durch geeignet Wahl von ψ jede antilineare Abbildung von $\mathcal{H}_1$ in $\mathcal{H}_2$ als s^{21} realisieren.

Für beliebige, nicht notwendigerweise endlich-dimensionale Hilberträume wird durch diese Zuordnung die Isomorphie von $\mathcal{H}_{12}$ mit dem linearen Raum der antilinearen Hilbert-Schmidt Abbildungen von $\mathcal{H}_1$ in $\mathcal{H}_2$ konstruiert. Die v.Neumannsch–Lüdersche Regel für die Präparation von Zuständen erlaubt die physikalische Realisierung dieser Isomorphie – ein bemerkenswerter Aspekt der mit reinen Zuständen arbeitenden EPR-Kanäle.

Sinngemäße Aussagen kann man auch für EPR-Kanäle treffen, die von einem beliebigen Dichteoperator über $\mathcal{H}_{12}$ beherrscht werden. □

4.4 Schrödingers Beispiele

Wie wir schon wissen, sollte der Zustandsvektor ψ *kein* Produktvektor sein, damit der EPR-Kanal arbeiten kann. Für einen Produktvektor wäre nämlich, geeignet numeriert, $p_1 = 1$ und ansonsten $p_j = 0$. Durch die Messsung erhielten wir also stets den Zustand $|\phi_2^1\rangle\langle\phi_2^1|$ im zweiten System zurück.

Ist ψ kein Produktvektor, so ist er verschränkt, und es entsteht eine nicht-klassische Korrelation zwischen beiden Systemen. ψ heißt *vollständig* verschränkt, wenn der Rang von ω_1 maximal, d. h. gleich der Dimension von $\mathcal{H}_1$ ist. Dann zieht *jede* Messung im ersten System eine Zustandsänderung im zweiten Teilsystem nach sich.

Um diese Verschränkung noch etwas zu erläutern, wollen wir in Anlehnung an Schrödinger [71] zwei Fälle genauer betrachten. Wir werden, um die Diskussion etwas zu vereinfachen, voraussetzen, daß die Hilberträume $\mathcal{H}_1, \mathcal{H}_2$ die gleiche endliche Dimension n haben .

Fall 1:

Die Eigenwerte $p_1, p_2, \ldots$ der zu $|\psi\rangle\langle\psi|$ gehörenden reduzierten Dichtematrizen ω_1, ω_2 in $\mathcal{H}_1$ bzw. $\mathcal{H}_2$ sind alle voneinander und von Null verschieden.

Dann ist die Gram-Schmidtsche Entwicklung (42) von ψ bis auf Phasenfaktoren eindeutig bestimmt. Wir betrachten jetzt die beiden maximal kommutativen Algebren $\mathcal{C}_1$ und $\mathcal{C}_2$ die von denjenigen Observablen erzeugt werden, deren Eigenbasis gerade durch die Orthonormalsysteme (ϕ_j^1) bzw. (ϕ_j^2) gegeben sind. Wählen wir jetzt Observable $A_1 \in \mathcal{C}_1$ und $A_2 \in \mathcal{C}_2$ mit den nicht entarteten Eigenwerten (λ_j^1) bzw. (λ_j^2), dann erhalten wir eine strenge Korrelation der Meßresultate: λ_j^1 zieht stets

λ_j^2 nach sich und umgekehrt. Die EPR-Abbildung s^{21} bildet ϕ_j^1 auf ϕ_j^2 ab. Wird der Zustand ψ immer wieder hergestellt, und von Alice immer wieder mit A_1 vermessen, so erhält sie eine Wahrscheinlichkeitsverteilung der Meßwerte. Dieselbe findet aber auch *Bob*, wenn er im gleichen Takt mit A_2 mißt. Bei einer räumlichen Trennung von Bob und Alice werden also an zwei verschiedenen Orten *identische* Verteilungen der Meßwerte erzeugt.

Wenn Alice allerdings zur Messung eine Observable A_1 verwendet, die nicht mit dem Dichteoperator ω_1 kommutiert, so gerät Bob ein wenig in Schwierigkeiten: s^{21} bildet die Eigenvektoren von A_1 auf ein Vektorsystem ab, das nicht mehr orthogonal ist. Daher findet Bob keine Observable, die das Resultat der Aliceschen Messung genau reproduziert: Bob muß zu diesem Zweck mehrere Observable benutzen, die nicht miteinander kommutieren. Damit er die richtige Auswahl trifft, benötigt er zusätzliche Informationen von Alice über einen klassischen Informationskanal.

Fall 2:

Das eben genannte Problem, das der Übertragung von Quanteninformation abträglich ist, tritt nicht auf, wenn die Eigenwerte der reduzierten Dichtematrizen ω_1, ω_2 alle gleich sind.

In diesem Fall ist $\omega_1 = \omega_2 = \frac{1}{n}\mathbf{1}$, und wir sagen, ψ (bzw. der Zustand $|\psi\rangle\langle\psi|$) sei *maximal verschränkt*. Dann ist auch die Entropie der reduzierten Dichteoperatoren maximal, nämlich ln n. Sie tragen keine Information, sind (quanten)logisch leer; es ist das Quantenanalogon des "unbeschriebenen Blattes". Maximal verschränkte Zustandsvektoren (Zustände) werden auch als *EPR-Vektoren (EPR-Zustände)* bezeichnet. In der Gram–Schmidt–Entwicklung von ψ haben wir nun maximale Freiheit: Zu jeder Orthonormalbasis (ϕ_j^1) aus $\mathcal{H}_1$ gibt es eine eindeutig bestimmte Orthonormalbasis (ϕ_j^2) aus $\mathcal{H}_2$, so daß

$$\psi = \frac{1}{\sqrt{n}} \sum \phi_j^1 \otimes \phi_j^2$$

ist. Entsprechend können wir nun eine *beliebige* Observable des ersten System, die eine vollständige Messung zuläßt, auswählen und finden eine Observable des zweiten Systems, die ebenfalls eine solche Messung zuläßt, so daß die im Fall 1 beschriebene Korrelation der Meßwerte eintritt.

4.5 EPR-Basen

Der EPR-Kanal, der mit einem EPR-Vektor arbeitet, wird uns im nächsten Kapitel beschäftigen. Daher sollten noch einige Bemerkungen über Hilbertraumbasen, die nur aus EPR-Vektoren bestehen, folgen.
In $\mathcal{H}_{12} = \mathcal{H} \otimes \mathcal{H}$ kann man immer eine orthonormale Basis aus EPR-Vektoren, also eine *EPR-Basis* wählen (siehe z.B. die Basiswahl in [9]). Für $\mathcal{H} \simeq C^2$ ist eine solche

EPR-Basis die *Bell-Basis*

$$\varphi^+ = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

$$\varphi^- = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right)$$

$$\psi^+ = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|10\rangle + |01\rangle\right)$$

$$\psi^- = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right).$$

Die Umkehrung liefert

$$|00\rangle = \frac{1}{\sqrt{2}}(\varphi^+ + \varphi^-)$$

$$|01\rangle = \frac{1}{\sqrt{2}}(\psi^+ + \psi^-)$$

$$|10\rangle = \frac{1}{\sqrt{2}}(\psi^+ - \psi^-)$$

$$|11\rangle = \frac{1}{\sqrt{2}}(\varphi^+ - \varphi^-).$$

Durch eine kleine Veränderung der Phasen der Bellschen Basis entsteht die "*magische Basis*"[46]:

$$e_1 = \varphi^+,\ e_2 = i\varphi^-,\ e_3 = i\psi^+,\ e_4 = \psi^-.$$

Ihre Bedeutung besteht u. a. darin, daß jeder Einheitsvektor, der eine *reelle* Linearkombination der e_j ist, maximal verschränkt und somit ein EPR-Vektor ist. Umgekehrt gilt: Jeder EPR-Vektor ist (eventuell bis auf einen komplexen Faktor) eine reelle Linearkombination der Vektoren e_j.

Eine Verallgemeinerung der Bell-Basis für $\mathcal{H} \simeq C^{2^k}$ ist die folgende EPR-Basis . (ϕ_i) sei eine Basis in C^{2^k}. Wir betrachten die 2^k orthonormalen Vektoren aus $C^{2^k} \otimes C^{2^k}$, die durch

$$\phi^\pi = \frac{1}{\sqrt{2^k}} \sum_{i=1}^{2^k} \quad \phi_i \otimes \phi_{\pi(i)}$$

mit der zyklischen Permutation π von $\{1,\ldots,2^k\}$ gegeben sind. Für jeden dieser Vektoren ϕ^π kann man weitere 2^k orthonormale Vektoren der Gestalt

$$\frac{1}{\sqrt{2^k}}\sum_{i=1}^{2^k} \quad \epsilon_k(i)\phi_i \otimes \phi_{\pi(i)}$$

mit $\epsilon_k(i) = \pm 1$ wählen.

Die 2^k Vorzeichenfunktionen ϵ_k werden wie folgt generiert: Jede der 2^{k-1} Vorzeichenfunktionen ϵ_{k-1} erzeugt zwei Vorzeichenfunktionen ϵ_k

$$\epsilon_k(i) = \epsilon_{k-1}(i \mod 2^{k-1})$$

und

$$\begin{aligned}\epsilon_k(i) &= \epsilon_{k-1}(i), i \leq 2^{k-1} \\ &= (-1)\epsilon_{k-1}(i \mod 2^{k-1}), i > 2^{k-1}.\end{aligned}$$

Weniger formal ausgedrückt, führt das auf den folgenden Erzeugungsprozeß der Vorzeichenmuster (für jede zyklische Permutation π):
k=0 +
- durch "identisches Anfügen bzw. Spiegelung" entsteht aus diesem Muster
k=1 ++ +− (*Bell-Basis*)
- durch "identisches Anfügen und Spiegelung" entsteht aus diesem Muster
k=2 ++++ ++−− +−+− +−−+
usw.

Bemerkung:

Man erkennt, daß hinter der Bell-Basis und ihrer Verallgemeinerung für Tensorprodukte des q-Bit-Hilbertraumes die schon beim Hadamard-Gate erwähnten Hadamard-Matrizen stecken. Eine reelle Matrix der Ordnung n heißt *reelle Hadamard-Matrix* [44], wenn $\mathrm{Tr}\, HH^t = n \cdot \mathbf{1}$ (H^t steht für die transponierte Matrix). Damit müssen die Matrixelemente den Wert 1 oder -1 haben und ihre Zeilenvektoren senkrecht aufeinander stehen. Eine weitere Folge ist, daß n nur 1, 2 oder ein Vielfaches von 4 sein. Es ist nicht bekannt, ob tatsächlich Hadamard-Matrizen in all diesen Dimensionen existieren. Unser obiger Fall $n = 2^k$ ist ein Spezialfall und ist (bis auf eine Permutation der Zeilen) die schon früher erwähnte Tensorierung der 2x2-Hadamard-Matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ - eine Konstruktion, die auf Sylvester zurückgeht. □

Sehen wir uns noch einige allgemeine Eigenschaften von EPR-Vektoren an. Sei ψ ein Einheitsvektor in $\mathcal{H} \otimes \mathcal{H}$ und $\phi_1, \phi_2, \ldots, \phi_n$ ein vollständiges Orthonormalsystem in $\mathcal{H}$. Dann gibt es eindeutig bestimmte Vektoren $\tilde{\phi}_1, \tilde{\phi}_2, \ldots$ so, daß

$$\psi = \sum \phi_j \otimes \tilde{\phi}_j$$

gilt. Die Matrixelemente des nach dem ersten Faktor reduzierten Dichteoperators bezüglich des Orthonormalsystems der ϕ_k sind

$$\langle\tilde{\phi}_j, \tilde{\phi}_k\rangle.$$

Der reduzierte Dichteoperator ist also genau dann gleich $(1/n)\mathbf{1}$, wenn die $\tilde{\phi}_j$ bis auf den Faktor $1/\sqrt{n}$ ebenfalls ein vollständiges Orthonormalsystem bilden. Es folgt, daß ψ genau dann ein EPR-Vektor, also maximal verschränkt ist, wenn mit einem unitären Operator U

$$\psi = \frac{1}{\sqrt{n}} \sum \phi_j \otimes U\phi_j \tag{52}$$

ist.

Seien nun ψ_j EPR-Vektoren, die nach dieser Vorschrift mit den unitären Operatoren U_j gebildet sind. Wir sehen dann

$$\langle\psi_k, \psi_l\rangle = \frac{1}{n}\mathrm{Tr}\, U_k^* U_j\,.$$

Zur Konstruktion eines vollständigen Orthonormalsystems von EPR-Vektoren benötigen wir also n^2 unitäre Matrizen mit

$$\mathrm{Tr}\, U_k^* U_l = 0 \text{ wenn } k \neq l, \quad k, l = 1, \ldots, n^2\,. \tag{53}$$

Ist beispielsweise $n = 2$, so erfüllt $\{\mathbf{1}, \sigma_1, \sigma_2, \sigma_3\}$ diese Forderungen, und man erhält die Bellsche Basis im 2-q-Bit-Hilbertraum. Bringt man die Determinanten auf Eins, $\{\mathbf{1}, i\sigma_1, i\sigma_2, i\sigma_3\}$, so entsteht die "magische" Basis (bis auf die Numerierung). Für $n = 4$ bieten sich die Identität und die Produkte der Dirac Matrizen an: $\mathbf{1}$, $\gamma_i\gamma_k$ mit $i < k$, $\gamma_i\gamma_j\gamma_k$ mit $i < j < k$ sowie $\gamma_1\gamma_2\gamma_3\gamma_4$.

Die Forderungen (53) lassen sich für beliebiges n erfüllen. Allerdings findet man, wie wir schon wissen, nur unter bestimmten Bedingungen (wie beispielsweise $n = 2^k$) orthogonale Matrizen. Wählt man als unitäre Wirkung eine Kombination aus Verschiebung der Basisvektoren und Multiplikation mit einem Phasenfaktor, so läßt sich eine schon von [9] angegebene Lösung finden, nämlich die n^2 unitären Matrizen $U_{kl}, k, l = 1, \ldots n$ mit der Wirkung

$$U_{kl}\,\phi_j = e^{\frac{2\pi ijk}{n}}\phi_{j+m} \quad j = 1, \ldots n \quad (j + m \,\mathrm{mod}\, n).$$

Bemerkung:

Der Zusammenhang zwischen der Lösung von (53) und komplexen Hadamard-Matrizen wird bei Werner [89] diskutiert. □

Wir halten abschließend das Resultat in folgender Form fest:

Im Hilbertraum $\mathcal{H}$ (dim $\mathcal{H} = n$) existieren n^2 unitäre Operatoren, die die Bedingungen

$$\mathrm{TrU_k^* U_l} = 0 \qquad \mathrm{k \neq l, k, l = 1, \ldots n^2}$$

erfüllen.
Mit ihrer Hilfe erzeugen die n^2 *lokalen* Operationen

$$\mathbf{1} \otimes U_1, \ldots \mathbf{1} \otimes U_{n^2},$$

oder die n^2 *lokalen* Operationen

$$U_1 \otimes \mathbf{1}, \ldots U_{n^2} \otimes \mathbf{1},$$

aus einem EPR-Vektor eine Orthonormalbasis des Gesamt-Hilbertraumes $\mathcal{H} \otimes \mathcal{H}$.

4.6 Dichtes Kodieren

Die letzte Ausage des vorherigen Abschnitts, daß man durch lokale Operationen eine orthogonale Basis des Gesamt-Hilbertraumes $\mathcal{H} \otimes \mathcal{H}$ erzeugen kann, wollen wir in ein Kodierungsprotokoll übersetzen, auf das zuerst Bennett und Wiesner [14] aufmerksam gemacht haben und das *dichtes Kodieren (dense coding)* heißt (manchmal findet man auch die etwas mystische Bezeichnung "superdense coding").

Gegeben sei ein Quantensystem, das aus den beiden Teilsystemen 1 und 2 besteht. Beide Teilsysteme sollen durch den Hilbertraum $\mathcal{H}$ der Dimension n beschrieben werden. Das Gesamtsystem mit dem Hilbertraum $\mathcal{H} \otimes \mathcal{H}$ soll sich in einem EPR-Zustand befinden. In dieser Situation spricht man (im Hinblick auf die beiden Teilsysteme und insbesondere, wenn sie räumlich unterschiedlich lokalisiert sind) auch von einem *EPR-Paar*. Solche EPR-Zustände lassen sich experimentell gezielt herstellen (s. auch Kapitel Teleportation). Betrachten wir nun wieder Alice und Bob, die über klassische und Quantenkanäle miteinander kommunizieren wollen. Wie wir gesehen haben, kann z.B. Alice durch lokale Operationen (sagen wir) im Teilsystem 1 eine Orthogonalbasis des Gesamt-Hilbertraumes erzeugen und damit $log_2\, n^2 = 2 \cdot log_2\, n$ klassische Bits kodieren. Bob, der am *Gesamtsystem* eine Observable mißt, die gerade diese Eigenvektoren hat, kann Alice´ Botschaft dekodieren.
Man hat den Eindruck, daß sich doppelt so viel Information kodieren läßt, wie klassisch möglich wäre. Allerdings darf man nicht vergessen (und damit klärt sich das Problem auf), daß die Information im EPR-Paar steckt, und Bob unbedingt am Gesamtsystem und nicht nur an einem Teilsystem messen muß.

Alice und Bob sollen (wenn auch nicht notwendigerweise) räumlich getrennt sein. In diesem Fall werden natürlich die bisher stillschweigend übergangenen räumlichen

Freiheitsgrade und die damit verbundenen räumlichen Lokalisierungseigenschaften der Teilsysteme des EPR-Paares wesentlich: Teilsystem 1 bzw. 2 sollte (zumindest während der Operationen) dort lokalisiert sein, wo Alice oder Bob einwirken können. Da Bob letzlich am EPR-Paar messen muß, sollte Alice nach der Operation am Teilsystem 1 dieses an Bob "senden". Da Alice *nur* am Teilysstem 1 operieren muß, könnte Teilsystem 2 auch schon vorher an Bob "gesandt"worden sein. Dieser zeitlich getrennte Versand der Teilsysteme an Bob ist möglicherweise technologisch und/oder im Zusammenenspiel mit anderen Protokollen von Bedeutung.
Wir wollen noch betonen, daß das, was quantenmechanisch nicht verboten und im Formalismus leicht zu bewerkstelligen ist, experimentell selbstverständlich eine knifflige Angelegenheit ist.

4.7 Nochmals Quantenkryptographie

Wir wollen in diesem Abschnitt noch auf ein weiteres Schlüsselaustauschprotokoll eingehen und dafür den EPR-Kanal nutzen. Wie im obigen Abschnitt über Quantenkryptographie soll der "geheime" Austausch einer Zufallsfolge zwischen Alice und Bob ermöglicht werden.
In der Protokoll-Variante BBM92 [11] messen Alice und Bob in ihren zweidimensionalen q-Bit-Hilberträumen $\mathcal{H}_1$ bzw. $\mathcal{H}_2$ in jeweils zufälliger Reihenfolge an einem regelmäßig von einer Quelle ausgesandten EPR-Zustandsvektor $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ immer eine von zwei nichtkommutierenden Ja-Nein-Observablen, deren Eigenwerte jeweils 0 und 1 sind. Als Beispiel betrachten wir die folgende Wahl: Alice und Bob haben (wie oben beschrieben) ihre Basen in den q-Bit-Hilberträumen synchronisiert. P_x sei der Projektor zum Eigenwert 1 von σ_x und P_z der Projektor zum Eigenwert 1 von σ_z. Alice wählt als Ja-Nein-Observable die Projektoren $P_x \otimes \mathbf{1}$ und $P_z \otimes \mathbf{1}$, Bob die Projektoren $\mathbf{1} \otimes P_x$ und $\mathbf{1} \otimes P_z$. Nach Abschluß der Messungen geben beide öffentlich bekannt, welche Folgen von Observablen sie gemessen haben, ohne natürlich die Resultate zu nennen. Es werden alle Meßresultate, die zu korrespondierenden Observablen (im obigen Beispiel $P_x \otimes \mathbf{1}$ und $\mathbf{1} \otimes P_x$ bzw. $P_z \otimes \mathbf{1}$ und $\mathbf{1} \otimes P_z$) gehören, von Alice und Bob markiert; der Rest wird gelöscht. Ein großer und zufällig ausgewählter Teil dieser markierten Ergebnisse wird nun öffentlich verglichen. Sind die technischen Übertragungsfehler und die Störungen durch Lauscher gering, dann läßt sich daraus die "ideale" Korrelation der Meßresultate (falls der EPR-Zustand nicht schon vorher bekannt war) bestimmen. Aus den beiden verbleibenden, nicht öffentlich verglichenen (0,1)-Folgen wird mit Hilfe der ermittelten Korrelationen der geheime Schlüssel erzeugt. Verwenden wir in unserem Beispiel den EPR-Zustand

$$\psi = \frac{1}{\sqrt{2}}[\,|\uparrow\rangle \otimes |\downarrow\rangle + |\downarrow\rangle \otimes |\uparrow\rangle\,],$$

dann führen Messungen von $P_z \otimes \mathbf{1}$ bzw. $\mathbf{1} \otimes P_z$ mit gleicher Wahrscheinlichkeit auf

$$|\uparrow\rangle \otimes |\downarrow\rangle \quad \text{oder} \quad |\downarrow\rangle \otimes |\uparrow\rangle.$$

Die q-Bit-Basis ist dabei aus Eigenvektoren $|\uparrow\rangle, |\downarrow\rangle$ von σ_z gewählt. Die Meßergebnisse 0 bzw. 1 von Alice sind mit den Ergebnissen 1 bzw. 0 von Bob gekoppelt

(ideale Empfangsbedingungen vorausgesetzt). Entsprechendes würde man auch für die P_x-Messungen erhalten. Bob müßte nun in seiner Folge immer 0 durch 1 und 1 durch 0 ersetzen und bekäme dadurch diesselbe Zufallsfolge wie Alice.

Wie sicher ist dieses Verfahren ? Es gelten auch hier die schon oben gemachten Bemerkungen zur Sicherheitsfrage, so daß wir wiederum nur eine der einfachsten "passiven" Abhörattacken betrachten wollen. Angenommen die Lauscherin Eve mißt am "informationslosen" EPR-Zustand ψ in $\mathcal{H}_1$ oder $\mathcal{H}_2$, bevor Alice und Bob tätig werden. Da nicht absehbar ist, welche der nichtkommutierenden Observablen von Alice und Bob gemessen werden, würde beim öffentlichen Vergleich die häufig fehlende Korrelation der Meßresultate (niedriger Rauschpegel natürlich angenommen) auf einen Lauscher hinweisen. Worauf aufmerksam gemacht werden sollte: ausschlaggebend für die Sicherheit dieser und ähnlicher Quanten-Schlüsselaustauschverfahren sind die Besonderheiten von Quantensystemen.

5 Quantenteleportation

Die Quantenteleportation wurde von Ch. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres und W. Wootters erfunden [9]. Das Verfahren ist unlängst auch experimentell bestätigt worden ([15] und noch aktueller [34] und [59]).

Auch hier handelt es sich um einen Quantenkanal, dessen Protokoll die Kanalabbildungen mit einem klassischen Informationskanal verbindet. Im Idealfall wird die Quanteninformation eines Ausgangssystems gelöscht, um sie im Zielsystem vollständig wiederherzustellen. Hierzu denke man sich die Hilberträume mit Referenzbasen ausgestattet, die die Lage der betreffenden Zustände eindeutig beschreiben.

Der Kanal wird durch eine präparierende Messung in Gang gesetzt und realisiert die dem gefundenen Meßwert entsprechende Kanalabbildung. Die Mitteilung des Meßwertes über den klassischen Kanal verweist auf eine eine lokale unitäre Transformation des Zielsystems , mit deren Ausführung das Protokoll abgeschlossen wird.

Dabei wird sorgfältig darauf geachtet, daß keine Quantenoperation erfolgt, die irgendeine Information über den zu teleportierenden Quantenzustand enthält: War dieser vor dem Ausführen des Protokolls unbekannt, so ist er es auch nach seiner Durchführung. Sonst könnte das oben besprochene Kopierverbot durchbrochen werden.

5.1 BBCJPW–Quantenteleportation

Seien $\mathcal{H}, \mathcal{H}_A, \mathcal{H}_B$ Hilberträume gleicher endlicher Dimension d. In ihnen seien Referenzbasen[35] gegeben, deren Vektoren jeweils mit

$$\phi_1, \phi_2, \ldots \quad \phi_1^A, \phi_2^A, \ldots \quad \phi_1^B, \phi_2^B, \ldots$$

bezeichnet werden. Mit diesen Hilberträumen verbinden wir zwei, möglicherweise räumlich getrennt liegende Beobachter: Alice, die Zugriff auf $\mathcal{H} \otimes \mathcal{H}_A$ haben muß, und Bob, dem $\mathcal{H}_B$ "gehört". Unser Anliegen ist es, einen unbekannten Zustandsvektor ϕ aus $\mathcal{H}$ im Hilbertraum $\mathcal{H}_B$ ("relativ zur Basis ") zu reproduzieren:

$$\phi = \sum \langle \phi_i, \phi \rangle \, \phi_i \Longrightarrow \phi^B = \sum \langle \phi_i, \phi \rangle \, \phi_i^B.$$

Als Ausgleich muß in $\mathcal{H}$ jegliche Information über diesen Vektor verlorengehen.

Wir benötigen als erstes einen EPR–Zustandsvektor φ aus $\mathcal{H}_A \otimes \mathcal{H}_B$, den eine EPR-Quelle produziere. Mit einem unitären $U^B \in \mathcal{B}(\mathcal{H}_B)$ kann er

$$\varphi = \frac{1}{\sqrt{d}} \sum \phi_i^A \otimes U^B \phi_i^B$$

[35] Wir erinnern: Referenzbasen sind immer normiert und orthogonal zueinander gewählt.

geschrieben werden. Mit diesen Vorgaben beschreibt der Vektor

$$\phi \otimes \varphi \in \mathcal{H} \otimes \mathcal{H}_A \otimes \mathcal{H}_B.$$

den Anfangszustand des Gesamtsystems.

Die Quantenteleportation wird durch eine Messung von Alice ausgelöst. Sie benutzt zu diesem Zweck eine nichtentartete Observable des von ihr verwalteten Teilsystems, deren Eigenvektoren

$$\varphi_l = \frac{1}{\sqrt{d}} \sum_i \phi_i \otimes U_l^A \phi_i^A \quad l = 1, \ldots, d^2$$

eine EPR–Basis von $\mathcal{H} \otimes \mathcal{H}_A$ bilden.
Das Meßresultat, dessen Informationsgehalt offenbar $2 \log_2 d$ bit ist, wird Bob mitgeteilt. Es soll ihm erlauben, den in seinem Hilbertraum durch den Meßprozeß induzierten Zustandsvektor in den Zustandsvektor ϕ^B zu transformieren.

Zur Analyse des Geschehens nehmen wir an, durch Alicens Messung wäre in $\mathcal{H} \otimes \mathcal{H}_A$ der EPR–Vektor φ_l präpariert worden. Mit Hilfe des Projektionsoperators

$$P_l = |\varphi_l\rangle\langle\varphi_l|$$

wird die im Gesamtsystem induzierte Zustandspräparation durch

$$\phi \otimes \varphi \longrightarrow \frac{(P_l \otimes \mathbf{1})\phi \otimes \varphi}{||(P_l \otimes \mathbf{1})\phi \otimes \varphi||} = \varphi_l \otimes \phi_l^B$$

mit noch zu bestimmenden ϕ_l^B beschrieben, denn es gilt

$$\begin{aligned}
(P_l \otimes \mathbf{1})\phi \otimes \varphi &= \frac{1}{\sqrt{d}} \sum_k P_l(\phi \otimes \phi_k^A) \otimes U^B \phi_k^B \\
&= \frac{1}{d} \sum_k \sum_i < \phi_i \otimes U_l^A \phi_i^A, \phi \otimes \phi_k^A > \varphi_l \otimes U^B \phi_k^B \\
&= \frac{1}{d}\, \varphi_l \otimes U^B \sum_{ik} < \phi_i, \phi > \langle U_l^A \phi_i^A | \phi_k^A \rangle \phi_k^B.
\end{aligned}$$

Aus der eingangs gegebenen Definition von ϕ^B folgern wir

$$< \phi_i, \phi > = < \phi_i^B, \phi^B >$$

für alle ϕ. Daher ist

$$V_l^B \phi^B := \sum_{ik} < \phi_i^B | \phi^B > \langle U_l^A \phi_i^A | \phi_k^A \rangle \phi_k^B$$

für jedes l korrekt definiert. V_l^B ist ein unitärer Operator aus $\mathcal{H}_B$. Somit erhalten wir

$$(P_l \otimes \mathbf{1})\phi \otimes \varphi = \frac{1}{d}\, \varphi_l \otimes U^B V_l^B \phi^B.$$

Damit beschreibt der Vektor $\phi_l^B = U^B V_l^B \phi^B$ den Zustand im Bobschen System.

In $\mathcal{H}$ und $\mathcal{H}_A$ erhält man dagegen die reduzierte Dichtematrix $\frac{1}{d}\mathbf{1}$, die keine Rückschlüsse auf den Startvektor ϕ zuläßt.

Kurz zusammengefaßt: die Zustände der Teilsysteme werden im Verlaufe der Teleportation folgendermaßen verändert

$$|\phi\rangle\langle\phi| \longrightarrow \frac{1}{d}\mathbf{1}, \quad \frac{1}{d}\mathbf{1}^A \longrightarrow \frac{1}{d}\mathbf{1}^A, \quad \frac{1}{d}\mathbf{1}^B \longrightarrow |\phi_l^B\rangle\langle\phi_l^B|.$$

Bob muß nun noch die Transformation

$$\phi_l^B \to \phi^B, \quad \text{bzw.} \quad |\phi_l^B\rangle\langle\phi_l^B| \to |\phi^B\rangle\langle\phi^B|$$

durch Anwendung der zu $U^B V_l^B$ inversen unitären Transformation leisten. Erst dann befindet sich sein System im Zustand ϕ^B.

Bei dieser Aufgabe muß Bob aus d^2 unitären Operationen U_l^A auswählen. Ohne weitere Kenntnisse ist die Wahrscheinlichkeit, die zutreffende zu erraten, gleich $1/d^2$. Um die richtige Wahl zu sichern, benötigt Bob Alicens Meßresultat, also einen Buchstaben aus einem Alphabet der Länge d^2. Die erforderliche Information beträgt, wie schon bemerkt, $I = 2\ln_2 d$ bit. Die reinen Zustände von $\mathcal{H}$ sind die Punkte einer (projektiven) Mannigfaltigkeit der reellen Dimension $2(d-1)$. Zur Markierung eines Punktes dieser Mannigfaltigkeit genügen Bob einige wenige Bit, eine bemerkenswerte Effektivität. (Allerdings sagt das Protokoll ihm nicht, um welchen Punkt es sich handelt!)

Bemerkung 1:

Hat das BBCJPW–Protokoll vielleicht noch eine kleine logische Lücke? Wenn Alice nicht weiß, welchen Zustandsvektor ϕ sie zu Bob teleportiert, woher nimmt sie dann die Gewissheit, es handele sich um einen *reinen* Quantenzustand?

Diese Bedenken kann man mit einer etwas ausgedehnteren Rechnung zerstreuen: Ist ϱ der Dichteoperator eines Zustandes im System $\mathcal{H}$, so ergibt die Messung von Alice tatsächlich in Bobs System einen Zustand mit einem der Dichteoperatoren $(U^B V_l^B)^* \varrho^B (U^B V_l^B)$. Dabei sind die Matrixelemente von ϱ^B wie folgt definiert:

$$\langle \phi_i^B, \varrho^B \phi_j^B \rangle = \langle \phi_i, \varrho \phi_j \rangle.$$

□

Bemerkung 2:

Im Experiment von Zeilinger et al. [15] produziert die EPR–Quelle (nichtlinearer Kristall mit einfallendem Ultraviolett–Photon) durch Konversion ein Infarot–Photonenpaar mit verschränkter Polarisation im Singulett–Zustand

$$\frac{1}{\sqrt{2}}[|\uparrow\rangle \otimes |\downarrow\rangle - |\downarrow\rangle \otimes |\uparrow\rangle] \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

wobei die Basisvektoren ($|\uparrow\rangle$ und $|\downarrow\rangle$ Zustände horizontaler und vertikaler Polarisation beschreiben. Als Eigenfunktionen des zu messenden Operators in $\mathcal{H}\otimes\mathcal{H}_A$ wurden die vier EPR–Zustände (Bell–Basis)

$$\frac{1}{\sqrt{2}}[|\uparrow\rangle\otimes|\downarrow\rangle\pm|\downarrow\rangle\otimes|\uparrow\rangle],\ \frac{1}{\sqrt{2}}[|\uparrow\rangle\otimes|\uparrow\rangle\pm|\downarrow\rangle\otimes|\downarrow\rangle]$$

gewählt. Mit Hilfe der verwendeten interferometrischen Technik (siehe [57]) läßt sich u.a. der Zustand $\frac{1}{\sqrt{2}}[|\uparrow\rangle\otimes|\downarrow\rangle-|\downarrow\rangle\otimes|\uparrow\rangle]$ identifizieren. Ist das einfallende Photon nun im Zustand $\frac{1}{\sqrt{2}}[|\uparrow\rangle+|\downarrow\rangle]\in\mathcal{H}$, so wird ein Viertel der Messungen in $\mathcal{H}\otimes\mathcal{H}_A$ zum Zustand $\frac{1}{\sqrt{2}}[|\uparrow\rangle\otimes|\downarrow\rangle-|\downarrow\rangle\otimes|\uparrow\rangle]$ führen, und obige Rechnung zeigt, daß dann in $\mathcal{H}_B$ der Polarisationszustand $\frac{1}{\sqrt{2}}[|\uparrow\rangle+|\downarrow\rangle]$ reproduziert werden müßte, was die Polarisationsdetektoren tatsächlich auch bestätigen. Die verwendete experimentelle Technik erlaubte noch nicht, alle Bell–Zustände zu unterscheiden. Die i.a. am Zielsystem notwendige unitäre Transformation, die den ursprünglichen Zustand reproduziert, ist durch die spezielle Wahl der beteiligten EPR–Zustände gerade die identische Abbildung. Nachfolgend sind weitere experimentelle Tests (mit kohärentem Licht [34] über Laborentfernungen und mit NMR–Techniken über interatomare Abstände hinweg [59]) durchgeführt worden. □

5.2 Erweiterte Protokolle

Quanten–Teleportation erfordert zwei lokale Aktionen: Die präparierende Messung durch Alice und eine unitäre Transformation im System von Bob.

Eine Messung benötigt keine Auszeichnung von Referenzbasen. Jede der Abbildungen $\phi\to\phi_l^B$ hängt nur von φ und φ_l ab und muß daher eine von der Basiswahl unabhängige Darstellung besitzen.

Diesem Gedanken wollen wir nachgehen und zeigen, daß jede der fraglichen Abbildungen als Aufeinanderfolge zweier EPR–Abbildungen verstanden werden kann. Gleichzeitig erlaubt dieses Vorgehen eine Erweiterung des Protokolls auf verrauschte Quanten–Teleportationen.

Wir nehmen zu diesem Zweck an, φ sei ein beliebiger Vektor aus $\mathcal{H}^A\otimes\mathcal{H}^B$. Außerdem dürfen die φ_l ein beliebiges Orthonormalsystem in $\mathcal{H}\otimes\mathcal{H}^A$ bilden. Von diesem nehmen wir an, es besteht aus den Eigenvektoren einer Observablen mit nicht–entarteten Eigenwerten, die Alice für ihre Messung nutzt.

Seien nun, wie in (49),

$$\varphi=\sum_j\tilde{\phi}_j^A\otimes\tilde{\phi}_j^B,\quad \varphi_l=\sum_j\tilde{\phi}_{l,j}\otimes\tilde{\phi}_{l,j}^A$$

beliebige Produktdarstellungen der relevanten Vektoren. Ihnen sind nach (50) und (51) eindeutig Operatoren zugeordnet, die $\mathcal{H}^A$ in $\mathcal{H}^B$ beziehungsweise $\mathcal{H}$ in $\mathcal{H}^A$ abbilden. Die im Folgenden erforderlichen Operatoren werden s^{BA} und s_l genannt und können mit Hilfe der obigen Produktdarstellungen gefunden werden:

$$s^{BA}\phi^A=\sum\langle\phi^A,\tilde{\phi}_j^A\rangle\tilde{\phi}_j^B,\quad s_l\phi=\sum\langle\phi,\tilde{\phi}_{l,j}\rangle\tilde{\phi}_{l,j}^A,$$

mit $\phi^A \in \mathcal{H}^A$ und $\phi \in \mathcal{H}$. Nun können wir formulieren, wie die l-te Kanalabbildung von $\mathcal{H}$ nach $\mathcal{H}^B$ aussieht. Wir behaupten

$$(|\varphi_l\rangle\langle\varphi_l| \otimes \mathbf{1}_B)\, \phi \otimes \varphi = \varphi_l \otimes s^{BA} s_l\, \phi. \qquad (T)$$

Die Ähnlichkeit mit (46) ist auffallend. Jedoch ist jede der d^2 Abbildungen *linear*, da zwei antilineare Operationen nacheinander ausgeführt werden. In Anlehnung an den vorhergehenden Abschnitt können wir den Bob betreffenden Teil auch

$$\phi \longrightarrow \phi_l^B := t_l\, \phi$$

schreiben. Allerdings muß t_l den Hilbertraum der zu teleportierenden Vektoren nicht notwendigerweise auf ganz $\mathcal{H}^B$ abbilden. Es folgt aus dem Beweis von (T), dem wir uns nun zuwenden, daß dies genau dann eintritt, wenn φ_l oder φ nicht vollständig verschränkt sind.

Beweis von (T) :

Die linke Seite von (T) schreiben um in

$$(|\varphi_l\rangle\langle\varphi_l| \otimes \mathbf{1}_B) \sum \phi \otimes \tilde{\phi}_j^A \otimes \tilde{\phi}_j^B = \varphi_l \otimes \sum_j \langle \varphi_l, \phi \otimes \phi_j^A\rangle \tilde{\phi}_j^B.$$

Jetzt fahren wir wie folgt fort:

$$\begin{aligned} &= \varphi_l \otimes \sum_{ij} \langle \tilde{\phi}_{l,i} \otimes \phi_{l,i}^A, \phi \otimes \phi_j^A\rangle \tilde{\phi}_j^B \\ &= \varphi_l \otimes \sum_{ij} \langle \tilde{\phi}_{l,i}, \phi\rangle \langle \phi_{l,i}^A | \phi_j^A\rangle \tilde{\phi}_j^B \\ &= \varphi_l \otimes \sum_{i} \langle \tilde{\phi}_{l,i}, \phi\rangle s^{BA} \tilde{\phi}_{l,i}^A. \end{aligned}$$

Nun nutzen wir die Antilinearität von s^{BA} und gewinnen

$$= \varphi_l \otimes s^{BA} \sum \langle \phi, \tilde{\phi}_{l,i}\rangle \tilde{\phi}_{l,i}^A = \varphi_l \otimes s^{BA} s_l \phi.$$

Damit ist der Beweis beendet. □

Rückblickend bemerken wir noch Folgendes: $\sqrt{d} \cdot s_l$ ist genau dann antiunitär, wenn φ_l maximal verschränkter Einheitsvektor ist. Analoges gilt für $\sqrt{d} \cdot s^{BA}$ und φ. Sind also diese Vektoren maximal verschränkt, so ist $d \cdot t_l$ als Produkt zweier antiunitärer Abbildungen unitär. Wir erhalten dann die Ergebnisse des vorhergehenden Abschnitts.

Ist ω^A der Dichteoperator, der durch Reduktion von φ auf $\mathcal{H}^A$ entsteht, so ist

$$\langle t_l \phi, t_r \phi\rangle = \langle s_r \phi, \omega^A s_l \phi\rangle.$$

Im allgemeinen Fall sind daher die Telekopien von ϕ nicht orthogonal zueinander. Es reichen dann die von Alice übermittelten Meßresultate nicht mehr aus, um im Bobschen System die Teleportation mit einer unitären, lokalen Operation zu beenden.

Nachwort

Der vorliegende Text ist bis auf kleinere Korrekturen und Zusätze identisch mit dem Preprint NTZ 33/1998 des Zentrums für Höhere Studien der Universität Leipzig. Seitdem sind mehrere Einführungen in dieses Gebiet erschienen. Wir möchten auf die folgende Arbeiten hinweisen, in denen man sich über andere Blickwinkel und auch weitere Aspekte informieren kann:
die Vorlesung von Preskill [68], die Reviews von Bennett & Shor [13], Werner [87], Galindo & Martin-Delgado [36] und die Bücher von Gruska [42], Chuang & Nielsen [58] und den von Lomonaco herausgegebenen Sammelband [55]. Speziell wollen wir auch noch auf den Review von Gisin et al. [38] zur Quanten-Kryptographie verweisen, in dem die von uns nur sehr fragmentarisch angeschnittenen Fragen (und insbesondere deren experimenteller Status) weiterbehandelt werden.

Literatur

[1] D. Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. Archive quant-ph/0301040.

[2] A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev*, A 52:3457–3467, 1995. Archive quant-ph/9503016.

[3] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher. Noncommuting mixed states cannot be broadcast. *Phys.Rev.Lett.*, 76:2818–2821, 1996. Archive quant-ph/9511010.

[4] F. L. Bauer. *Entzifferte Geheimnisse. Codes und Chiffren und wie sie gebrochen werden.* Springer-Verlag, Berlin, New York, 1995.

[5] D. Beckman, A. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. *Phys. Rev*, A 54:1034–1063, 1996. Archive quant-ph/9602016.

[6] P. Benioff. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *J.Stat.Phys.*, 22:563–591, 1980.

[7] C. H. Bennett. Logical reversibility of computation. *IBM J.Res.Develop.*, 6:525–532, 1973.

[8] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, 1992.

[9] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys.Rev.Lett.*, 70:1895–1898, 1993.

[10] C. H. Bennett, G. Brassard, and A. Ekert. Quanten-Kryptographie. *Spektrum der Wissenschaft*, Heft 12:96–104, 1992.

[11] C. H. Bennett, G. Brassard, and D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[12] C. H. Bennett, C. A. Fuchs, and J. A. Smolin. Entanglement-enhanced classical communication on a noisy quantum channel. 1996. Archive quant-ph/9611006.

[13] C. H. Bennett and P. Shor. Quantum information theory. *IEEE Trans. Info. Theory*, 44:2724–2742, 1998.

[14] C. H. Bennett and S. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys.Rev.*, 69:2881–2884, 1992.

[15] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575, 1997.

[16] M. Boyer, G. Brassard, P. Hoyer, and A. Trapp. Tight bounds on quantum searching. *Fortschr. Phys.*, 46:493–506, 1998. Archive quant-ph/9605034.

[17] G. Brassard and C. Crepeau. Cryptology column - 25 years of quantum cryptography. *SIGACT News*, 27:13–24, 1996.

[18] D. Bruß D. DiVincenzo, A. Ekert, C. Fuchs, C. Macchiavello, and J. Smolin. Optimal universal and state-dependent quantum cloning. *Phys. Rev*, A 57:2368–2378, 1998. Archive quant-ph/9705038.

[19] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283–3286, 1998. Archive quant-ph/9805071.

[20] V. Bužek and M. Hillery. Quantum copying: beyond the no-cloning theorem. *Phys. Rev*, A 54:1844–1852, 1996. Archive quant-ph/9607018.

[21] N. Cerf. Asymmetric cloning machines. *J. Mod. Optics*, 47:187, 2000. Archive quant-ph/9805024.

[22] I. Chuang, N. Gershenfeld, and M. Kubinec. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.*, 80:3408–3411, 1998.

[23] I. Chuang, L. Vandersypen, X. Zhou, D. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393:143–146, 1998.

[24] E. B. Davies. Quantum communication systems. *IEEE Trans. Inform. Theory*, 23:530–534, 1977.

[25] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond.*, A 400:97–117, 1985.

[26] D. Deutsch. Quantum computational networks. *Proc. R. Soc. Lond.*, A 425:73–90, 1989.

[27] D. Dieks. Communication by EPR devices. *Phys.Lett.*, A 92:271–272, 1982.

[28] P. A. M. Dirac. Quantum mechanics and a preliminary investigation of the hydrogen atom. *Proc.R.Soc. Lond.*, A 110:561–579, 1926.

[29] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Phys.Rev.*, 47:777–780, 1935.

[30] A. Ekert and R. Jozsa. Quantum computation and Shors factoring algorithm. *Rev. Mod. Phys.*, 68:733–753, 1996.

[31] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. A limit on the speed of quantum computation in determining parity. *Phys. Rev. Lett.*, 81, 1998.

[32] R. Feynman. Simulating physics with computers. *Internat. J. Theoret. Phys.*, 21:467–488, 1982.

[33] R. Feynman. Quantum mechanical computers. *Optics News*, 11:11–20, 1985. auch: Found.Phys. 16(1986)507-531.

[34] A. Furusawa, J. Sørensen, S. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science*, 282:706–709, 1998.

[35] D. Gabor. Communication theory and physics. *Phil.Mag.*, 41:1161–1187, 1950.

[36] A. Galindo and M. A. Martin-Delgado. Information & computation: Classical and quantum aspects. *Rev. Mod. Phys.*, 74:347–423, 2002.

[37] N. Gisin and S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.*, 79:2153–2156, 1997. Archive quant-ph/9705046.

[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. Archive quant-ph/0101098.

[39] J. P. Gordon. Quantum effects in communication systems. *Proc. IRE*, 50:1898–1908, 1962.

[40] L. Grover. A fast quantum algorithm for database research. In *Proc. 28th ACM Symp. on Theory of Computation*, pages 212–219, Philadelphia, 1996.

[41] L. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997. Archive quant-ph/9706033.

[42] J. Gruska. *Quantum Computing*. McGraw-Hill, London, 1999.

[43] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, 1979.

[44] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays*. Springer Series in Statistics. Springer-Verlag, Berlin, New York, 1999.

[45] C. W. Helstrom, J. Liu, and J. P. Gordon. Quantum-mechanical communication theory. *Proc. IEEE*, 58:1578–1598, 1970.

[46] S. Hill and W. Wootters. Entanglement of a pair of quantum bits. *Phys. Rev. Lett.*, 78:5022–5025, 1997.

[47] A. Holevo. Problems in the mathematical theory of quantum communication channels. *Rep. Math. Phys.*, 12:273–278, 1977.

[48] R. Hughes, D. Alde, P. Dyer, G. Luther, G. Morgan, and M. Schauer. Quantum cryptography. *Contemp. Phys.*, 36:149–163, 1995.

[49] R. Ingarden. Quantum information theory. *Rep. Math. Phys.*, 10:43–72, 1976.

[50] J. A. Jones and M. Mosca. Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer. *J. Chem. Phys.*, 109:1648–1653, 1998. Archive quant-ph/9801027.

[51] R. Jozsa. Quantum effects in algorithms. Archive quant-ph/9805086.

[52] N. Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, New York, 1987.

[53] L. B. Levitin. On the quantum measure of information. In *Proc. 4th All-Union Conference on Information and Coding Theory*, pages 111–115, Taschkent, 1969. engl. Übersetzung: Ann. Fond. L. de Broglie 21(1996)345-348.

[54] G. Lindblad. Completely positive maps and entropy inequalities. *Comm. Math. Phys.*, 40:147–151, 1975.

[55] S. J. Lomonaco, editor. *Quantum Computation: A Grand Mathematical Challenge fot the Twenty First Century and the Millenium*. Proc. Symp. Appl. Math. 58. American Mathematical Soc., Providence, Rhode Island, 2002.

[56] G. Lüders. Über die Zustandsänderung durch den Meßprozeß. *Ann.d.Physik*, 8:322–328, 1951.

[57] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger. Interferometric Bell-state analysis. *Phys. Rev*, A 53:R1209–1212, 1996.

[58] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[59] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation by nuclear magnetic resonance. *Nature*, 396:52–55, 1998. Archive quant-ph/9811020.

[60] C.-S. Niu and R. Griffith. Optimal copying of one quantum bit. *Phys. Rev*, A 58:4377–4393, 1998. Archive quant-ph/9805073.

[61] M. Ohya. On compound state and mutual information in quantum information theory. *IEEE Trans. Inf. Theory*, 29:770–774, 1983.

[62] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, Berlin, New York, 1993.

[63] Y. Ozhigov. Quantum computers speed up classical with probability zero. *Chaos Fractals Solitons*, 10:1707–1714, 1999. Archive quant-ph/9803064.

[64] A. Peres. Reversible logic and quantum computer. *Phys. Rev*, A 32:3266–3276, 1985.

[65] C. A. Petri. Grundsätzliches zur Beschreibung diskreter Prozesse. In *3. Kolloquium über Automatentheorie,Hannover 1965*, pages 121–140, Basel,Stuttgart, 1967. Birkhäuser Verlag.

[66] S. Phoenix and P. Townsend. *Quantum cryptography: protecting our future networks with quantum mechanics*, volume 1025 of *Lecture Notes in Computer Science*, pages 112–131. Springer-Verlag, Berlin, New York, 1995.

[67] J. Preskill. Fault-tolerant quantum computation. 1997. Archive quant-ph/9712048.

[68] J. Preskill. Course on quantum information and computation. *http://www.theory.caltech.edu/ preskill/ph229*, 1997-1999.

[69] H. Riesel. *Prime Numbers and Computer Methods for Factorization*, volume 126 of *Progress in Mathematics*. Birkhäuser, Boston, Basel, second edition, 1994.

[70] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23:807–812,823–828,844–849, 1935.

[71] E. Schrödinger. Discussion of probability relations between separated systems. *Proc.Cambr.Phil.Soc.*, 31:555–563, 1935.

[72] B. Schumacher. Quantum coding. *Phys. Rev*, A 51:2738–2747, 1995.

[73] Y. Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computation. Archive quant-ph/0205115.

[74] P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe*, pages 124–134. IEEE Computer Society Press, 1994.

[75] P. Shor. Fault-tolerant quantum computation. In *Proc. 37th Symp. on Foundations of Computer Science*, pages 56–65, Los Alamitos, 1996. IEEE Computer Soc. Press.

[76] P. W. Shor. Polynomial -time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 5:1448–1509, 1997.

[77] D. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26:1474–1483, 1997.

[78] A. Steane. Multiple particle interference and quantum error correction. *Proc.Roy.Soc. Lond.*, A 452:2251, 1996. Archive quant-ph/9601029.

[79] A. Steane. Efficient fault-tolerant quantum computing. 1998. Archive quant-ph/9809054.

[80] A. Steane. Quantum computing. *Rep.Prog.Phys.*, 61:117–173, 1998. Archive quant-ph/9708022.

[81] T. Toffoli. Bicontinuous extensions of invertible combinatorial functions. *Math. Systems Theory*, 14:13–23, 1981.

[82] A. Uhlmann. On the Shannon entropy and related functionals on convex sets. *Rep. Math. Phys.*, 1:147–159, 1970.

[83] A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[84] A. Uhlmann. Zur Beschreibung irreversibler Quantenprozesse. *Sizungsber. AdW DDR*, 14 N:1–25, 1976.

[85] V. Vedral and M. Plenio. Basics of quantum computation. *Prog. Quant. Electron.*, 22:1–40, 1998. Archive quant-ph/0111116.

[86] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer-Verlag, Berlin, 1932.

[87] R. Werner. Quantum information: An invitation. Archive quant-ph/0101061, to appear: Springer Tracts in Modern Physics.

[88] R. Werner. Optimal cloning of pure states. *Phys. Rev*, A 58:822–829, 1998. Archive quant-ph/9804001.

[89] R. F. Werner. All teleportation and dense coding schemes. Archive quant-ph/0003070.

[90] W. K. Wooters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[91] C. Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev*, A 60:2746–2751, 1999. Archive quant-ph/9711070.

[92] P. Zanardi. A note on quantum cloning in d dimensions. *Phys. Rev*, A 58:3484, 1998. Archive quant-ph/9804011.