Quanteninformationstheorie
Wintersemester 1998/99

Helge Kreutzmann
Christian Trump

auf Grundlage der Vorlesung von M. Lewenstein
Institut für Theoretische Physik
Universität Hannover

31. März 2004
Version 0.92

Inhaltsverzeichnis

Danksagung

Diese Vorlesung basiert auf Material, das ich von Dagmar Bruss, Ignacio Cirac und Anna Sanpera erhalten habe. Mein eigener Beitrag zu dieser Vorlesung war begrenzt. Ich danke meinen Freunden, die mir das Material zur Verfügung gestellt haben.

Maciej Lewenstein

1 Einleitung

1.1 Einführung - warum Quanteninformationstheorie?

Diese Vorlesung behandelt quantenmechanische Informationstheorie. Die klassische Informationstheorie, wie sie insbesondere von SHANNON betrieben wurde, ist heutzutage auf „Software-Ebene“ realisiert, z.B. im Rahmen logischer Ausdrücke in höheren Programmiersprachen (if-statements), ebenso auf Hardware-Ebene mit klassischer Digital-Technik. Zustände sind 1 (high, +5 Volt), und 0 (low, 0 Volt), und die Bauteile eines Chips sind in ihrer Funktion über diese beiden Zustände definiert. Dies wird auch Binärcodierung genannt.
Quantenmechanisch gibt es jedoch nicht nur diese beiden Zustände, sondern auch die Superposition. Quantenmechanik (QM) ist auch die fundamentale Beschreibung der Zustände eines Festkörpers, d.h. der Hardware. Mit immer fortschreitender Miniaturisierung der logischen Bausteine werden die quantenmechanischen Effekte relevant. Andererseits ist es - unabhängig von der Größe der Hardware - auch reizvoll, mehr über die Möglichkeiten einer Rechnung mit quantenmechanischen Gesetzen zu wissen. Eventuell liegen nämlich in der Quantenmechanik Vorteile gegenüber der klassischen Rechnung, die durch die besondere Wirkungsweise der QM zustande kommen. Insbesondere hat hier in den letzten Jahren das Problem der Primfaktorzerlegung eine große Rolle gespielt. Die Vorlesung legt auf den zweiten Aspekt ein größeres Gewicht.

1.2 Klassische Informationstheorie

1.2.1 Unsicherheit

Eigenschaften der Unsicherheit $H(p_1, \ldots, p_n)$:
Seien im folgenden p_i Wahrscheinlichkeiten (z.B. einer Zufallsvariablen X: $P(X = a_k) = p_k$. Für Wahrscheinlichkeiten gilt: $\sum_i p_i = 1$. Damit wird die Größe H mit den folgenden Eigenschaften eingeführt (axiomatisch, SHANNON 48):

1. $H(p_1, \ldots, p_n)$ ist maximal, wenn $p_1 = p_2 = \cdots = p_n$
2. Für jede Permutation π ist $H(p_{\pi(1)}, \ldots, p_{\pi(n)}) = H(p_1, \ldots, p_n)$
3. $H(p_1, \ldots, p_n) \geq 0$; $H(p_1, \ldots, p_n) = 0 \Leftrightarrow p_i = 1,\ p_j = 0 \quad \forall j \neq i$
4. $\underbrace{H(\frac{1}{n}, \ldots, \frac{1}{n})}_{\text{n Argumente}} \leq \underbrace{H(\frac{1}{n+1}, \ldots, \frac{1}{n+1})}_{\text{n+1 Argumente}}$

5. $H(p_1, \ldots, p_n, 0) = H(p_1, \ldots, p_n)$

6. $H(p_1, \ldots, p_n)$ ist eine stetige Funktion der p_i

7. $H(\frac{1}{m \cdot n}, \ldots, \frac{1}{m \cdot n}) = H(\frac{1}{m}, \ldots, \frac{1}{m}) + H(\frac{1}{n}, \ldots, \frac{1}{n})$

8. Seien zwei Ereignisse A, B mit den Wahrscheinlichkeiten $p_A = p_1 + p_2 + \cdots + p_m$, $q_B = q_1 + q_2 + \cdots + q_n$ aus mehreren (Elementar)ereignissen zusammengesetzt mit der Bedingung $p + q = 1$. Dann soll folgen:
   $H(p_1, \ldots, p_m, q_1, \ldots, q_n) \stackrel{!}{=} H(p, q) + pH(\frac{p_1}{p}, \ldots, \frac{p_m}{p}) + qH(\frac{q_1}{q}, \ldots, \frac{q_n}{q})$
   Dies ist vernünftig: Falls bekannt ist, zu welcher Gruppe das Ereignis gehört, ist die Unsicherheit um $-H(\sum p_i, \sum q_j)$ gefallen, die restliche Unsicherheit ist:

   - für A: $H(\frac{p_1}{\sum p_i}, \ldots, \frac{p_m}{\sum p_i})$,
   - für B: $H(\frac{q_1}{\sum q_j}, \ldots, \frac{q_n}{\sum q_j})$,

   Die gewichtete Summe der Restunsicherheiten und die abgezogene Unsicherheit sollen gleich der Gesamtunsicherheit sein. (Gruppierungsaxiom)

Theorem 1 *$H(p_1, \ldots, p_n)$ definiert für jedes n, $\sum_{i=1}^{n} p_i = 1$, $0 \leq p_i \leq 1$. Wenn H die Bedingungen 1-8 (1.2.1) erfüllt $\Leftrightarrow$*

$$H = -\lambda \sum_k p_k \ln(p_k) \qquad \text{SHANNON: } \textit{Entropie}$$

$$H = -\sum_k p_k \log_2(p_k) \qquad \textit{„bits“}$$

wobei die Konstante λ je nach verwendetem Logarithmus unterschiedlich ist. Für ein System mit zwei Zuständen $(0, 1)$ wird $\log_2$ benutzt. Die Konstante λ ist nicht mehr notwendig, wenn wir nur Zweiersysteme betrachten, da über die absolute Größe von H keine Aussage gemacht wird (s. Def.!).
Beweis:
„$\Leftarrow$“ läßt sich durch Nachrechnen überprüfen, „$\Rightarrow$“, s. z.B. in der Literatur [3].
Betrachten wir nun das Verbundereignis zweier Zufallsgrößen X und Y mit Werten $x_1, \ldots x_k$ bzw. $y_1, \ldots y_l$.

Def. 1 *Verbundwahrscheinlichkeit: $p(x_i, y_j) := P(X = x_i, Y = y_j)$*
kurze Schreibweise für M Größen: $p(x_1, \ldots, x_M)$

Def. 2 *Joint Entropy: Entropie eines Verbundereignisses*
Für zwei Zufallsgrößen:

$$H(X,Y) \;:=\; -\sum_{j,i=1}^{k,l} p(x_i,y_j)\log(p(x_i,y_j))$$

Für M Zufallsgrößen:

$$H(X,\ldots,X_M) \;:=\; -\sum_{x_1,x_2,x_3,\ldots,x_M} p(x_1,x_2,\ldots x_M)\log p(x_1,x_2,\ldots x_M)$$

So läßt sich z.B. für die fünf Zufallsgrößen Luftdruck, Temperatur, Windstärke und -richtung und Sonnenscheindauer die Entropie des Wetters berechnen, indem man die Verbundwahrscheinlichkeitsdichte so auswertet.

Theorem 2 $H(p_1,\ldots,p_m) \le \log_2(m) \quad (= \log_2(m)$ *wenn* $p_i = \frac{1}{m})$

Lemma 1 *Wenn* p_i, q_i *Wahrscheinlichkeiten* $\Rightarrow$ *Minimum von* $G(q_1,\ldots,q_m) = -\sum p_i \ln(q_i)$ *ist erreicht für* $q_i = p_i$ *(bis auf Permutationen)*

Theorem 3 X, Y *Zufallsvariablen:* $H(X,Y) \le H(X) + H(Y)$

Das Wetter soll jetzt in Abhängigkeit der Regenmenge am Vortag untersucht werden. Dazu wird die bedingte Entropie benötigt:

Def. 3 *Bedingte Entropie:*
Es seien X, Y *Zufallsvariablen mit Verbundwahrscheinlichkeit* $p(x_i,y_j)$. *Falls* Y *den Wert* y_j *annimmt, ist die* bedingte Entropie unter Annahme $Y = y_j$

$$H(X|Y=y_j) := -\sum_{i=1}^{k} p(x_i|y_j)\log_2 p(x_i|y_j)$$

Die gewichtete Summe über alle y_j *ist die* bedingte Entropie.

$$\begin{aligned} H(X|Y) \;&:=\; -\sum_{j=1}^{l} p(y_j)\sum_{i=1}^{k} p(x_i|y_j)\log_2 p(x_i|y_j) \\ &=\; \sum_{i,j}^{k,l} p(x_i,y_j)\log_2 p(x_i|y_j) = \sum_{j=1}^{l} H(X|y_j) \end{aligned}$$

$\rightsquigarrow H(X|X) = 0$; $H(X|Y) = H(X)$ wenn X, Y unabhängig, d.h. $p(x_i, y_j) = p(x_i)p(y_j)$.
Das Wetter hält also, falls wir die Regenmenge Y vom Vortag wissen, diese Menge an Information (=Überraschung) für uns bereit.
Zwischen bedingter und Verbundentropie besteht außerdem folgender Zusammenhang:

Theorem 4 $H(X,Y) = H(Y) + H(X|Y); \quad H(X|Y) \leq H(X)$

Es lassen sich noch viele andere Beziehungen herleiten und/oder definieren, dafür sei aber auf die Spezialliteratur verwiesen.

1.2.2 Information

Zur Definition von Information kann formal folgende Regel angeben werden: Sind E_1 und E_2 Ereignisse mit den Wahrscheinlichkeiten p_1 und p_2, dann ist $I(p_1 p_2) = I(p_1) + I(p_2)$. Die so definierte Information wird manchmal auch als Unsicherheit oder Entropie (teilweise auch Negentropie) bezeichnet. Es geht um die Unsicherheit, die ich von einem bestimmten Ereignis besitze. Nach dem Ereignis ist der Ausgang bekannt, ich habe Information gewonnen. Wieviel? Genau soviel, wie der vorherigen Unsicherheit entspricht.

Def. 4 $I(E) = -\log_2(p(E))$
$\rightsquigarrow H(X) = \sum_k p_k I(X = a_k)$ *wenn* X *die Werte* a_k *mit* p_k *annimmt.*

2 Rauschloses Codierungstheorem für gedächtnislose Quellen

2.1 Einführung

(Noiseless Coding Theorem for Memoryless Sources)
In diesem Abschnitt wird das allgemein als „SHANNONS Theorem“ bekannte Theorem abgeleitet und die dafür notwendigen Größen definiert. Das Theorem ist ein sehr allgemein und gibt eine untere Grenze für die Codewortlänge eines Codierverfahrens an. Auch der in der Nachrichtentechnik meistverwandte Codieralgorithmus (von HUFFMAN) liegt innerhalb dieser Grenzen. An einem Beispiel soll dieser dann einmal vorgeführt werden.
Die Signifikanz von SHANNONS Theorem liegt jedoch auch in der Allgemeinheit: Eine Codierung mit Wortlängen entspricht im informationstheoretischen Sinn auch einer Strategie mit Zuglängen (bis zum Erreichen des Zieles): beide Male ist die Frage, wie viele Einzelentscheidungen benötigt werden, um eine bestimmte Information zu übertragen/herauszufinden.

2.2 Definitionen

Im Folgenden werden einige Definitionen aufgeführt. Diese machen Gebrauch von *Zeichenketten (Strings)*. Zeichenketten bestehen aus Untereinheiten, den sog. *Wörtern*, und diese wiederum aus *Symbolen*. Ein binärer Symbolvorrat $\Sigma = 0, 1$ besteht nur aus 0en und 1en, der Symbolvorrat des Deutschen besteht aus 29[1] verschiedenen Zeichen. Symbole werden meist mit a_i bezeichnet. Beispiele für einen Symbolvorrat in diesem Sinne können auch sein: die Vokale a, e, i, o, u. Der Code ist eine Abbildung vom ersten Symbolvorrat in den zweiten. Dadurch entstehen Probleme, da die Größe des Symbolvorrates unterschiedlich ist (z.B. $2 \leftrightarrow 26$). Deshalb wird jedes *Symbol* der deutschen Sprache in der digitalen Nachrichtentechnik durch ein *Wort* repräsentiert. So kann z.B. auch der ASCII-Code ($a \mapsto 1000001$ (binäres Wort)) als eine solche (ineffiziente) Codierung verstanden werden.
Die Begriffe Wort, Symbol usw. gelten sowohl für die ursprüngliche als auch für die verschlüsselte Nachricht. Ein *Alphabet* ist die Menge aller aus Σ bildbaren Wörter, also ein *Wörterbuch*. Das Alphabet besteht damit aus lauter einzelnen Wörtern. Die Menge Σ^* ist die Menge aller endlichen Zeichenketten, d.h. aller möglichen Nachrichten aus diesen Wörtern.
Quellen sind Nachrichtensender, die eine Folge von Symbolen (=Nachricht)

[1] ohne Groß/Kleinschreibung , mit ä,ß, . . . :-))

aussenden. Dabei bezeichnet X_i den Platzhalter für das i-te Symbol der Nachricht, das z.B. durch das Symbol a_j realisiert sein kann.
Quellen sind gekennzeichnet durch ihren Symbol- (bzw. Wort-)Vorrat a_j *und* durch die jeweilige Wahrscheinlichkeiten der Symbole $p_j = P(X_i = a_j)$. Dabei kann grundsätzlich das Auftreten eines Wortes abhängig vom Auftreten anderer Wörter sein (z.B. in der deutschen Sprache: ein „u“ tritt selten auf, auf ein „q“ folgt das „u“ mit sehr hoher Wahrscheinlichkeit). Eine *gedächtnislose Quelle* zeigt genau dieses Verhalten nicht: jedes Wort ist immer gleich wahrscheinlich; es existieren keine *Interdependenzen*. Die Quelle ist also insofern einfacher zu beschreiben. Die Codierungstheorie fragt, wie die Symbole der Nachricht einer Quelle möglichst redundanzfrei durch binäre Wörter dargestellt werden können, so daß die Entropie der codierten Nachricht nicht weit über der der Quelle liegt.

Def. 5 *Gedächtnislose Quellen (memoryless sources, MLS)*
Eine MLS erzeugt eine Zeichenkette von Symbolen X_i mit Wahrscheinlichkeiten $P(X_i = a_j) = p_j$, die von i und allen vorherigen $X_k, k < i$ unabhängig sind (gedächtnislos).

Beispiel:
Symbolvorrat=$a_1, \ldots, a_n$. Nachricht=$X_1X_2X_3X_4$, X_i ein Wert aus dem Symbolvorrat. Zusammen mit den Wahrscheinlichkeiten für die Symbole ergibt sich ein Ensemble, nämlich die Quelle.
Entropie der Quelle:
$H = -\sum_i p_i \log(p_i)$, wobei log immer zur Basis 2.

2.3 Instantane Codes (I-Codes) und eindeutig entzifferbare Codes (UD-Codes)

(Instananeous Codes and Uniquely Decipherable Codes)
Sei eine MLS gegeben durch $W = \{w_1, w_2, \ldots, w_m\}$ mit Wahrscheinlichkeiten $p_1, \ldots, p_m$. Sei Σ ein Alphabet von $D = 2$ (z.B. $\Sigma = \{0, 1\}$) Symbolen. Die Frage ist nun, wie die Wörter auf effizienteste Weise mit Σ codiert werden können. Als Beispiel erzeuge eine Quelle S $\{w_1, w_2, w_3, w_4\}$ (Wertevorrat), mit Wahrscheinlichkeiten $P(X_i = w_1) = 0.9$, $P(X_i = w_2) = 0.05$, $P(X_i = w_3) = 0.025$, $P(X_i = w_4) = 0.025$. Vergleiche folgende Codierungen:

Codierung	w_1	w_2	w_3	w_4	$\langle n \rangle$
A	0	111	110	101	1.2
B	00	01	10	11	2

wobei sich die mittlere Wortlänge aus $\langle n \rangle = \bar{n} = \sum_i n(w_i)p(w_i)$ ergibt.
Seien Σ ein Alphabet („Wörterbuch“) und $\Sigma^* = W^*$ die Menge aller endlichen Strings der Wörter.

Def. 6 *Codierung/Code*
Eine Codierung (Chiffre) ist eine Funktion f mit:
$f : \{w_1, w_2, \ldots, w_m\} \mapsto \Sigma^*$

Eine Nachricht $m = (w_{i_1} w_{i_2} w_{i_3} \ldots w_{i_k})$ der Quelle aus W^* wird in Σ^* mit der Vorschrift

$$f(m) := f(w_{i_1}) f(w_{i_2}) f(w_{i_3}) \ldots f(w_{i_k})$$

codiert. Die *Länge* eines einzelnen codierten Wortes $|f(w_i)| \sim$ der Zahl der Symbole aus Σ, die zur Codierung benötigt werden. Die *mittlere Wortlänge* ist definiert als $\langle f_S \rangle := \sum_i p_i |f(w_i)|$.

Def. 7 *Präfix*
Seien $x, y \in \Sigma^*$. x ist ein Präfix *von y wenn es ein $z \in \Sigma^*$ gibt, so daß xz=y.*

Def. 8 *I-Code Ein Code f ist* instantan *(I-Code), wenn es kein w_i, w_j gibt, für die $f(w_i)$ ein Präfix von $f(w_j)$ ist*[2].

Damit ist jeder I-Code auch eindeutig decodierbar.
Beispiel: Komma-Code mit $\Sigma = \{0, 1\}$.
Der Symbolvorrat einer Quelle sei mit w_1, w_2, w_3, w_4 erschöpft. Codierung: $f(w_1) = 0$, $f(w_2) = 10$, $f(w_3) = 110$, $f(w_4) = 1110$. Die Symbolfolge $011010011101100\ldots$ wird zurückübersetzt in $w_1 w_3 w_2 w_1 w_4 w_3 w_1 \ldots$.
Jedoch ist nicht jeder UD-Code ein I-Code. Als Beispielcode kann z.B. der Quellsymbolvorrat $W = \{w_1, w_2\}$, abzubilden in den Symbolraum $\Sigma = \{0, 1\}$ mittels der Vorschrift (Code): $f(w_1) = 0$, $f(w_2) = 01$ dienen.
Da $f(w_1)$ Präfix von $f(w_2)$ ist, ist er nicht instantan (von vorne nach hinten) lesbar. Jedoch sobald die gesamte Nachricht angekommen ist, ist sie eindeutig decodierbar (lese von hinten):

$$001010100010101$$

Generell gesagt, ist das Konzept eines UD-Codes etwas komplexer als das Konzept eines I-Codes.

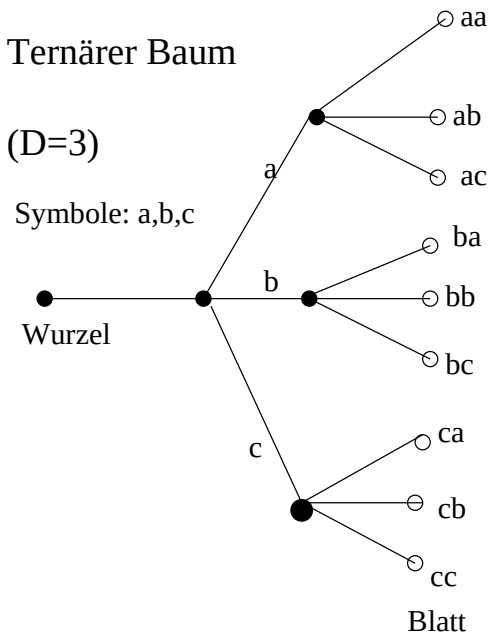
[2] I-Codes werden auch als Präfixcodes bezeichnet

2.4 Kraft-McMillan-Ungleichungen

Theorem 5 KRAFT*sche Ungleichung*
Sei eine Quelle mit N Symbolen gegeben, die mittels des Codes in N Wörter mit Wortlänge $l_i, i = 1 \dots N$ des Alphabetes Σ übersetzt werden sollen. Die Anzahl der Symbole in Σ sei D. Dann existiert ein I-Code $\Leftrightarrow$

$$\sum_{i=1}^{N} D^{-l_i} \leq 1.$$

Beweis: „$\Leftarrow$“
Sei $\sum_{i=1}^{N} D^{-l_i} \leq 1$.
Führe eine Entartung n_j zu l_i ein: Anzahl der Wörter mit Länge $l_i = j$. Weiter bezeichne $l = \max(l_i)$. Dann gilt
$\sum_{j=1}^{l} n_j D^{-j} \leq 1$
Dies entspricht der Zusammenfassung von Wörtern gleicher Länge. Umformen ergibt
$n_l \leq D^l - n_1 D^{l-1} - n_2 D^{l-2} - \dots - n_{l-1} D$, also auch
$0 < D^l - n_1 D^{l-1} - n_2 D^{l-2} - \dots - n_{l-1} D$. Dividiere durch D:
$n_{l-1} < D^{l-1} - n_1 D^{l-2} - n_2 D^{l-3} - \dots - n_{l-2} D$ wiederhole Prozedur
$\vdots$
$n_2 < D^2 - n_1 D$
$n_1 < D$
Es können n_1 Wörter der Länge 1 codiert werden (da $D > n_1$, D Anzahl der Symbole). Sei W_1^* die Menge dieser Symbole (Wörter). Damit existieren n_1 Wörter der Länge 1, und $D - n_1$ noch nicht benutzte Symbole. Es existieren n_2 Wörter der Länge 2. Ohne Präfixe aus W_1^* zu verwenden, gibt es noch $D(D - n_1)$ mögliche Kombinationen von zwei Symbolen aus Σ, was nach obigen Ungleichungen ausreicht. Diese Menge sei W_2^*.
Entsprechend gibt es n_3 Wörter der Länge 3. Um diese darzustellen, werden aus den (präfix-freien) $D^3 - n_2 D^2 - n_1 D$ möglichen Wörtern n_3 ausgewählt. Dieses Verfahren wird entsprechend bis n_l fortgesetzt.
„$\Rightarrow$“
Zum Beweis der Ungleichung für I-Codes betrachte einen D-ären Baum der Ebenenzahl l_{max} (=Länge des längsten Codewortes). Ein Codewort mit Länge l_i befindet sich in diesem Baum auf Ebene l_i und hat in der obersten Ebene $D^{l_{max} - l_i}$ Nachfolger. Man kann nun die Summe der Nachfolger aller Codewörter ($\sum_i$) in der obersten Ebene bilden. Da es sich um einen I-Code handelt, kann kein Nachfolger zu 2 Codewörtern gehören. Die Gesamtzahl der Nachfolger in der obersten Ebene ist also $\sum_i D^{l_{max} - l_i}$.



Auf der anderen Seite ist die Gesamtzahl der Blätter (=Knoten auf oberster Ebene) $D^{l_{max}}$. Daher folgt:

$$\sum_{i=1}^{N} D^{l_{max}-l_i} \leq D^{l_{max}} \quad \rightarrow \quad \sum_{i=1}^{N} D^{-l_i} \leq 1.$$

Theorem 6 McMillan*sche Ungleichung*
Mit den Bezeichnungen wie oben:
Es existiert ein UD-Code mit max. Wortlänge $N \Leftrightarrow$

$$\sum_{i=1}^{N} D^{-l_i} \leq 1.$$

Beweis „$\Leftarrow$“ Diese Richtung ist einfach, da Kraft erlaubt, aus der Bedingung einen I-Code zu entwickeln. Jeder I-Code ist aber auch ein UD-Code.

„$\Rightarrow$“ Sei ein UD-Code mit Wörtern der Länge $l_1, \ldots, l_N$ gegeben. Ist $l = \max l_i$ und wird eine Wortfolge der Länge r konstruiert, dann gilt

$$\left(D^{-l_1} + \cdots + D^{-l_N}\right)^r = \sum_{i=1}^{rl} b_i D^{-i} \qquad r \in \mathbb{N}.$$

b_i ist hierbei die Anzahl der Kombinationen, mit denen eine Wortfolge aus r Wörtern des Alphabets Σ der Gesamtlänge i konstruiert werden kann[3]. Da

[3] z.B. beim Komma-Code mit $r = 3$ ist $b_1 = b_2 = 0$, $b_3 = 1$, $b_4 = 3$, $b_5 = 6$, $b_6 = 9$ usw.

der Code eindeutig entzifferbar ist, muß die Anzahl der *erlaubten* Kombinationsmöglichkeiten der Symbole maximal die Anzahl der *möglichen* Kombinationen sein, d.h. $b_i \leq D^i$ und somit

$$\begin{aligned} \left(\sum_{i=1}^{N} D^{-l_i}\right)^r &\leq \sum_{i=1}^{rl} 1 = rl \\ \sum_{i=1}^{N} D^{-l_i} &= (rk)^{\frac{1}{r}} \xrightarrow{r\to\infty} 1 \end{aligned}$$

Aus beidem Theoremen folgt: Es existiert ein UD-Code mit fester Wortlänge $l_1 \dots l_n \Leftrightarrow$ es existiert ein I-Code mit festen Wortlängen $l_1 \dots l_n$.

2.5 Rauschlose Codierung-Theorem

Sei S eine Quelle mit den zu codierenden Symbolen $w_1 \dots w_m$ mit Wahrscheinlichkeiten $p_1, \dots, p_m$. Gesucht wird ein UD-Code mit dem Alphabet Σ so daß die mittlere Wortlänge so kurz wie möglich wird (Dies wird kompakter Code (C-Code) genannt). Die Entropie der Quelle berechnet sich zu $H = -\sum_{i=1}^{m} p_i \log(p_i)$.

Theorem 7 SHANNONs *Theorem*
Habe S die Entropie H. Dann muß jeder UD-Code von S in Σ die mittlere Wortlänge $l(S) \geq \frac{H}{\log_2 D}$ haben. Es existiert mind. ein UD-Code mit Wortlänge $l(S) \leq \frac{H}{\log_2 D} + 1$.

2.6 Huffman-Code

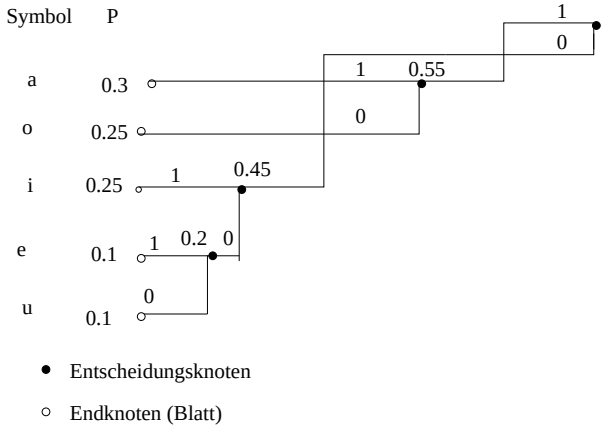
Nehmen wir einen reduzierten Wortschatz anstelle des kompletten Alphabets (z.B ein Baby, das nur die Vokale a, e, i, u, o von sich gibt). Die interessierten Eltern wollen vom Nebenzimmer hören, was ihr Baby für Geräusche macht. Das elektronische Gerät soll nun nur die Symbole a,e,i,o,u binär codieren. Folgende Wahrscheinlichkeitsverteilung sei gegeben:

Symbol	a	o	i	e	u
P(Symbol)	0.3	0.25	0.25	0.1	0.1

Die beiden kleinstwahrscheinlichsten Symbole werden nun zu einem Hilfssymbol zusammengefaßt, und dessen Wahrscheinlichkeit berechnet:

Symbol	a	o	i	(e/u)
P(Symbol)	0.3	0.25	0.25	0.2

Zuerst wird neu nach absteigender Wahrscheinlichkeit sortiert (hier bereits erfüllt). Dieser Schritt wir nun so oft wiederholt, bis ein Symbol mit Wahrscheinlichkeit 1 auftritt.
Vom obersten Entscheidungsknoten ausgehend wird jetzt der jeweils oberen Verzweigung der Wert 1, der jeweils unteren der Wert 0 zugeordnet. Jedes Blatt besitzt nun eine eindeutige Symbolfolge: Die Binärfolge beginnend von der Wahrscheinlichkeit 1 bis zum Symbol. Für den Beispielcode ergibt sich:



Symbol	a	o	i	e	u
Codewort	11	10	01	001	000

Offensichtlich ist dies ein Präfixcode. Zum Beispiel wird die Symbolfolge *11010100111000* in *aiioau* übersetzt. Die mittlere Wortlänge des Codes beträgt hier 2.4 bit/Symbol, die Entropie der Quelle ist $\sum_i p_i \log_2 p_i = 2.185$ bit/Symbol[4].
Spätestens zu Beginn einer Übertragung muß der Code feststehen. Ein Code, der nach den obigen Prinzipien aufgebaut ist, ist z.B. der MORSE-Code. Auch viele digitale Komprimierverfahren arbeiten nach diesem Prinzip. Da hier oft für jede Datei eine eigene Tabelle verwendet wird, ist es bei ähnlichen Daten daher sinnvoller, diese erst zu einer Einheit (Datei) zusammenzufassen.

[4]genaueres dazu z.B. im Vorlesungsskript Nachrichtentechnik [9]

3 Einzelne Quantensysteme

Im folgenden sei S ein Quantensystem das durch eine Basis von nur zwei orthogonalen Zuständen $|0\rangle$ und $|1\rangle$ im HILBERTraum $\mathcal{H}_2$ beschrieben wird. Beispielsweise sind folgende Systeme mögliche Realisationen hiervon:

- 2 Zustands-Atom. Hierbei werden aus einer großen Anzahl von Zuständen z.B. durch einen Laserübergang zwei Zustände ausgewählt, so daß

$$\begin{aligned} |0\rangle &= |n_0, l_0, m_0, s_0\rangle, \\ |1\rangle &= |n_1, l_1, m_1, s_1\rangle. \end{aligned}$$

- Die zwei Polarisationsrichtungen des Photons:

$$|0\rangle = |\leftrightarrow\rangle \quad \text{und} \quad |1\rangle = |\updownarrow\rangle.$$

  Entsprechend können auch links- und rechtszirkular polarisierte Photonen als Basiszustände dienen.

- Jedes Spin-$\frac{1}{2}$-Teilchen.

3.1 Reine Zustände

Ein reiner Zustand wird durch

$$\begin{aligned} |\psi\rangle &= C_0|0\rangle + C_1|1\rangle, \qquad C_1, C_2 \in \mathbb{C} \\ 1 &= |C_0|^2 + |C_1|^2 \end{aligned}$$

beschrieben. Beispiel:

$$\psi = \cos\left(\frac{\vartheta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\vartheta}{2}\right)|1\rangle \qquad \vartheta, \varphi \in [0, 2\pi)$$

Die Zustände lassen sich auch als „normale“ Vektoren darstellen:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad \rightsquigarrow |\psi\rangle = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix}$$

Im allgemeinen (s. insb. 3.2) erfolgt die Beschreibung jedoch über die Dichtematrix ρ, die in $\mathcal{H}_2$ wirkt. Es muß gelten

$$\rho \geq 0 \qquad \rho = \rho^\dagger \qquad \text{Spur}\,(\rho) = 1$$

d.h. ρ muß eine hermitesche, positiv definite[5] Matrix mit der Spur 1 sein. Für reine Zustände gilt zudem $\rho = \rho^2$ und ρ läßt sich als Projektor schreiben:

$$\begin{aligned} \rho &\equiv |\psi\rangle\langle\psi| = \begin{pmatrix} C_0 \\ C_1 \end{pmatrix} ({C_0}^*, {C_1}^*) = \begin{pmatrix} |C_0|^2 & C_0 C_1^* \\ C_1 C_0^* & |C_1|^2 \end{pmatrix} \\ \text{Spur}\,(\rho) &= |C_0|^2 + |C_1|^2 = 1, \qquad \rho^2 = |\psi\rangle \underbrace{\langle\psi|\psi\rangle}_{=1} \langle\psi| = \rho \end{aligned}$$

$\forall|\varphi\rangle \in \mathcal{H}_2$ gilt damit

$$\langle\varphi|\rho|\varphi\rangle \geq 0 \quad \Leftrightarrow \quad \text{Spur}\,(\rho P) \geq 0,$$

wie sich durch einsetzen leicht zeigen läßt.

3.2 Gemischte Zustände

Aus einer Quelle kommen Zustände $|\psi_1\rangle$,$|\psi_2\rangle$,$|\psi_3\rangle$ usw. mit den Wahrscheinlichkeiten $p_1, p_2, p_3, \ldots p \in \mathbb{R}_+$. Die Dichtematrix schreibt sich jetzt als

$$\rho = p_1|\psi_1\rangle\langle\psi_1| + p_2|\psi_2\rangle\langle\psi_2| + p_3|\psi_3\rangle\langle\psi_3| + \ldots \tag{1}$$

Auch hier gilt wieder

$$\begin{aligned} \rho &= \begin{pmatrix} q_{00} & q_{01} \\ q_{10} & q_{11} \end{pmatrix}, \qquad q_1, q_2 \in R,\ q_{00}^2 + q_{11}^2 = 1, q_{01} = q_{10}^* \\ \rightsquigarrow \rho &\geq 0,\ \text{Spur}\,(\rho) = 1,\ \text{und}\ \rho = \rho^\dagger, \end{aligned}$$

d.h. zur Beschreibung von ρ werden 3 Zahlen aus $\mathbb{R}$ benötigt.
Hiermit kann die VON NEUMANN-*Entropie* definiert werden:

$$S(\rho) = -\text{Spur}\,(\rho \log_2 \rho) = -\sum p_i \log_2 p_i$$

Hierbei sind die p_i die Eigenwerte von ρ.
Bei einem reinen Zustand $|\psi\rangle$ gibt es eine Basis, in der $|\psi\rangle = |1\rangle$ und somit $S = 0$ ist, d.h. ρ hat den Rank 1. Ein gemischter Zustand zeichnet sich dadurch aus, daß $S \neq 0$, so ist z.B. beim maximal gemischten Zustand

$$\rho_m = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) \qquad S(\rho_m) = -\sum_1^2 \frac{1}{2}\log_2\left(\frac{1}{2}\right) = 1.$$

[5] hier lax als $\rho \geq 0$ geschrieben

3.3 Operatoren

Die Operatoren

$$P_0 \equiv |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = P_0^2 \qquad \sigma_- \equiv |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
$$P_1 \equiv |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = P_1^2 \qquad \sigma_+ \equiv |1\rangle\langle 0| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

sind linear unabhängig und bilden daher in $\mathcal{H}_2$ eine Basis, d.h. jeder Operator kann als Linearkombination von P_0, P_1, σ_+ und σ_- geschrieben werden.
Es gilt

$$\begin{aligned} \sigma_+|0\rangle &= |1\rangle \qquad \text{Erzeugungsoperator} \\ \sigma_-|1\rangle &= |0\rangle \qquad \text{Vernichtungsoperator} \end{aligned}$$

Das Skalarprodukt zwischen den Operatoren A, B ist definiert als

$$\langle A, B\rangle = \text{Spur}\left(B^\dagger A\right) \qquad \|A\| = \sqrt{\langle A, A\rangle}.$$

Im allgemeinen wird eine andere Orthonormalbasis gewählt: die Pauli-Matrizen:

$$\begin{aligned} \mathbb{1} &= P_0 + P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \sigma_x &= \sigma_+ + \sigma_- = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= i\left(\sigma_+ - \sigma_-\right) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_z &= P_0 - P_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

Die σ_i sind idempotente, spurlose Matrizen, d.h. ihre Eigenwerte sind ± 1.
Sie erfüllen die Vertauschungsrelation

$$[\sigma_x, \sigma_y] = 2i\sigma_z$$

und sind zyklisch.
Damit läßt sich für jedes σ_i eine Eigenbasis finden:

$$|0\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad |0\rangle_y = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right) \qquad |0\rangle_z = |0\rangle$$
$$|1\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad |1\rangle_y = \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right) \qquad |1\rangle_z = |1\rangle$$

Damit ist $\sigma_i|0\rangle_i = +|0\rangle_i$ und $\sigma_i|1\rangle_i = -|1\rangle_i$.
Um Spins in beliebige Richtungen beschreiben zu können, wird eine verallgemeinerte PAULI-Matrix

$$\sigma_{\vec{n}} \quad = \quad \vec{\sigma} \cdot \vec{n} \qquad \sigma^T = (\sigma_x, \sigma_y, \sigma_z)$$

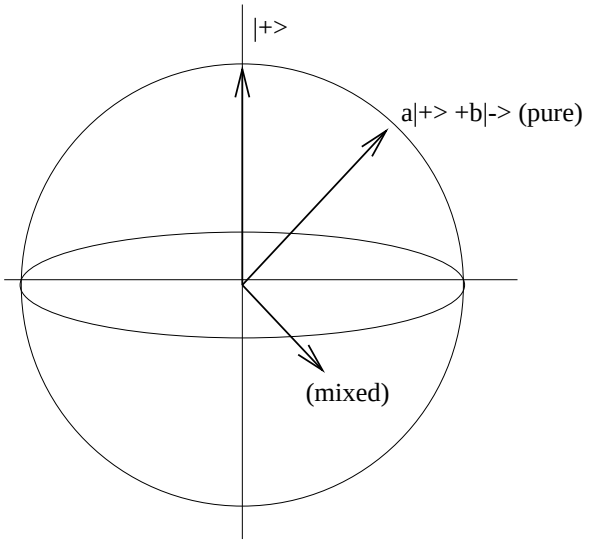
Auch $\sigma_{\vec{n}}$ ist idempotent mit Eigenwerten ± 1.
Damit kann ρ in der PAULI-Basis entwickelt werden:

$$\rho = \frac{1}{2} \sum_{i=0}^{3} \lambda_i A_i \qquad A_i = \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\},\ \lambda_0 = 1,\ \lambda_i = \text{Spur}\,(\rho A_i)$$

Aus $\lambda_0 = 1$ folgt $\text{Spur}\,(\rho) = 0$. Die anderen drei Parametern λ_i sind in einer Messung die Erwartungswerte der Spinoperatoren in die drei Raumrichtungen, und daher reell:

$$\langle \sigma_x \rangle = \lambda_1, \langle \sigma_y \rangle = \lambda_2, \langle \sigma_z \rangle = \lambda_3$$

Durch Einsetzen kann leicht überprüft werden, daß $\text{Spur}\,(\rho^2) = 1 \Leftrightarrow \lambda_1^2 + \lambda_2^2 + \lambda_3^2 = 1 \Leftrightarrow \rho$ ist reiner Zustand. Ansonsten ist $\text{Spur}\,(\rho^2) < 1$. Geometrisch bedeutet dies, daß reine Zustände auf der Oberfläche der von den λ_i aufgespannten Kugel liegen, während gemischte Zustände sich im inneren befinden. Damit wird auch sofort offensichtlich, daß gemischten Zuständen viel häufiger sind.



3.4 Observable

Observablen entsprechen selbstadjungierte (oder „hermitesche“) Operatoren, d.h. $B = B^\dagger$ mit

$$\begin{aligned} B &= \frac{1}{2}\sum_{i=0}^{3} b_i A_i \qquad \{A_i\} = \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\},\ b_i \equiv \text{Spur}\,(BA_i) \\ B &= \begin{pmatrix} B_{00} & B_{01} \\ B_{10} & B_{11} \end{pmatrix} \end{aligned}$$

3.5 Messungen

Allgemeine Messungen überführen den zu messenden Zustand in einen Eigenzustand des Meßoperators. In unseren Anwendungen ist dieser Operator ein Projektor, d.h. $P^2 = P$ und $P = P^\dagger$ mit den zwei Eigenwerten $\{0, 1\}$, die damit z.B. „ja“ oder „nein“ entsprechen können:

$$\begin{aligned} \text{ja} &: \rho \to \frac{P\rho P}{\text{Spur}\,(P\rho P)} \\ \text{nein} &: \rho \to \frac{(1-P)\rho(1-P)}{\text{Spur}\,(P\rho P)} \end{aligned}$$

$1 - P$ wird auch als Q abgekürzt und ist der zu P komplementäre Operator in dem Sinne, daß

$$QP|\psi\rangle = (1-P)P|\psi\rangle = 0$$

Q projeziert also auf den Unterraum, der $\perp$ zum Unterraum von P steht.
Der Erwartungswert einer physikalischen Größe errechnet sich damit als $\langle B\rangle = \text{Spur}\,(B\rho)$. Diesen Erwartungswert kann natürlich nicht in *einer* singulären Messung erhalten werden, sondern erst nachdem viele Messungen an dem Teilchenensemble durchgeführt wurden. Man kann sich das gemischte Ensemble als einen Kasten aus einer großen Anzahl Teilchen vorstellen, von denen man nicht weiß, ob sie sich in dem Zustand $|-\rangle$ oder $|+\rangle$ befinden. Ein reiner Zustand entspricht einem Ensemble, bei dem von allen Teilchen bekannt ist, in welchem Zustand sie sich befinden, z.B. $|+\rangle$. Zwar kann auch hier der Meßausgang einer Einzelmessung stochastisch sein - wenn zum Beispiel den Spin in einer Richtung zu der $|+\rangle$ nicht Eigenzustand gemessen werden soll. Wenn aber die „richtige Frage“ gestellt wird (d.h. den Spin in der Richtung mißt, zu der $|+\rangle$ Eigenzustand ist), so ergibt sich beim reinem Zustand *immer* dieselbe Antwort: up. Dies wird auch „maximum quantum test“ genannt.

Beim Gemisch ist das nicht der Fall. Selbst in der „richtigen“ Richtung wird mal „up“ und mal „down“ erhalten: der Zustand ist ein Mischung. Die Wahrscheinlichkeiten, mit der die einzelnen Zustände in dem Gemisch vertreten sind, ergeben sich aus der relativen Häufigkeit des Meßausganges bei der „richtigen“ Fragestellung, wenn viele Teilchen gemessen. Diese Wahrscheinlichkeiten p_i zusammen mit den vertretenen Zuständen ergeben den Gesamtzustand eines Systems: folglich Gleichung (1).

3.6 Zeitentwicklung

In abgeschlossenen Systemen kann die Zeitentwicklung durch eine unitären Operator beschrieben werden (Zeitumkehr). Bei offenen Systemen kommt es aber zu *Zerfallsprozessen* (Energieaustausch) und *Kohärenzverlust* (Phasenverlust). In vielen Systemen ist der Kohärenzverlust der problematischere Einfluß der Umwelt[6]. Kohärenzverluste spielen sich in Zeiträumen von ca. 10^{-12} s ab, während Dissipation, d.h. Energieaustausch (=spontane Strahlung), im Bereich von 10^{-9} s liegt. Zwei Fälle werden grundsätzlich unterschieden:

3.6.1 Isolierte Quantensysteme

In isolierten Sytemen ist die Zeitentwicklung unitär:

$$|\psi(t_2)\rangle = U(t_2, t_1)|\psi(t_1)\rangle$$

U ist dabei ein unitärer Operator, d.h. U ist invertierbar und U erhält die Norm:

$$\langle\psi|U^+U|\psi\rangle = \langle\psi|\psi\rangle \quad \Rightarrow U^+U = UU^+ = 1$$

Das gleiche gilt bei einer $2 \otimes 2$-Darstellung der Operatoren für die entsprechenden Matrizen. Der unitäre Zeitentwicklungsoperator U läßt sich aus dem HAMILTONoperator gewinnen, falls H nicht explizit zeitabhängig ist:

$$U = \exp(-i\frac{Ht}{\hbar})$$

Damit läßt sich die zeitabgeleitete Form der obigen Gleichung angeben als:

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H(U)|\psi(t)\rangle$$

[6]Z.B bei Femtosekunden-Lasern ist der Zerfall auf Zeitskalen von 10^{-9} s total irrelevant

H ist hermitesch, und es ist Spur (H) =0, also ist die Determinante von $U = 1$.
Die Zeitentwicklung eines Gemisches wird durch die VON-NEUMANN-Gleichung beschrieben:

$$i\hbar\partial_t\rho = [H(t), \rho]$$

Im $\mathcal{H}_2$ ist der HAMILTONoperator entwickelbar in der Basis $\{\mathbb{1}, \sigma_i\}$, so daß er sich schreiben läßt als

$$H(t) = \frac{\hbar}{2}\sum n_i(t)A_i$$

Falls H nicht von der Zeit abhängt, sind die $n_i(t) = n_i = const.$, so daß sich mit $\omega = \frac{1}{2}\sqrt{n_1^2 + n_2^2 + n_3^2}$ und $\vec{n} = \frac{(n_1,n_2,n_3)}{\sqrt{n_1^2+n_2^2+n_3^2}}$ ergibt:

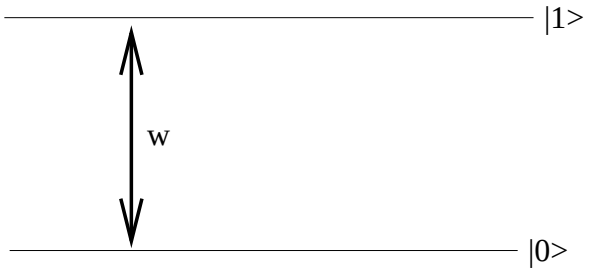
$$H = \hbar\omega\vec{n}\cdot\vec{\sigma} + \frac{\hbar n_0}{2}\mathbb{1}$$

Mit der Abkürzung $\vec{\sigma}_{\vec{n}} = \vec{n}\vec{\sigma}$ lautet die Lösung der SCHRÖDINGER-Gleichung dann:

$$\begin{aligned} U(t) &= e^{-i\frac{Ht}{\hbar}} = e^{-i\omega\vec{\sigma}_{\vec{n}}} = \cos(\omega_{\vec{n}}t) - i\sin(\omega\vec{\sigma}_{\vec{n}}t) \\ &\overset{\vec{\sigma}_{\vec{n}}^2=\mathbb{1}}{=} \mathbb{1}\cos(\omega t) - i\vec{\sigma}_{\vec{n}}\sin(\omega t) \end{aligned}$$

Ein Beispiel für einen solchen HAMILTONian, der die zeitliche Entwicklung eines 2-Zustandssystems beschreibt, ist der in der Quantenoptik sehr oft verwendete

$$H = \frac{\hbar}{2}\Delta\sigma_z + \frac{\hbar\Omega}{2}(\sigma_+ e^{i\phi} + \sigma_- e^{-i\phi})$$



mit ω_L: Laserfrequenz, ω_0: Übergangsfrequenz, $\Delta = \omega_L - \omega_0$: Verstimmung, $\hbar\Omega$: Dipolmatrixelement des Übergangs, $e^{i\phi}$: Phase des elektrischen Feldes. Im resonanten Fall ($\Delta = 0$) ergibt sich als Lösung:

$$U(t) = \begin{pmatrix} \cos(\frac{\Omega t}{2}) & -i\sin(\frac{\Omega t}{2})e^{-i\phi} \\ i\sin(\frac{\Omega t}{2})e^{i\phi} & \cos(\frac{\Omega t}{2}) \end{pmatrix}$$

Das zeitliche Verhalten sind die bekannten RABI-Oszillationen zwischen dem oberen und unteren Niveau, Ω bezeichnet die RABI-Frequenz.

3.6.2 Nichtisolierte (offene) Quantensysteme

Offene Quantensysteme wechselwirken per Definition mit der Umgebung. Dabei sind zwei Phänomene zu unterscheiden:

Zerfall = Dissipation

Spontane Emission eines Photons durch ein Atom beruht auf Wechselwirkung des Atoms mit der Umgebung, nämlich dem Vakuum. Das Photon geht in einen Mode des elektromagnetischen Feldes. Solche Wechselwirkungen können unterbunden werden, wenn man entweder einen verbotenen Dipolübergang betrachtet oder man dem Atom keinen Mode anbietet, in den es ein Photon passender Energie abstrahlen kann. Dadurch kann effektiv eine Wechselwirkung des Systems mit der Umgebung verhindert werden. Lebensdauern verbotener Übergänge im Sekundenbereich sind keine Seltenheit. Ein Zerfall modifiziert die Diagonalelemente von ρ, die den Besetzungszahlen entsprechen.

Dekohärenz

Anders als bei Dissipation findet bei Dekohärenz kein Energieaustausch des Systems mit der Umgebung statt. Stattdessen verteilen sich die Phasen einzelner Quantensuperpositionen sehr schnell zufällig über den gesamten Bereich. Dieser Effekt führt auch zum Paradoxon der SCHRÖDINGERschen Katze und den ihrer modernen Nachfolgern. Dekohärenz modifiziert die Nichtdiagonalelemente von ρ, die Kohärenzen.

3.7 Diskrete Zeitentwicklung

Betrachten wir die Zeitentwicklung eines Zustandes diskretisiert. Der Zustand sei $|0\rangle$. Zwei äquivalente Darstellungen sind

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cong |0\rangle \cong \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Eine diskrete Zeittransformation ist z.B. durch

$$U_A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = U_A^T = U_A^{-1} = U_A^+$$

gegeben. Das letzte Gleichheitszeichen bedeutet Unitarität.
N.B.: Diese Matrix ergibt sich aus $U_A = U_{A,2} U_{A,1}$ wobei

$$U_1 = \frac{1}{\sqrt{2}} = i\vec{\sigma}\vec{n}\sin(\frac{\theta_1}{2}), \qquad \vec{n} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \theta_1 = \frac{\pi}{2}$$

eine Drehung um 90 Grad um den Raumrichtungsvektor $\vec{n}$ und

$$U_2 = -i\mathbb{1} = i\vec{\sigma}\vec{n}\sin(\frac{\theta_2}{2}), \qquad \vec{n} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad \theta_2 = \pi$$

eine Drehung entlang der z-Achse um $\theta_2 = \pi$ darstellt.
Mit einem solchen diskreten Zeitschritt wird

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \overset{U_A}{\mapsto} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

oder in Matrixschreibweise:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \overset{U_A}{\mapsto} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Dann folgt

$$\frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \overset{U_A}{\mapsto} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \Rightarrow \quad \rho_{\text{final}} = \rho_{\text{initial}}$$

Dekohärenz beeinflußt die Nichtdiagonalelemente im Zwischenschritt:

$$\rho_{\text{in}} \overset{U_A}{\mapsto} \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \overset{\text{dec}}{\mapsto} \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \overset{U_A}{\mapsto} \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \rho_{\text{fin}} \quad \Rightarrow \quad \rho_{\text{fin}} \neq \rho_{\text{in}}$$

Die Eigenwerte ändern sich also von $\{0, 1\}$ nach $\{\frac{1}{2}\}$. Damit ist die Operation nicht mehr unitär, denn unitäre Operationen ändern das Spektrum (die Eigenwerte) nicht. Als ein Beispiel soll das 2-Niveausystem zusammen mit seiner Umgebung dienen:

$$|0\rangle, \quad |1\rangle, \quad |E\rangle$$

Da System und Umgebung zusammen isoliert sind, ist die gemeinsame Zeitentwicklung von (S+E) unitär. Der Zustand läßt sich als Produktzustand schreiben:

$$|0\rangle \otimes |E\rangle \overset{U}{\mapsto} |0\rangle \otimes |E_{00}\rangle + |1\rangle \otimes |E_{01}\rangle$$

$$|1\rangle \otimes |E\rangle \overset{U}{\mapsto} |0\rangle \otimes |E_{10}\rangle + |1\rangle \otimes |E_{11}\rangle$$

Unitäre Zeitentwicklung bedeutet, daß das Skalarprodukt invariant gelassen wird. Daraus ergibt sich (mit $\langle E|E\rangle = 1$) als Bedingung:

$$1 = (\langle 0| \otimes \langle E|)(|0\rangle \otimes |E\rangle) \overset{\text{uni}}{=} \langle E_{00}|E_{00}\rangle + \langle E_{01}|E_{01}\rangle = 1$$

und ebenso aus der zweiten Zeile

$$\langle E_{10}|E_{10}\rangle + \langle E_{11}|E_{11}\rangle = 1$$

und aus dem Vergleich der beiden

$$\langle E_{00}|E_{10}\rangle + \langle E_{01}|E_{11}\rangle = 0$$

Betrachten wir jetzt konkret einen reinen Zustand des Untersystems und den des dazugehörigen des Gesamtsystems:

$$|\phi\rangle = c_0|0\rangle + c_1|1\rangle, \quad |\xi\rangle = |\phi\rangle \otimes |E\rangle$$

Die unitäre Entwicklung ergibt:

$$\begin{aligned} |\xi\rangle \overset{U}{\mapsto} |\xi'\rangle &= c_0(|0\rangle \otimes |E_{00}\rangle + |1\rangle \otimes |E_{01}\rangle) + c_1(|0\rangle \otimes |E_{10}\rangle + |1\rangle \otimes |E_{11}\rangle) \\ &= |0\rangle \otimes (c_0|E_{00}\rangle + c_1|E_{10}\rangle) + |1\rangle \otimes (c_0|E_{01}\rangle + c_1|E_{11}\rangle) \end{aligned}$$

Die Dichtematrix transformiert in:

$$\rho_{\text{in}} = |\xi\rangle\langle\xi| \overset{U}{\mapsto} |\xi'\rangle\langle\xi'| = \rho'$$

ρ' sieht explizit wie folgt aus ($|E\rangle$ ohne, $|0\rangle, |1\rangle$ in Basisdarstellung):

$$\rho' = \begin{pmatrix} c_0c_0^*|E_{00}\rangle\langle E_{00}| + c_1c_1^*|E_{10}\rangle\langle E_{10}| + c_0c_1^*|E_{00}\rangle\langle E_{10}| + c_0^*c_1|E_{10}\rangle\langle E_{00}| & \dots \\ \dots & \dots \end{pmatrix}$$

Die Zustände der Umgebung werden aber per Definition nicht gemessen. Das meßbare Ensemble beschränkt sich auf die reduzierte Matrix $\rho'_s = \text{Spur}\,(\rho')_E$, die Dichtematrix die sich ergibt, wenn über die Untermatrix von $|E\rangle$ die Spur gebildet wird. Der oben dargestellte Matrixausschnitt entspricht $\langle 0|\rho'|0\rangle$, dieser Ausschnitt für die reduzierte Matrix ρ'_s ist[7]:

$$\langle 0|\rho'_s|0\rangle = |c_0|^2\langle E_{00}|E_{00}\rangle + |c_1|^2\langle E_{10}|E_{10}\rangle + c_0c_1^*\langle E_{10}|E_{00}\rangle + c_0^*c_1\langle E_{00}|E_{10}\rangle$$

Da $\text{Spur}\,(\rho'_s) = 1$ folgt

$$\langle 1|\rho'_s|1\rangle = 1 - \langle 0|\rho'_s|0\rangle$$

Außerdem gilt für die Nichtdiagonalelemente:

$$\langle 0|\rho'_s|1\rangle = |c_0|^2\langle E_{01}|E_{00}\rangle + |c_1|^2\langle E_{11}|E_{10}\rangle + c_0^*c_1\langle E_{01}|E_{10}\rangle + c_0c_1^*\langle E_{11}|E_{00}\rangle$$

[7]Beachte: Spur $(|A\rangle\langle A|)$=Spur $(\langle A|A\rangle)$=$\langle A|A\rangle$Spur (1)=$\langle A|A\rangle$

ρ_{in} entspricht einem reinen Zustand, ρ'_s bildet jedoch ein Gemisch (überprüfe durch $(\rho'_s)^2 \neq \rho'_s$). Die Nichtdiagonalterme wie $\langle 0|\rho'_s|1\rangle$, also die Kohärenzen zwischen System und Umgebung, gehen schnell gegen Null. So entwickelt sich die Dichtematrix des (Unter-)Systems im Laufe der Zeit zu einer Diagonalmatrix mit klassischen Wahrscheinlichkeiten für die verschiedenen Zustände[8] Ein Spezialfall tritt ein, falls alle $|E_{ij}\rangle$ senkrecht aufeinander stehen. Dann folgt $\langle 0|\rho'_s|0\rangle = |c_0|^2 + |c_1|^2 = 1$.[9]

[8] dies entspricht der modernen Beschreibung für den Meßprozeß und den Übergang von Amplituden in klassische Wahrscheinlichkeiten für einen Zustand nach der Messung.

[9] Messung eines Eigenzustandes ?

4 Zusammengesetzte Quantensysteme

4.1 Notation

Die beiden Teilsysteme seien mit A[10] und B[11] bezeichnet. Die zugehörigen HILBERTräume sind $\mathcal{H}_A$ und $\mathcal{H}_B$, der Gesamtraum $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Die Dimension dieses Raumes ist $N = N_A \cdot N_B$. Beispiele dafür sind zwei 2-Niveau-Atome, zwei Spin $\frac{1}{2}$-Teilchen oder zwei Photonen in zwei Moden des EM-Feldes. Um eine Definition für Verschränkung sauber zu notieren, sollen zunächst unterschiedliche Schreibweisen aufgeführt werden. Es handelt sich immer um zweidimensionale Teilsysteme. Daher ist die Dimension des Gesamtraumes 4. Eine Basis in diesem vierdimensionalen Raum stellen die folgenden Vektoren dar:

$$\{|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B\}$$

Eine Darstellungsart ergibt sich aus der üblichen Spaltenschreibweise und anschließender Umschreibung:

$$|0\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_A \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_B = \begin{pmatrix} 1 = a_0 b_0 \\ 0 = a_0 b_1 \\ 0 = a_1 b_0 \\ 0 = a_1 b_1 \end{pmatrix} \overset{oder}{=} |0,0\rangle \overset{oder}{=} |0\rangle_{\mathcal{H}_4}$$

Für die zweite Kombination ergibt sich:

$$|0\rangle_A \otimes |1\rangle_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_A \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_B = \begin{pmatrix} 0 = a_0 b_0 \\ 1 = a_0 b_1 \\ 0 = a_1 b_0 \\ 0 = a_1 b_1 \end{pmatrix} \overset{oder}{=} |0,1\rangle \overset{oder}{=} |1\rangle_{\mathcal{H}_4}$$

In der letzten Darstellungsweise wird bis 3 gezählt.

4.2 Reine Zustände

Ein reiner Zustand wir durch

$$|\psi\rangle = c_{00}|0,0\rangle + c_{01}|0,1\rangle + c_{10}|1,0\rangle + c_{11}|1,1\rangle$$

dargestellt. Dabei gilt, daß die Koeffizienten bis auf einen (irrelevanten) globalen Phasenfaktor der Beziehung

$$\sum_{i,j=0}^{1} c_{ij}^2 = 1$$

[10] oft auch als Alice bezeichnet
[11] der männliche Vertreter Bob

genügen. Damit läßt sich z.B c_{00} immer reell schreiben und es ergeben sich insgesamt 6 reelle Parameter (3 komplexe, 1 reeller, -1 Bedingung).
Somit ist[12]

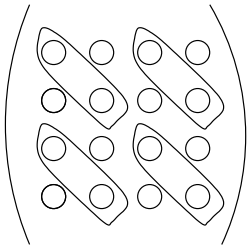
$$\rho = \begin{pmatrix} |c_{00}|^2 & c_{00}c_{01}^* & \cdots & \\ c_{00}^* c_{01} & |c_{01}|^2 & & \\ \vdots & & |c_{10}|^2 & \\ & & & |c_{11}|^2 \end{pmatrix}.$$

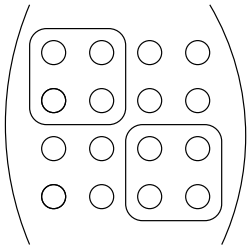
Wichtig ist auch die reduzierte Dichtematrix:

$$\rho_A = \text{Spur}\,(\rho)_B = \sum_{i_B} \langle \vartheta_i^B | \rho | \vartheta_i^B \rangle$$

$$\rho_B = \text{Spur}\,(\rho)_A = \sum_{i_A} \langle \vartheta_i^A | \rho | \vartheta_i^A \rangle$$

Bei den von uns betrachteten Systemen (d.h. in einer 2×2 Basis) ist

$\rho =$  $\rightsquigarrow \rho_A = \begin{pmatrix} \rho_A^{00} & \rho_A^{01} \\ \rho_A^{10} & \rho_A^{11} \end{pmatrix}$

$\rho =$  $\rightsquigarrow \rho_B = \begin{pmatrix} \rho_B^{00} & \rho_B^{01} \\ \rho_B^{10} & \rho_B^{11} \end{pmatrix}$

Da es sich hier um reine Zustände handelt ist

$$\rho = |\psi\rangle\langle\psi| \quad \text{mit} \quad \rho^2 = \rho, \text{Spur}\left(\rho^2\right) = 1$$

Die reduzierten Dichtematrizen werden jedoch im allgemeinen gemischte Zustände darstellen, d.h.

$$\text{Spur}\left(\rho_A^2\right) < 1 \qquad \text{Spur}\left(\rho_B^2\right) < 1$$

Lemma 2 *Für jeden gemischten Zustand ρ_A existiert ein reiner Zustand $\rho = |\psi\rangle\langle\psi|$ derart, daß*

$$\rho_A = \mathit{Spur}\,(\rho)_B$$

[12] s. hierzu auch Anhang A

4.3 Unkorrelierte (Produkt-)Zustände

Zustände der Form

$$|\psi\rangle = |\psi^A\rangle \otimes |\psi^B\rangle \qquad (\ \Rightarrow\ \rho = \rho_A \otimes \rho_B)$$

heißen *Produkt-Zustände*. Werden die Zustände durch Basisvektoren ausgedrückt, d.h.

$$\begin{aligned} |\psi^A\rangle &= c_0^A|0\rangle_A + c_1^A|1\rangle_A \\ |\psi^B\rangle &= c_0^B|0\rangle_B + c_1^B|1\rangle_B \\ \rightsquigarrow |\psi\rangle &= \begin{pmatrix} c_0^A c_0^B \\ c_0^A c_1^B \\ c_1^A c_0^B \\ c_1^A c_1^B \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} \end{aligned}$$

ergibt sich daraus die Bedingung

$$\Leftrightarrow z_1 z_4 - z_2 z_3 = 0$$

Weitere Eigenschaften der Produktzustände/vektoren:

1. Produktvektoren sind eine Menge mit Maß Null (Punktmenge)
2. Produktvektoren formen *keinen* linearen Unterraum
3. Aus $\rho = |\psi\rangle\langle\psi|$ folgt $\rho_{A,B} = |\psi_{A,B}\rangle\langle\psi_{A,B}|$ ist ein reiner Zustand

4.4 Verschränkte Zustände

Alle Zustände, die sich nicht als Produktzustände darstellen lassen, heißen *verschränkte Zustände:*

$$\nexists |\psi^A\rangle, |\psi^B\rangle \ : \ |\psi\rangle = |\psi^A\rangle \otimes |\psi^B\rangle$$

Physikalisch bedeutet dies, daß Quantenkorrelationen vorliegen. Die beteiligten Teilchen (z.B. Spin-$\frac{1}{2}$-Teilchen) werden auch „EPR[13]“-Teilchen genannt. Zum Beispiel läßt sich

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

[13] Einstein-Podolsky-Rosen

nicht als Produktzustand schreiben.
Verschränkte Zustände liegen dicht im HILBERTraum und können daher eine Basis bilden, z.B. die BELL-Basis:

$$\begin{aligned} |\psi^{\mp}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \mp |10\rangle\right) \\ |\phi^{\mp}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \mp |11\rangle\right) \end{aligned}$$

Alle Zustände, die durch beliebige lokale Transformationen aus dieser Basis hervorgehen, d.h.

$$|\psi\rangle = U_A \otimes U_B \begin{cases} |\psi^{\pm}\rangle \\ |\phi^{\pm}\rangle \end{cases}$$

sind *maximal verschränkt*. Desweiteren gibt es die GHZ[14]-Zustände. Dies sind Zustände in höherdimensionalen Räumen:

$$\frac{1}{\sqrt{2}}(|\underbrace{000\ldots0}_{n}\rangle - |\underbrace{111\ldots1}_{n}\rangle)$$

4.5 Schmidt Orthogonalisierung

Im Produktraum $\mathcal{H} = H_A \otimes H_B$ mit den Dimensionen N_A, N_B läßt sich jeder Zustand als Summe von Produktzuständen schreiben

$$\begin{aligned} |\psi\rangle &= \sum_{i=1}^{\min(N_A,N_B)} \lambda_i |u_i^A\rangle \otimes |u_i^B\rangle \qquad \text{mit} \\ \langle u_i|u_j\rangle &= \delta_{ij} \end{aligned}$$

Betrachte z.B.

$$|\phi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Die reduzierte Dichtematrix ergibt sich mit

$$\begin{aligned} |\psi\rangle &= \sum \lambda_i |u_i\rangle|v_i\rangle, \qquad \rho = |\psi\rangle\langle\psi| \text{ zu} \\ \text{Spur}\,(\rho)_B &= \sum \lambda_i^2 |u_i\rangle\langle u_i| \\ \text{Spur}\,(\rho)_A &= \sum \lambda_i^2 |v_i\rangle\langle v_i| \end{aligned}$$

[14] GREENBERGER, HORNE, ZEILINGER

Da die Zustände normiert sind, ist

$$1 = \langle\psi|\psi\rangle \quad \Rightarrow \quad \sum_i \lambda_i^2 = 1$$

Bei den maximal verschränkten Zuständen, den BELL-*Zuständen*, ist

$$\text{Spur}\,(\rho)_{A,B} \quad = \quad \frac{1}{2}\mathbb{1}_{A,B}$$

Es sind äquivalent:

1. $|\psi\rangle$ ist ein Produktvektor.
2. $|\psi\rangle$ hat nur einen Term in der SCHMIDT-Zerlegung.
3. ρ_A, ρ_B entsprechen reinen Zuständen.

Bei reinen Zuständen kann als Maß für die Verschränkung die Entropie der Subsysteme genommen werden, d.h.

$$E(|\psi\rangle) = S(\rho_A) = S(\rho_B)$$

Wenn $|\psi\rangle$ ein Produktzustand ist, dann ist $\rho_{A,B}$ ein reiner Zustand und damit die Entropie E gleich null.

4.6 Gemischte Zustände

Bei gemischten Zuständen lautet die Dichtematrix

$$\rho \quad = \quad \sum_{i=0}^{3}\sum_{j=0}^{3}\sum_{k=0}^{3}\sum_{l=0}^{3} \rho_{ij}^{kl}|i\rangle_A\langle j| \otimes |k\rangle_B\langle l| = \sum_{ij}^{3} \rho^{ij}|i\rangle_{AB}\langle j|$$

ρ läßt sich in diesem Fall in die hermitesche Basis der PAULI-Operatoren im Raum der 4×4 Matrizen entwickeln:

$$\begin{aligned}\{A_i\}_{i=0,\ldots,15} \quad = \quad & \{\mathbb{1}_4, \sigma_x \otimes \mathbb{1}_2, \sigma_y \otimes \mathbb{1}_2, \sigma_z \otimes \mathbb{1}_2, \mathbb{1}_2 \otimes \sigma_x, \mathbb{1}_2 \otimes \sigma_y, \mathbb{1}_2 \otimes \sigma_z, \\ & \sigma_x \otimes \sigma_x, \sigma_x \otimes \sigma_y, \sigma_x \otimes \sigma_z, \sigma_y \otimes \sigma_x, \sigma_y \otimes \sigma_y, \sigma_y \otimes \sigma_z, \\ & \sigma_z \otimes \sigma_x, \sigma_z \otimes \sigma_y, \sigma_z \otimes \sigma_z\}\end{aligned}$$

In dieser Basis läßt sich die Dichtematrix jetzt als

$$\rho = \frac{1}{4}\sum_{i=0}^{15} \lambda_i A_i \quad \text{mit} \quad \lambda_0 = 0,\ \lambda_i = \text{Spur}\,(\rho A_i)$$

schreiben, wobei in dieser Basis die λ_i zudem reell sind.
Drei Fälle müssen jetzt unterschieden werden:

- Unkorrelierte Zustände

$$\rho = \rho_A \otimes \rho_B \qquad\qquad \rho = \text{Spur}\,(\rho)_A \otimes \text{Spur}\,(\rho)_B\,,$$

  dabei müssen ρ_A und ρ_B keine reinen Zustände sein. Während der Zustandspräparation findet kein Informationsaustausch zwischen den Teilsystemen statt.

- Separierbare Zustände

$$\rho = \sum_k \Lambda_k \rho_A^k \otimes \rho_B^k \qquad\qquad \sum \Lambda_k = 1,\ \Lambda_i \geq 0$$

  Die Λ_i können als (klassische) Wahrscheinlichkeiten verstanden werden, d.h. während der Zustandspräparation findet ein *rein klassischer* Informationsaustausch statt.

- Nicht separierbare Zustände, z.B.

$$\rho = f|\psi^+\rangle\langle\psi^+| + (1-f)|\phi^+\rangle\langle\phi^+|$$

Die nicht seperierbaren Zustände sind theoretisch am schwierigsten zu betrachten. In Räumen der Dimension $N \times M$ mit $N \cdot M \geq 6$ ist das *Seperierbarkeitskriterium* noch ein offenes Problem, siehe dazu [7] für eine eher physikalische bzw. [8] für eine eher mathematische Betrachtung.
Um ein solches Kriterium zu finden, wird der Begriff der *Teiltranspositon* benötigt.

Def. 9 *Teiltransposition:*

$$\rho = \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix} \Rightarrow \begin{cases} \rho^{T_A} & = \begin{pmatrix} A & B^\dagger \\ B & C \end{pmatrix} \\ \rho^{T_B} & = \begin{pmatrix} A^T & B^T \\ (B^\dagger)^T & C^T \end{pmatrix} \end{cases}, \left(\rho^{T_A}\right)^{T_B} = \rho^T$$

Mit Ket- und Bravektoren geschrieben heißt das:

$$\begin{aligned} \rho &= {}_A\langle 0|\rho|0\rangle_A|0\rangle_A\langle 0| + {}_A\langle 0|\rho|1\rangle_A|0\rangle_A\langle 1| + \\ &\quad {}_A\langle 1|\rho|0\rangle_A|1\rangle_A\langle 0| + {}_A\langle 1|\rho|1\rangle_A|1\rangle_A\langle 1| \\ \rho^{T_A} &= {}_A\langle 0|\rho|0\rangle_A|0\rangle_A\langle 0| + {}_A\langle 0|\rho|1\rangle_A|1\rangle_A\langle 0| + \\ &\quad {}_A\langle 1|\rho|0\rangle_A|0\rangle_A\langle 1| + {}_A\langle 1|\rho|1\rangle_A|1\rangle_A\langle 1| \end{aligned}$$

Bei dieser Operation geht σ_y^A über in $-\sigma_y^A$, d.h. die Operation ist eine antiunitäre Transformation im A-Raum, sie entspricht einer Zeitumkehr (nur im A-Raum!)
Damit läßt sich in unserem Fall ein Seperierbarkeitskriterium finden:

Theorem 8 *ρ im Raum $\mathcal{H}_2 \otimes \mathcal{H}_2$ ist separierbar $\Leftrightarrow \rho^{T_A} \geq 0 \Leftrightarrow \rho^{T_B} \geq 0$*

Mit anderen Worten: Wenn bei (genau) einem der Subsysteme die Zeit umgekehrt wird und die entstehende Dichtematrix immer noch physikalische Bedeutung besitzt, dann ist die Dichtematrix des Gesamtsystemes seperierbar.
Wichtig: Das Separierbarkeitskriterium in 2×3-Dimensionen funktioniert *nicht* in höheren Dimensionen:

$$\begin{aligned} \rho &= \sum \Lambda_k |e_k, f_k\rangle\langle e_k, f_k| \\ \rho^{T_B} &= \sum \Lambda_k |e_k, f_k^*\rangle\langle e_k, f_k^*| \end{aligned}$$

Damit gilt zwar noch die Beziehung ρ separierbar $\Rightarrow \rho^{T_A} \geq 0$, aber es gibt Zustände, bei denen $\rho^{T_A} \geq 0$ erfüllt ist, die aber dennoch verschränkt sind.
Messung der Verschränktheit hier z.B. nach [10]; eine allgemeine Definition ist noch nicht gelungen. Die hier betrachtete Meßmethode heißt auch *Formationsmessung*. Hierbei wird von allen möglichen Zerlegung von ρ ausgegangen:

$$\begin{aligned} \rho = \sum p_i |\psi_i\rangle\langle\psi_i| \qquad & \sum p_i = 1 \\ E(\rho) = \min_{\{p_i,\psi_i\}} \sum_i p_i E(|\psi\rangle) \quad = \quad & \min_{\{p_i,\psi_i\}} \sum_i p_i S(\text{Spur}\,(|\psi_i\rangle\langle\psi_i|)_A) \end{aligned}$$

Wie dieses Minimum im allgemeinen Fall gefunden werden kann, ist noch nicht geklärt.

4.7 Observable und Messungen

Auch hier ist wieder jeder Observablen q ein hermitescher Operator O zugeordnet[15], der sich wieder als

$$O = \frac{1}{4} \sum_{i=0}^{15} o_i A_i \quad \text{mit} \quad o_i = \text{Spur}\,(OA_i)$$

schreiben läßt. Vier Typen von Messungen können jetzt unterschieden werden:

[15] Die Darstellung ist jetzt natürlich eine 4×4 Matrix

- Lokale Messungen, d.h. entweder A oder B messen:

$$O = O_A \otimes \mathbb{1}_B \quad \text{bzw.} \quad O = \mathbb{1}_A \otimes O_B$$

Das Ergebnis der lokalen Messung wird von der reduzierten Dichtematrix bestimmt:

$$\begin{aligned} \text{Spur}\,(\rho O) = \text{Spur}\,(\text{Spur}\,(\rho O)_B)_A &= \text{Spur}\,(\text{Spur}\,(\rho)_B\, O_A)_A \\ &= \text{Spur}\,(\rho_A O_A)_A \end{aligned}$$

- Korrelationsmessungen, d.h. A und B messen gleichzeitig aber unabhängig voneinander:

$$O = O_A \otimes O_B$$

Bei Produktzuständen ergibt sich damit

$$\text{Spur}\,(O\rho_A \otimes \rho_B) = \langle O \rangle = \langle O_A \rangle \cdot \langle O_B \rangle$$

- Nicht lokale Messungen[16]

$$O \neq O_A \otimes O_B \quad \text{z.B.} \quad \sigma_x^A \sigma_y^B + \sigma_y^A \sigma_x^B$$

Als weiteres Beispiel kann die Bell-Messung betrachtet werden:

$$\rho = |\psi^{\pm}\rangle\langle\psi^{\pm}| + |\phi^{\pm}\rangle\langle\phi^{\pm}|$$

- POVM (positive Operator reduzierte Messungen):

$$A_\mu = A_\mu^\dagger, \quad \sum A_\mu = 1, \quad A_\mu \geq 0$$

Hierbei wird zusätzlich ein externes System (d.h. die Umwelt) mittels ρ_a betrachtet. Somit ist

$$\begin{aligned} \rho_g &= \rho \otimes \rho_a \\ p_\mu &= \text{Spur}\,(P_\mu \rho \otimes \rho_a) = \sum_{mn} \sum_{rs} (P_\mu)_{mr,ns} \rho_{mn} (\rho_a)_{sr} \\ &= \sum (A_\mu)_{mn} (\rho_g)_{mn} = \text{Spur}\,(A_\mu \rho_g) \end{aligned}$$

Die P_μ sind dabei orthogonale Projektoren mit $\sum p_\mu = 1$. Die A_μ erfüllen dann die POVM-Eigenschaften.

[16] engl. joint measurements

5 Verschränkung und Nichtlokalität

5.1 Verschränkte Zustände

Verschränkte Zustände von zusammengesetzten Systemen können, wenn sie genau bekannt sind, durch einen reinen Zustand $|\psi\rangle$ gekennzeichnet werden, z.B.

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B\right)$$

Eine physikalische Realisierung eines solchen Zustandes ist durch den Zerfall des neutralen Pions gegeben: $\pi^0 \to e^+ + e^-$. Aufgrund der Drehimpulserhaltung ist klar, daß der Gesamtspin 0 erhalten bleiben muß, so daß das e^+ genau entgegengesetzten Spin zum e^- hat $(+\frac{1}{2}, -\frac{1}{2})$. Die Teilchen können sehr weit auseinander sein. Jedoch bilden sie, solange sie nicht durch äußere Einflüsse gestört wurden, ein korreliertes Quantenpaar, so daß der Gesamtzustand sich nicht als Produktzustand darstellen läßt:

$$|\psi\rangle \neq |\psi\rangle_A \otimes |\psi\rangle_B$$

Betrachten wir die verschiedenen Arten von Messungen, die an einem solchen System durchgeführt werden können. Das System sei vor der Messung im Singulettzustand $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_z^A|1\rangle_z^B - |1\rangle_z^A|0\rangle_z^B)$, wobei $|0\rangle \sim |\downarrow\rangle, |1\rangle \sim |\uparrow\rangle$:

1. Messung entlang der x-Achse
   Der Zustand wird in z-Basis dargestellt. Eine Messung der x-Komponente (Operator σ_x^A) bei Alice ergibt als Meßwert einer Einzelmessung $m_x^A = \pm 1$.
   Nun mißt Bob. Auch er erhält bei der Messung der x-Komponente durch $\sigma_x^B \quad m_x = \pm 1$, und zwar in Abhängigkeit des Ergebnisses von Alice:

   - falls Alice $m_x^A = +1$ erhält $\quad \Rightarrow \quad m_x^B = -1$ für Bob
   - falls Alice $m_x^A = -1$ erhält $\quad \Rightarrow \quad m_x^B = +1$ für Bob

   Nachrechenbar wie folgt: Ein Basiswechsel ergibt für Alice und Bob:

$$|0\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle_z + |1\rangle_z\right) \qquad |1\rangle_x = \frac{1}{\sqrt{2}}\left(|0\rangle_z - |1\rangle_z\right)$$

$$\begin{aligned} {}_x^A\langle 0|\psi\rangle &= \frac{1}{2}({}_z^A\langle 0| + {}_z^A\langle 1|)(|0\rangle_z^A|1\rangle_z^B - |1\rangle_z^A|0\rangle_z^B) \\ &= \frac{1}{2}(|1\rangle_z^B - |0\rangle_z^B) = |1\rangle_x^B \end{aligned}$$

2. Messung entlang der y-Achse
   Alice mißt nun entlang der y-Achse mittels σ_y^A und erhält $m_y^A = +1$ oder $m_y^A = -1$. Bob kennt die Folgerungen daraus:

   - falls Alice $m_y^A = +1$ erhält $\Rightarrow$ $m_y^B = -1$ für Bob
   - falls Alice $m_y^A = -1$ erhält $\Rightarrow$ $m_y^B = +1$ für Bob

   Falls Alice Bob vorher schon mitteilt, entlang welcher Achse und mit welchem Ergebnis sie gemessen hat, kann Bob sein Ergebnis vorhersagen.

3. Messung entlang z-Achse
   Hier geschieht noch einmal das gleiche wie in den oben besprochenen Fällen.

5.2 EPR-Paradoxon

Für EINSTEIN war die Lokalität ein physikalisches Prinzip, das in diesem Fall der Spinmessungen besagt, daß die Messung an Teilchen A eine Messung an Teilchen B nicht beeinflussen darf.
In einem Experiment erhält man folgendes: Wenn z.B. A eine Messung an seinem Teilchen macht, und B seine Messung, bevor Information von A nach B gelangen kann, so werden die beiden feststellen, daß ihre Ergbnisse *immer noch* korreliert sind: $m_x^A m_x^B = -1$. Manchmal wird A „up“ erhalten, manchmal B, aber niemals beide, wie es nach einer statistischen Theorie zu erwarten wäre.
Es gibt nun 2 Möglichkeiten, sich dies zu erklären: entweder werden noch weitere (verborgene) Parameter postuliert, die den Zustand schon vorher festlegten, nur nicht (prinzipiell oder meßtechnisch) gemessen werden konnten (EINSTEINs Lösungsansatz) oder man postuliert, daß es sich noch immer nur um einen Zustand handelt, dessen Teilsysteme nicht unabhängig voneinander betrachtet werden können (heutige akzeptierte Vorstellung: Nichtlokalität der Quantenmechanik).

EINSTEINs Lösung beruhte auf der Idee, daß Größen, die prinzipiell gemessen werden können, auch immer existieren müssen; unabhängig davon, ob ich sie beobachte oder nicht. In seinen Worten (rückübersetzt[17]): „Falls wir, ohne in irgendeiner Weise eine System zu beeinflussen, mit Sicherheit den Wert einer physikalischen Größe bestimmen können, dann existiert ein Element der physikalischen Realität, das zu dieser Größe korrespondiert.“ (Prinzip

[17] Originalzitat lag leider nicht vor

der physikalischen Realität).

Ein weiteres von EINSTEIN postuliertes Prinzip ist die Lokalität:
„Die realen Zuständen von 2 räumlich getrennten Systemen sind unabhängig voneinander."

Da also 2 räumlich getrennte Systeme sich nicht beeinflussen können, folgerte EINSTEIN, daß die physikalische Größe, die B auch ohne Messung bestimmen kann, eine physikalische Realität haben muß.
So sollte bei jedem Experiment, egal ob in x, y, z-Richtung, die Spinkomponente bereits vor der Messung feststehen, denn ein solches Experiment kann -wie oben beschrieben- in jede Raumrichtung durchgeführt werden. Die Spinkomponenten sollten daher - nach EINSTEIN - durch sogenannte „verborgene Parameter" festliegen.
Die Quantenmechanik dagegen macht keine Aussagen über Größen, die nicht gemessen werden. Anstatt jedoch zu sagen, daß diese Größen nicht existieren, sagt man, die Quantenmechanik sei nichtlokal. Das wichtige am Lokalitätsprinzip ist nämlich durch die Korrelation nicht verletzt: die Informationsübertragung ist weiterhin nur begrenzt, d.h. mit Lichtgeschwindigkeit, möglich: Bobs Meßausgang verwundert ihn solange nicht, bis er von Alice die Nachricht erhält, daß ihr Spin (bei jeder Messung) entgegengesetzt gerichtet ist. Er kann aus einem reinen „Spin down" noch nichts ablesen. Angemerkt sei noch, daß EINSTEINS Argument durch BOHR entkräftet wurde, der bemerkte, daß zur Konstruktion des Paradoxons 3 Einzelmessungen nötig sind, was keinen Rückschluß auf ein einzelnes Teilchen zuläßt. (Information ist nicht das, was das Teilchen weiß (Quelle), sondern was wir über es erfahren.)

5.3 Bells Theorem

Wenn die Gültigkeit des Prinzipes der Lokalität von EINSTEIN angenommen wird, dann ist die Quantenmechanik inkompatibel mit der Existenz der „verborgenen lokalen Variablen"[18], die eine sogenannte „realistische Theorie" darstellen. Eine solche Theorie und ihre Konsequenzen sollen nun näher betrachtet werden (natürlich nur auf einem abstraktem Niveau, denn es gibt z.Z. keine Realisierung einer solchen Theorie[19]: die BELLschen Ungleichungen (s. 5.4) zeigen, daß eine solchen Theorie vorhersagen macht, die *nicht mit dem Experiment übereinstimmen*; während die Quantenmechanik mit dem Expe-

[18] engl.: local hidden variables
[19] jedenfalls keine die uns bekannt ist

riment übereinstimmt.)
Dazu dient ein Gedankenexperiment: ein EPR-Paar (2 total korrellierte Teilchen aus einer Quelle, z.B. Pionzerfall, s.o.) fliegen mit hoher Geschwindigkeit auseinander. Ihr gemeinsamer Zustand sei der Singulett-Zustand

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle), \quad |\uparrow\downarrow\rangle = |\downarrow\rangle_A \otimes |\uparrow\rangle_B$$

Durch die hohe Geschwindigkeit ist keine Wechselwirkung zwischen den beiden mehr möglich (sie sind „weit weg“). Eine Spinmessung von A entlang der Achse $\vec{a}$, bezeichnet mit $\sigma_{\vec{a}} = \vec{\sigma} \cdot \vec{a}$, ergibt als Einzelmessung einen der zwei Werte $m_a = \pm 1$.
B mißt entlang der $\vec{b}$-Achse, und erhält $m_b = \pm 1$. Falls $\vec{a} = \vec{b}$, gilt immer $m_a^A m_b^B = -1$. EINSTEINs Interpretation des Ergebnisses lautet wie folgt:
Das Ergebnis jeder einzelnen Realisierung des Experimentes hängt von einem Satz von (verborgenen) Parametern $\{\lambda\}$ ab, die von Experiment zu Experiment wechseln. Jedoch folgen sie einer statistischen Verteilung (ähnlich wie die BOLTZMANNverteilung aus deterministischen Ensembles von mikroskopischen Teilchen makroskopische, schwankende Größen entstehen läßt). Die λ folgen einer Verteilung $\rho(\lambda) > 0$, die auf 1 normiert ist: $\int d\lambda \rho(\lambda) = 1$.
In dieser Interpretation läßt sich folgendes ableiten:

- Wenn A eine Messung macht, dann gilt für die zugehörige Funktion $A(\vec{a}, \lambda) = \pm 1$.
- Wenn B eine Messung macht, dann gilt für die zugehörige Funktion $B(\vec{b}, \lambda) = \pm 1$.
- Für die Gesamtfunktion gilt[20]: $A(\vec{a}, \lambda)B(\vec{b}, \lambda) = -1$.

Quantenmechanisch hingegen wird davon gesprochen, daß manche Größen lokal (z.B. Ort), andere - wie z.B. der Spin - nichtlokal sind: das System ist bezüglich dieser Quantenzahl noch „ganz“.

5.4 Bellsche Ungleichungen

Für den Fall das beide Richtungen übereinstimmen ($\vec{a} = \vec{b}$), verlangt das Experiment: $A_a \cdot B_a = -1$. Da der Erwartungswert von $A_a \cdot B_b$ als $E[AB] = \int d\lambda\, p(\lambda) A_a B_b$ definiert ist, gilt:

$$E(\vec{a}, \vec{b}) \;=\; \int d\lambda\, \rho(\lambda) A_a B_b$$

[20] im folgenden $A_a := A(\vec{a}, \lambda)$ usw.; wichtig ist die noch immer vorhandene Abhängigkeit von λ!

Für das zweite Teilchen in einer anderen Richtung gilt

$$E(\vec{a},\vec{c}) \;=\; \int d\lambda\,\rho(\lambda)A_aB_c,$$

also als Differenz:

$$E(\vec{a},\vec{b})-E(\vec{a},\vec{c}) \;=\; \int d\lambda\,\rho(\lambda)A_a\,(B_b-B_c)$$

Außerdem gilt:

$$\begin{aligned} A_bB_b &= -1\\ A_bA_b &= 1\\ \Rightarrow\qquad B_b &= -A_b \end{aligned}$$

Für den Integranden auf der rechten Seite der Differenz folgt damit:

$$\begin{aligned} &(A_aB_b-A_aB_c)\\ =\;& -(A_aA_b-A_a\underbrace{A_bA_b}_{1}B_c)\\ =\;& -A_aA_b(1+A_bB_c)) \end{aligned}$$

Insgesamt ergibt sich, da $A_aA_b=\pm1$ (2 Messungen),

$$\begin{aligned} E(\vec{a},\vec{b})-E(\vec{a},\vec{c}) &= \pm\int d\lambda\,\rho(\lambda)(1+A_bB_c)\\ \Rightarrow\qquad \left|E(\vec{a},\vec{b})-E(\vec{a},\vec{c})\right| &\le \left|\int d\lambda\,\rho(\lambda)(1+A_bB_c)\right| \end{aligned}$$

denn z.B. $x-y=\pm2\Rightarrow|x-y|\le2$. Da der Integrand nicht negativ ist, ist auch das Integral nicht negativ, so daß der Betrag überflüssig ist:

$$\begin{aligned} \left|E(\vec{a},\vec{b})-E(\vec{a},\vec{c})\right| &\le \int d\lambda\,\rho(\lambda)1+\int d\lambda\,\rho(\lambda)A_bB_c\\ &= 1+E(\vec{b},\vec{c}) \end{aligned}$$

Diese Ungleichung stellt eine Form der Bellschen Ungleichung dar: jede Theorie, die mit lokalen verborgenen Parametern arbeitet, erfüllt diese Ungleichung.
Als Vergleich dazu der Erwartungswert in der Quantenmechanik:

$$\begin{aligned} E(\vec{a},\vec{b})=\langle\sigma_{\vec{a}}\sigma_{\vec{b}}\rangle=\langle\psi^-|\sigma^A_{\vec{a}}\otimes\sigma^B_{\vec{b}}|\psi^-\rangle &= (\vec{a}\cdot\vec{b})\underbrace{\langle\psi^-|\sigma^A_z\otimes\sigma^B_z|\psi^-\rangle}_{-1}\\ &= -\cos(\angle(\vec{a},\vec{b})) \end{aligned}$$

Der Erwartungswert der Quantenmechanik stimmt mit dem Experiment überein. Jede andere Theorie, die mit dem Experiment übereinstimmt, muß also dieses Ergebniss liefern. Nehmen wir jetzt an, daß der

- Winkel zwischen $\vec{a}, \vec{b} = \frac{\pi}{3} \quad \Rightarrow \quad \cos(\frac{\pi}{3}) = \frac{1}{2}$
- Winkel zwischen $\vec{b}, \vec{c} = \frac{\pi}{3} \quad \Rightarrow \quad \cos(\frac{\pi}{3}) = \frac{1}{2}$
- Winkel zwischen $\vec{a}, \vec{c} = \frac{2\pi}{3} \quad \Rightarrow \quad \cos(\frac{2\pi}{3}) = -\frac{1}{2}$

Eingesetzt in die Bellschen Ungleichungen ergibt sich:

$$\left| -\frac{1}{2} - \frac{1}{2} \right| = 1 \leq 1 - \frac{1}{2}$$

Eine lokale Theorie mit verborgenen Parametern ist damit unmöglich! Die Bellschen Ungleichungen werden durch einen reinen verschränkten Zustand verletzt. Experimente dazu sind in den 80ern von Alain Aspect, in Paris durchgeführt worden, die die Bellschen Ungleichungen mit 6facher Standardabweichung verletzten.

5.5 CHSH-Ungleichung

CHSH steht für die Namen Clauser-Horne-Shimony-Holt. Diese Gleichung arbeitet mit 4 Richtungen. In unserem Beispiel fordert sie für ein lokale Theorie mit verborgenen Parametern:

$$S = \left| E(\vec{a}, \vec{b}) + E(\vec{b}, \vec{c}) + E(\vec{c}, \vec{d}) - E(\vec{d}, \vec{a}) \right| \leq 2$$

Nimmt man z.B. für die Winkel

- $\angle(\vec{a}, \vec{b}) = \angle(\vec{b}, \vec{c}) = \angle(\vec{c}, \vec{d}) = \frac{\pi}{4}$
- $\angle(\vec{a}, \vec{d}) = \frac{3\pi}{4} \quad \Rightarrow$

$$S = 2\sqrt{2} \geq 2 \quad \text{Widerspruch}$$

Der Vorteil der CHSH-Ungleichungen besteht in der Tatsache, daß Bell $A = \pm 1, B = \pm 1$ verlangt, CHSH jedoch nur $|A|, |B| \leq 1$. Dies trägt den Fällen Rechnung, in denen der Detektor nicht anspricht.

5.6 Nichtlokalität ohne Ungleichungen

Beiden Ungleichungen ist gemein, daß sie Ungleichungen für Erwartungswerte sind. Um sie zu messen, benötigt man eine Anzahl n von z.B Singulettzuständen. Eine einzige Messung sagt noch nichts aus. Daher kann die Ungleichungen auch nur mit einer bestimmten Wahrscheinlichkeit (siehe ASPECTs Experiment oben) widerlegt werden. Einen andern Weg beschritt MERMIN, der drei zusammengesetzte Systeme A, B, C(laire) mit Spin $s = \frac{1}{2}$ betrachtet. Der Singulett-Zustand ist nun GHZ-Zustand (s. S.30)

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$$

$$|000\rangle - |111\rangle = \underbrace{|0\rangle_A}_{\mathcal{H}_2} \otimes \underbrace{|0\rangle_B}_{\mathcal{H}_2} \otimes \underbrace{|0\rangle_C}_{\mathcal{H}_2} - \underbrace{|1\rangle_A}_{\mathcal{H}_2} \otimes \underbrace{|1\rangle_B}_{\mathcal{H}_2} \otimes \underbrace{|1\rangle_C}_{\mathcal{H}_2} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix}_{8-dim}$$

Der Operator $\sigma_x^A \sigma_y^B \sigma_y^C$ wird in dieser Notation aufgeblasen zu

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}_B \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}_C = \begin{pmatrix} & & 0 & -1 \\ & & 1 & 0 \\ 0 & 1 & & \\ -1 & 0 & & \end{pmatrix}_{4\times 4}$$

$$\sigma_x^A \sigma_y^B \sigma_y^C = \begin{pmatrix} & & & & & & 0 & -1 \\ & & & & & & 1 & 0 \\ & & & & 0 & -1 & & \\ & & & & 1 & 0 & & \\ & & 0 & -1 & & & & \\ & & 1 & 0 & & & & \\ 0 & -1 & & & & & & \\ 1 & 0 & & & & & & \end{pmatrix}_{8\times 8}$$

(alle Leerstellen = 0)
Der Zustand $|\psi\rangle_{GHZ}$ ändert sich unter der Wirkung dieses Operators nicht:

A	B	C	$state_{in}$	$state_{fin}$	Größe	Wert
σ_x	σ_y	σ_y	$\|\psi\rangle$	$= \|\psi\rangle$	$m_x^A m_y^B m_y^C$	1
σ_y	σ_x	σ_y	$\|\psi\rangle$	$= \|\psi\rangle$	$m_y^A m_x^B m_y^C$	1
σ_y	σ_y	σ_x	$\|\psi\rangle$	$= \|\psi\rangle$	$m_y^A m_y^B m_x^C$	1
σ_x	σ_x	σ_x	$\|\psi\rangle$	$= \|\psi\rangle$	$m_x^A m_x^B m_x^C$	-1

es gilt für alle A, B, C: $(m_x^{A,B,C})^2 = 1$, $(m_y^{A,B,C})^2 = 1$, $(m_z^{A,B,C})^2 = 1$.
Daher ergibt eine Multiplikation der ersten mit der zweiten Zeile:

$$(m_x^A m_y^A)(m_y^B m_x^B) = 1$$

Dito für dritte mit vierter:

$$(m_x^A m_y^A)(m_y^B m_x^B) = -1$$

Der Widerspruch dieser zwei Gleichungen zeigt, daß es unmöglich ist, daß zugleich m_x^A und m_y^A „Elemente der Realität“ sind: Die Eigenwerte sind nicht alle drei gleichzeitig vorhanden. Sämtliche Operationen müssen mit Operatoren durchgeführt werden; sie betreffen alle Teilchen eines Ensembles. Eine *Messung* überführt ein Teilchen in *einen* Eigenzustand, ihm zugeordnet ist *ein* Meßwert. Es hat keine „physikalische Realität“, diesen Meßwert als Produkt darzustellen und zwischen *verschieden gebauten* Messungen vergleichen zu wollen.

6 Quantenkommunikation/-kryptographie

6.1 Sinn der Kryptographie

Das Ziel der Kryptographie ist es, daß Alice eine Nachricht an Bob sendet, ohne daß der Lauscher (hier mit Eve[21] bezeichnet) die Nachricht abhören kann.

6.2 Traditionelle Kryptographie

Einfache Verschlüsselungen, die schon in der Antike verwendet wurden:

Transposition KALT → TALK

Substitution Die Buchstaben werden in eindeutiger Weise durch andere Buchstaben ersetzt, z.B. K→W, L→R, T→M und A→A. Damit wird aus KALT das Wort WARM.

Diese Codes sind allerdings nicht sicher, da mit statistischen Methoden bei hinreichender Nachrichtenlänge über Buchstabenhäufigkeiten der Code geknackt werden kann. Schön werden diese Codes in [11] dargestellt.

6.3 Einmalschlüssel-Kryptographie

Während des ersten Weltkrieges erfanden 1917 beide Kriegsparteien unabhängig voneinander die sog. Einmalschlüsselkryptographie[22]. Diese Verschlüsselungsform ist unknackbar, allerdings auch sehr unpraktisch.
A und B kennen beide den Schlüssel, wobei der Schlüssel mindestens genauso lang wie die Nachricht sein muß. Wie auch für alle folgenden Verschlüsselungsarten muß das Alphabet zuerst in einer universell bekannten Art und Weise numerisch codiert werden. Hierzu kann z.B. die folgende Tafel dienen:

A	B	C	...	Z		?	,	.
01	02	03	...	26	27	28	29	30

Alternativ kann natürlich auch der ASCII oder BCD-Code verwendet werden. Das Alphabet umfaßt hier 30 Zeichen (d.h. $N = 30$). Alice verwendet jetzt z.B. den folgenden Schlüssel:

12 01 18 27 03 23 05 10 21 24

Nun addiert sie den Schlüssel mit der Nachricht modulo N:

[21] aus dem englischen: eavesdropper
[22] engl.: One time pad

Schlüssel	12	01	18	27	03	23	05	10	21	24
Nachricht	U	N	I	V	E	R	S	I	T	Y
	21	14	09	22	05	18	19	09	20	25
Ergebnis	03	15	27	19	08	11	24	19	11	19

Bob, der den Schlüssel kennt, kann jetzt die Nachricht durch Subtraktion des Codes modulo N entschlüsseln. Das Verfahren hat aber mehrere Nachteile:

1. Die Schlüssel sind sehr lang.
2. Der Schlüssel kann nur einmal verwendet werden.

Da die sichere Schlüsselübertragung problematisch ist, kann auch ein längerer Code verwendet werden, wobei jedesmal ein neues Teilstück gewählt wird. Durch Zusatzprotokolle ist es auch möglich, am Anfang der Nachricht eine Position in einer frei und eindeutig zugänglichen Quelle (z.B. in einem Buch) zu kennzeichnen, z.B. einem Lexikon oder einem Roman. Die Positionsangabe (Seite, Zeile, Spalte) stellt dann den Beginn des Codes dar. Die Anwendung eines solchen Codes bei Geheimdiensten ist sehr schön auch in [12] beschrieben.

6.4 Schlüssel-Verteilungsproblem

Die sichere bzw. geheime Verteilung der Schlüssel kann auf mehrere Weisen erfolgen:

1. Klassische physikalische Methoden (Übertragung des Schlüssels durch ein Medium)
2. Übertragung durch öffentliche Schlüssel[23]
3. Quantenmechanische Methoden

Die klassischen Methoden sind unsicher, d.h. sie können abgehört werden ohne daß eine der beteiligten Seiten dies nachweisen kann.

Public-Key-Methoden

Die Public-Key-Methode wurde erst 1976 vorgestellt und ist heute ein Standardverfahren der Schlüsselkommunikation. Es wird nicht nur von Banken und anderen Finanzinstitutionen eingesetzt, sondern wird auch bei normaler

[23] engl.: public key cryptography

email mittlerweile in der Fassung von PHIL ZIMMERMANN als PGP[24] vielfach verwendet.
Das Verfahren beruht darauf, daß es in der Zahlentheorie Rechnungen gibt, die in einer Richtung sehr einfach, in der anderen Richtung dagegen sehr schwer durchzuführen sind. Konkret wird hierbei die Faktorisierung großer Zahlen betrachtet. Die beiden Richtungen lauten hier am Beispiel:

$$127 \times 229 = ? \qquad 29083 = ? \times ?$$

Alice multipliziert zwei nur ihr bekannte große Primzahlen N_1 und N_2 und veröffentlicht das Produkt $N_1 \cdot N_2$. Bob verschlüsselt jetzt mit Hilfe des öffentlichen Produktes $N_1 \cdot N_2$ seine Nachricht. Alice kann diese nun leicht entschlüsseln, da sie die Primzahlen kennt während alle anderen erst eine Primfaktorzerlegung durchführen müssen. Als Beispiel ist der RSA-Code in Anhang B vorgestellt.
Dieses Verfahren hat zwei Nachteile:

1. Bei derzeitigen Faktorieralgorithmen skaliert die Rechendauer exponentiell mit der Größe von $N_1 \cdot N_2$. Es ist jedoch *nicht* bewiesen, daß es nicht auch schnellere Algorithmen geben könnte.

2. Für (noch hypothetische) Quantencomputer gibt es Algorithmen, die in polynomialer Zeit das Faktorisierungsproblem lösen können.

Das Problem der Schlüsselübertragung kann jedoch dank der Quantenmechanik mit garantierter Sicherheit durchgeführt werden. Viele weitergehende Information zu den hier vorgestellten Schlüsselaustauschverfahren findet sich in [13] und in den dort angegebenen Quellen.

6.5 BB84-Protokoll

Das Protokoll von BENNETT und BRASSARD (s.[14]) hat folgenden Ablauf:

1. Alice präpariert Spin $\frac{1}{2}$-Teilchen in Eigenzustände von x oder z, d.h. $|0\rangle_x$,$|1\rangle_x$, $|0\rangle_z$ oder $|1\rangle_z$, und sendet diese an Bob. In realen Systemen werden oft Photonen in den Zuständen $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\circlearrowright\rangle$ und $|\circlearrowleft\rangle$ präpariert. Da die Wahl des Zweizustandssystems für die folgende Betrachtung keine Rolle spielt, wird der Einfachheit halber beim Bild der Spin-$\frac{1}{2}$-Teilchen geblieben.

2. Bob mißt zufällig ausgewählt entweder σ_x oder σ_z.

[24] Infos unter `http://www.heise.de/ct/pgpCA/pgp.shtml`

3. Öffentliche Diskussion:
   Bob und Alice verkünden öffentlich die von ihnen ausgewählten Richtungen. Wenn die Richtungen übereinstimmen, dann stimmen auch die Ergebnisse überein, da perfekte Korrelation vorliegt. Diese Qubits werden akzeptiert. Die anderen Qubits werden ignoriert.

4. Authentification:
   Alice und Bob verkünden öffentlich einen Teil der akzeptierten Qubits. Wenn diese Qubits übereinstimmen, dann werden die restlichen Qubits als Schlüssel akzeptiert. Sollten sie nicht übereinstimmen und können Übertragungsfehler ausgeschlossen werden, dann wurde ihr Schlüsselaustausch abgehört.

Beispiel:

Qubit	Alice Zustand	Bob Richtung	Bob Ergebnis	Öffentl. Diskus.	Authent.	Ergebnis Authent.	Schlüssel
1	$\|0\rangle_x$	z	0				
2	$\|1\rangle_x$	x	1	OK			1
3	$\|1\rangle_z$	x	1				
4	$\|1\rangle_z$	z	1	OK	1	OK	
5	$\|0\rangle_x$	x	0	OK			0
6	$\|0\rangle_z$	x	1				
7	$\|1\rangle_x$	x	1	OK	1	OK	
8	$\|0\rangle_z$	z	0	OK	0	OK	
9	$\|1\rangle_z$	x	1				
10	$\|0\rangle_z$	z	0	OK			0

Der Schlüssel ist also sicher übertragen worden und lautet 100.

Eve hört ab: Einfache Strategie

Primitives Abhören bedeutet, daß Eve einfach mißt. Nehmen wir an, sie hätte beim ersten Qubit in z-Richtung gemessen. Sie mißt entweder $|0\rangle_z$ oder $|1\rangle_z$, da Alice den Zustand in x-Richtung präpariert hatte. Mit der Wahrscheinlichkeit $\frac{1}{2}$ mißt sie die falsche Richtung (z.B. z statt x), mit der gleichen Wahrscheinlichkeit mißt Bob die richtige Richtung und das Abhören fällt auf, d.h. die Wahrscheinlichkeit beim Abhören eines Qubits erwischt zu werden ist $p = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. Die Wahrscheinlichkeit, daß Eve die N Qubits nicht ändert, die für die Authentifikation benötigt werden, beträgt daher $\left(\frac{3}{4}\right)^N$. Für hinreichend große N wird Eves Abhören daher mit Sicherheit nachgewiesen.

In [13] werden weitere, intelligentere Abhörverfahren vorgestellt, die aber dennoch detektiert werden können.
Praktische Anwendungen dieses Verfahren sind bereits vielfach bei Übertragungen über Glasfaserkabel verwendet worden, vor kurzem ist auch erstmals die Übertragung durch Luft gelungen (s. dazu [17]). Daher zeigen Banken und andere Finanzinstitutionen bereits massives Interesse an dieser Schlüsselverteilungsmethode.

6.6 E91-Protokoll

Das Protokoll von Ekert [15] hat folgenden Ablauf:

1. Eine Quelle emittiert Paare von Teilchen, die sich z.B. in dem Bell-Singulett-Zustand $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ befinden. Eines der Teilchen erhält Alice, das andere erhält Bob.

2. Alice und Bob messen unabhängig voneinander Ihr Teilchen in einer zufällig ausgewählten Richtung. Dabei wählen Sie einen der folgenden Winkel zur z-Achse aus:
   Alice $\phi_a = 0, \frac{\pi}{4}, \frac{\pi}{2}$
   Bob $\phi_b = \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}$

3. Öffentliche Diskussion:
   Alice und Bob geben Ihre Richtungen (d.h. Meßwinkel) öffentlich bekannt. Dabei teilen Sie Messungen in zwei Gruppen ein:

   - Gleiche Richtung (Schlüssel)
   - Verschiedene Richtungen (Authentifikation)

4. Authentification:
   Die Ergebnisse ihrer Messungen in verschiedene Richtungen werden noch korreliert sein; dies wurde in Abschnitt 5.5 gezeigt. Sie geben die Ergebnisse dieser Messungen bekannt und ermitteln die Korrelation zwischen Ihren Ergebnissen:

$$\begin{aligned} S &= E(\vec{a}_1, \vec{b}_2) - E(\vec{a}_1, \vec{b}_3) + E(\vec{a}_1, \vec{b}_1) + E(\vec{a}_3, \vec{b}_3) \\ E(\vec{a}_i, \vec{b}_j) &= \langle \sigma_{\vec{a}_i} \sigma_{\vec{b}_j} \rangle = -(\vec{a}_i \vec{b}_j), \qquad \text{wobei} \\ E(\vec{a}_2, \vec{b}_1) &= -1 = E(\vec{a}_3, \vec{b}_2) \end{aligned}$$

   Wenn Ihre Kommunikation nicht abgehört wurde, ergibt sich $S = -2\sqrt{2}$, ansonsten $-\sqrt{2} \leq S \leq \sqrt{2}$. Da der relative Fehler mit $\frac{1}{\sqrt{N}}$ geht, läßt sich eventuelles Abhören sehr schnell ermitteln.

Bei diesem Protokoll beträgt die Wahrscheinlichkeit, daß Bob und Alice in die gleiche Richtung messen, $p = \frac{2}{9}$.
Ob dieses Verfahren praktikabel ist, kann zur Zeit noch nicht entschieden werden. In [18] wird beschrieben, wie mittels des E91-Protokolls ein Schlüssel einmal um den Genfer-See herum übertragen wurde.
Weitere Einzelheiten auch hier wieder in [13].

6.7 B92-Protokoll

Das B92-Protokoll von Bennett [16] basiert auf einer Messung nicht senkrecht zueinander stehender Zustände[25], wie es z.B. bei den sog. Glauber-Zuständen der Fall ist (dies sind kohärente Zustände des elektromagnetischen Feldes). In unserem Fall betrachten wir eine zweidimensionale Basis mit

$$\{|u_0\rangle, |u_1\rangle\} \quad \text{und} \quad \langle u_0|u_1\rangle \neq 0, \langle u_0|u_0\rangle = 1, \langle u_1|u_1\rangle = 1$$

Beißpiele dafür sind $|u_0\rangle$: spin up, z-Achse, $|u_1\rangle$: spin up, y-Achse. Diese beiden bilden eine Basis für alle möglichen Spineinstellungen, ohne orthogonal zu sein. Eine andere Realisierung sind Photonen, z.B. $|\circlearrowleft\rangle$ und $|\updownarrow\rangle$ Das Protokoll sieht nun wie folgt aus:

1. A führt eine zufällige Sequenz von Messungen durch, z.B. mit Endzuständen $|u_0\rangle, |u_1\rangle, |u_1\rangle, |u_0\rangle, |u_1\rangle, |u_0\rangle, \ldots$
2. A sendet die Zustände an B.
3. B mißt nun die erhaltenen Zustände mittels folgender Operatoren[26]:
   - $P_1 = \mathbb{1} - |u_0\rangle\langle u_0|$
   - $P_0 = \mathbb{1} - |u_1\rangle\langle u_1|$
4. Da auch B die beiden Operatoren zufällig anwendet, sind folgende vier Ergebnisse möglich:
   - A schickt $|u_0\rangle \quad \Rightarrow \quad P_1|u_0\rangle = |u_0\rangle - |u_0\rangle\langle u_0|u_0\rangle = 0$
   - A schickt $|u_0\rangle \quad \Rightarrow \quad P_0|u_0\rangle = 1$ oder 0[27]
   - A schickt $|u_1\rangle \quad \Rightarrow \quad P_1|u_1\rangle = 1$ oder 0
   - A schickt $|u_1\rangle \quad \Rightarrow \quad P_0|u_1\rangle = 0$

[25] engl.: non-orthogonal-states measurement
[26] Hierbei handelt es sich um eine POVM-Messung (s. 4.7)
[27] Der Zustand ist $P_0|u_0\rangle = |u_0\rangle - |u_1\rangle\langle u_1|u_0\rangle = |u_0\rangle - \alpha|u_1\rangle$ mit $\alpha \in \mathbb{C}$

Die Ergebnisse „0“ und „0 oder 1“ sollten etwas genauer gefaßt werden: Für den Zustand $|u_0\rangle$ gilt folgendes: der Erwartungswert des Projektors P_1 berechnet sich zu:

$$\langle P_1\rangle = \langle u_0|P_1|u_0\rangle = \langle u_0|u_0\rangle - \langle u_0|u_0\rangle\langle u_0|u_0\rangle = 1 - 1 = 0$$

Für P_0 ergibt sich:

$$\langle P_0\rangle = \langle u_0|P_0|u_0\rangle = \langle u_0|u_0\rangle - \langle u_0|u_1\rangle\langle u_1|u_0\rangle = 1 - |\langle u_0|u_1\rangle|^2$$

Ähnlich für $|u_1\rangle$. Für P_0 besteht also die Möglichkeit eines „Clicks“ in der Apparatur bei einem einzelnem Teilchen. Das Ergebnis einer einzelnen Messung ist 0 oder 1. Bei P_1 hingegen gibt es niemals ein „Click“.

A	B	mög. Ergebnis.	Ergebnis	Schlüssel
u_0	P_1	0		
u_1	P_1	0/1	1	1
u_1	P_0	0		
u_0	P_0	0/1	0	
u_1	P_1	0/1	1	1
u_0	P_0	0/1	1	0
u_0	P_1	0		
u_1	P_1	0/1	1	1
u_1	P_0	0		
u_0	P_1	0		
u_0	P_0	0/1	0	

Alle „0-Ergebnisse“ werden nicht betrachtet. B weiß: wenn der Meßausgang „Click“ ist und der Operator P_1 angewandt wurde, dann war das Zustand $|u_1\rangle$. Als Schlüsselbits werden nun die von A verwendeten Zustände benutzt. Teile des Gesamtresultates werden veröffentlicht. Es kann nun überprüft werden, ob E (ein eavesdropper) mitgehört hat. Die gesamte Click-Wahrscheinlichkeit ergibt sich aus der Addition der beiden Erwartungswerte, geteilt durch die Anzahl der möglichen Kombinationen:

$$P_{\text{Click}} \;=\; \frac{2}{4}\left(1 - |\langle u_0|u_1\rangle|^2\right)$$

N.B.: Dieses Ergebnis läßt sich auch erhalten, indem die Norm der entstandenen Zustände $|\psi\rangle = P_0|u_0\rangle$ ausgewertet wird. Für Projektoren ist der Erwartungswert nämlich mit der Norm der entstandenen Zustände identisch (Beispiel für $|u_0\rangle$):

$$\langle\psi|\psi\rangle = \langle u_0|P_0^\dagger P_0|u_0\rangle = \langle u_0|P_0|u_0\rangle \text{ wegen } P^\dagger = P,\ P^2 = P$$

7 Teleportation

7.1 Einführung

Da uns leider kein Heisenbergkompensator vorliegt [27] muß zuerst geklärt werden, was als Teleportation bezeichnet wird:

Def. 10 *Teleportation: Transfer eines unbekannten quantenmechanischen Zustandes von einem Ort (A) an einen anderen Ort (B)*

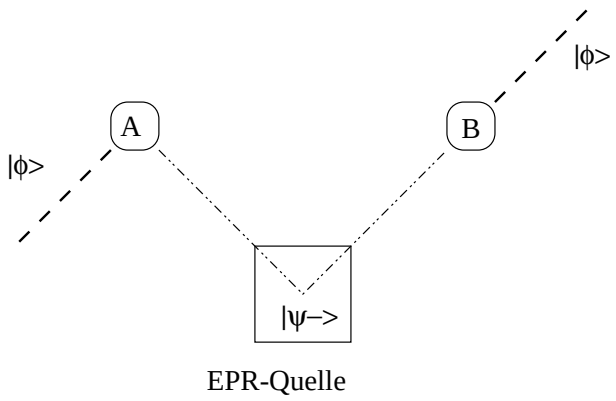


Abbildung 1: Schematische Darstellung von Quantenteleportation

Wie aus der Skizze ersichtlich wird, wird für die Teleportation eine Quelle benötigt, die Bell-Zustände emittiert. Im folgenden betrachten wir eine Quelle, die zwei Teilchen im Singulett-Zustand ($|\psi^-\rangle$) ausstrahlt. Es kann sich hier wie in Experimenten häufig verwendet um verschränkte Photonen oder auch um Elektronen handeln. Eines der verschränkten Teilchen erhält A, das andere B. A führt eine Bell-Messung mit dem zu teleportierenden Zustand $|\phi\rangle$ und seinem EPR-Teilchen durch. Danach teilt A das Meßergebnis über einen klassischen Kommunikationskanal B mit. Offensichtlich erfolgt dies mit Unterlichtgeschwindigkeit. B kann nun durch eine unitäre Transformation an seinem EPR-Teilchen den ursprünglichen Zustand wieder herstellen. Während der gesamten Teleportation ist keine Information über den Zustand gewonnen worden; hätte A einfach nur $|\phi\rangle$ gemessen, dann wäre die Wellenfunktion kollabiert und B hätte keine Möglichkeit der Rekonstruktion gehabt. Auch ist kein Klonen von Quantenzuständen möglich, da A bei der Bell-Messung den ursprünglichen Zustand zerstört.
Sei im folgenden $|\phi\rangle_1 = a|0\rangle + b|1\rangle$ der Zustand, der transferiert werden soll. Als Kanal dient der Bell-Zustand $|\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 - |1\rangle_2|0\rangle_3)$, der die zwei EPR-Teilchen (hier mit 2 und 3 bezeichnet) beschreibt. Diese beiden

Zustände sind zunächst voneinander unabhängig und werden darum durch einen Produktzustand

$$\begin{aligned} |\psi\rangle_{123} &= |\phi\rangle_1 \otimes |\psi^-\rangle_{23} \\ &= \frac{a}{\sqrt{2}}(|0\rangle_1|0\rangle_2|1\rangle_3 - |0\rangle_1|1\rangle_2|0\rangle_3) + \frac{b}{\sqrt{2}}(|1\rangle_1|0\rangle_2|1\rangle_3 - |1\rangle_1|1\rangle_2|0\rangle_3) \end{aligned}$$

beschrieben.
A führt nun eine lokale vollständige („POVM“)-Messung an dem Zustand der Teilchen 1 und 2 zusammen beschreibt durch. Dazu wird der Zustand mit Hilfe der Bell-Basis

$$\begin{aligned} |\psi^\pm\rangle_{12} &= \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 \pm |1\rangle_1|0\rangle_2) \\ |\phi^\pm\rangle_{12} &= \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 \pm |1\rangle_1|1\rangle_2) \end{aligned}$$

wie folgt umgeschrieben:

$$\begin{aligned} |\psi\rangle_{123} = \frac{1}{2}[&- |\psi^-\rangle_{12}(a|0\rangle + b|1\rangle)_3 \\ &+ |\psi^+\rangle_{12}(-a|0\rangle + b|1\rangle)_3 \\ &+ |\phi^-\rangle_{12}(a|1\rangle + b|0\rangle)_3 \\ &+ |\phi^+\rangle_{12}(a|1\rangle - b|0\rangle)_3] \end{aligned}$$

Die Basistransformation erfolgt durch sukzessive Projektionen auf den 1-2-Unterraum, für den ersten Koeffizient ist dies

$$_{12}\langle\psi^-|\psi\rangle_{123} = -\frac{1}{2}(a|0\rangle_3 + b|1\rangle_3).$$

Nachdem der Zustand $|\psi\rangle_{123}$ nun umgeschrieben wurde, kann das Ergebnis einer Messung an Teilchen 1 *und* 2 leicht bestimmt werden: A führt eine Bell-Messung durch, als Ergebnis erhält sie einen der vier Bellzustände. Damit ist der Zustand des Teilchens 3 bei B eindeutig bestimmt. A teilt nun B klassisch ihr Ergebnis mit. Mittels einer (eindeutigen) unitären Operation reproduziert B nun den ursprünglichen Zustand $|\phi\rangle$.
Mißt Alice $|\psi^-\rangle$ braucht B nichts zu tun, der neue Zustand des Teilchens 3 entspricht bereits dem alten von 1. Im zweiten Fall wird eine Stern-Gerlach-Messung vorgenommen, also der Operator σ_z angewendet. Im dritten Fall erhält B durch Anwendung von σ_x und im vierten von σ_y auf den neuen Zustand von Teilchen 3 den gewünschten Zustand. Die Teleportation

ist komplett.
Die obigen BELLzustände sind im Photonenbild Polarisationen. Die Eigenschaften des Lichtfeldes sind im quantisierten Formalismus dieselben wie im klassischen Fall für Felder mit großer Photonenzahl, so daß man die obigen teleportierten Zustände wie folgt interpretieren kann (mit $|a| = |b| \in \mathbb{R}$, $|0\rangle = |\circlearrowleft\rangle$, $|1\rangle = |\circlearrowright\rangle$):

- Fall 1: linear polarisiert, vertikal
- Fall 2: linear polarisiert, horizontal
- Fall 3: linear, vertikal, um π gegenüber Fall 1 phasenverschoben
- Fall 4: linear, horizontal, um π gegenüber Fall 2 phasenverschoben

Die BELLzustände zu interpretieren und zu messen ist schwieriger.
Wichtige Eigenschaften der Teleportation sind:

1. A besitzt keine Information über den Anfangszustand mehr (der Zustand wird nicht kopiert). Der ursprüngliche Zustand des Teilchens ist in einen Teil des BELLzustandes bei A kollabiert. Aus dem BELL-Zustand läßt sich keine Information über den ursprünglichen Zustand gewinnen (Fidelity = 0,5).

2. Ein Zustand läßt sich nicht mit $v > c$ teleportieren; ohne das Telephonat von A nach B wird B den Zustand nicht rekonstruieren können.
   Jedoch weiß B schon mehr als „nichts“ über den Zustand: Die noch fehlende, klassische Information beträgt 2 bit. Der komplette Zustand läßt sich als ein Vektor auf der BLOCHkugel darstellen, und zur Bestimmung eines Vektors auf der Kugel werden mehr als 2 bit (zwei *kontiniuierliche* Parameter) benötigt. Es findet also eine Unterteilung in klassische und nichtklassische Information statt.

3. Die benutzten Operatoren sind sämtlich linear. Deshalb kann die Teleportation auch für Gemische benutzen werden:
   Befindet sich Teilchen 1 in einem Gemischzustand, so kann es auch Teilsystem eines größeren Systems ansehen werden, das sich in einem reinen Zustand befindet (s. Lemma 2), z.B. zusammengesetzt aus einem Teilchen 0 und Teilchen 1. Die Teilspur[28] über den reinen Zustand

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle_{01} + |11\rangle_{01}) \\ \Rightarrow \text{Spur}\,(|\psi\rangle\langle\psi|)_0 &= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \end{aligned}$$

[28] lt. Vorlesung Teilchen 2; muß aber wohl 0 sein ?

ist ein Gemisch. Bei einer solchen Teleportation existiert vorher Verschränkung (quantenmechanische Korrelation) zwischen 1 (Quelle) und 0 (Hilfsteilchen), sowie zwischen 2 (dem Überbringer) und 3 (Ziel). Durch die Messung werden 1 und 2 sowie 0 und 3 miteinander verschränkt, und da 0 nicht näher bekannt ist, wird damit das Gemisch effektiv von 1 auf 3 übertragen.

7.2 Separierbare Zustände

Wie oben gezeigt, werden zur Telportation verschränkte Zustände benötigt. Diese Verschränkung (quantenmechanische Korrelation) tritt nicht bei Produktzuständen und aus ihnen zusammengebauten Gemischen („separierbare Zustände“[29]) auf: Ein separierbarer Zustand besitzt klassische Korrelation in Form gleicher (klassischer) Wahrscheinlichkeiten. Z.B. ist eine korrelierte, separierbare Dichtematrix:

$$\rho = \sum_{\alpha} p_\alpha |\psi_{A,\alpha}\rangle\langle\psi_{A,\alpha}| \otimes |\psi_{B,\alpha}\rangle\langle\psi_{B,\alpha}|$$

Diese ist aus korrelierten lokalen Operationen aufgebaut:

1. Erzeuge mit der Wahrscheinlichkeit p_1 den Produktzustand $|\psi_{1,A}\rangle \otimes |\psi_{1,B}\rangle$.
2. Erzeuge mit der Wahrscheinlichkeit p_2 den Produktzustand $|\psi_{2,A}\rangle \otimes |\psi_{2,B}\rangle$.
3. So fortfahren, bis alle gewünschten Zustände drin sind.

Alle Zustände in A und in B wurden durch *lokale* Operationen erzeugt (z.B. von $|\psi_1\rangle \mapsto |\psi_2\rangle$ in A bzw. B).
Eine andere Facette dieses Sachverhaltes ist durch die Tatsache gegeben, daß der verschränkte Bellzustand $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ die Dichtematrix $|\psi^+\rangle\langle\psi^+|$ besitzt. Diese ist jedoch *ungleich* der Dichtematrix

$$\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11| = \frac{1}{2}(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B + |1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B)$$

7.3 Übertragung von Verschränkung

Die im folgenden vorgestellten Gedankengänge entstammen [19], [20] und den darin zitierten Arbeiten.

[29] engl. seperable state

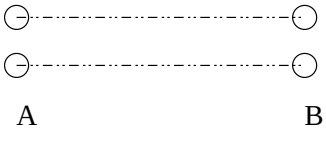


Abbildung 2: Vor Alice Operation

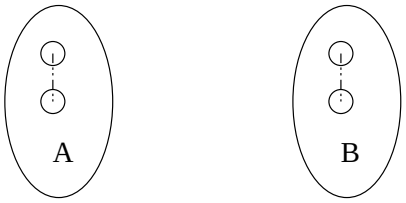


Abbildung 3: Nach Alice Operation

Am Anfang besitzen A und B wie in 2 gezeigt zwei korrelierte Quantenpaare. Die Aufgabe besteht nun darin, daß durch lokale Operationen von A der Zustand in Abbildung 3 realisiert werden soll, d.h. daß die Teilchen von A und B nicht mehr miteinander, sondern untereinander korreliert sind. Hierbei kann z.B. die Vorstellung helfen, daß A ein gut ausgestattetes Labor besitzt und leicht gemeinsame, verschränkte Zustände manipulieren kann, während B nicht über diese Möglichkeit verfügt.
Im folgenden werden einige Anfangssituationen und die möglichen Verschränkungen beschrieben.

1. Idealer Fall: Alice und Bob haben zwei Singulett-Paare:
   Die Wellenfunktion jedes einzelnen Teilchenpaares ist also

$$|\psi^-\rangle_i \;=\; \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

   und somit die Gesamtwellenfunktion

$$|\Psi\rangle \;=\; \frac{1}{2}\left[|00\rangle|11\rangle + |11\rangle|00\rangle - |01\rangle|10\rangle - |10\rangle|01\rangle\right]$$

   Alice führt nun eine Bell-Messung durch, d.h.

$$|\psi^-\rangle_A\langle\psi^-|\Psi\rangle \;=\; |\psi^-\rangle_A\frac{1}{2\sqrt{2}}\left(-|10\rangle_B + |01\rangle_B\right) = \frac{1}{2}|\psi^-\rangle_A|\psi^-\rangle_B \qquad \text{mit}$$

$$|\psi^-\rangle_A \;=\; \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \qquad \text{bzw.}$$

$$|\psi^+\rangle_A\langle\psi^+|\Psi\rangle \;=\; -\frac{1}{2}|\psi^+\rangle_A|\psi^+\rangle_B \qquad \text{usw.}$$

   Mit der Wahrscheinlichkeit $P_{\psi^\pm,\phi^\pm} = \frac{1}{4}$, so daß nach der Messung Bobs Teilchen im Zustand $|\psi^\pm\rangle$, $|\phi^\pm\rangle$ sind, obwohl die Lichtkegel seiner beiden Teilchen verschieden sein können und sie keinerlei Wechselwirkung unterlagen.

2. Alice und Bob teilen sich zwei Paare in verschiedenen Zuständen, von denen einer noch Singulett ist:
   Die Zustände der beiden Teilchen sind damit also

$$\begin{aligned} |\psi\rangle_1 &= \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right) \\ |\psi\rangle_2 &= \cos(\Theta)|0\rangle|1\rangle - \sin(\Theta)|1\rangle|0\rangle. \end{aligned}$$

   Im Fall $\cos^2(\Theta) = \sin^2(\Theta) = \frac{1}{2}$ ist dies wieder Fall 1. Jetzt ist somit der Gesamtzustand

$$\begin{aligned} |\Psi\rangle = \frac{1}{\sqrt{2}}[&\cos(\Theta)|00\rangle|11\rangle + \sin(\Theta)|11\rangle|00\rangle \\ &- \cos(\Theta)|01\rangle|10\rangle - \sin(\Theta)|10\rangle|01\rangle] \end{aligned}$$

   Jetzt führt Alice wieder eine ideale Bell-Messung durch:

$$\begin{aligned} |\psi^-\rangle\langle\psi^-|\Psi\rangle &= |\psi^-\rangle_A \frac{1}{2}\left[-\cos(\Theta)|10\rangle_B + \sin(\Theta)|01\rangle_B\right] \\ &=: \frac{1}{2}|\psi^-\rangle_A|\psi^-(\Theta)\rangle_B \qquad \text{und} \\ |\psi^+\rangle\langle\psi^+|\Psi\rangle &= |\psi^+\rangle_A \frac{1}{2}\left[\cos(\Theta)|10\rangle_B + \sin(\Theta)|01\rangle_B\right] \end{aligned}$$

   Hierbei ist $P_{\phi^\pm(\Theta),\psi^\pm(\Theta)} = \frac{1}{4}$ und $E(\phi^\pm) = E(\psi^\pm) = E$, da alle Schmidt-Koeffizienten identisch sind.

3. Alice und Bob teilen sich zwei gleiche, nicht-Singulett Zustände:

$$\begin{aligned} |\psi\rangle_{1,2} &= \cos(\Theta)|0\rangle|1\rangle - \sin(\Theta)|1\rangle|0\rangle \qquad \text{und damit} \\ |\Psi\rangle &= \cos^2(\Theta)|00\rangle|11\rangle + \sin^2(\Theta)|11\rangle|00\rangle \\ &\quad - \cos(\Theta)\sin(\Theta)\left(|01\rangle|10\rangle + |10\rangle|01\rangle\right) \end{aligned}$$

   Jetzt führt Alice wieder eine ideale Bell-Messung durch, d.h. mit

$$\begin{aligned} |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \qquad \text{und} \\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \qquad \text{wird z.B.} \\ |\psi^\pm\rangle_A\langle\psi^\pm|\Psi\rangle &= |\psi^\pm\rangle_A \frac{1}{\sqrt{2}}\left[-\cos(\Theta)\sin(\Theta)\right]\left(|10\rangle \pm |01\rangle\right) \\ &= \mp\left[\cos(\Theta)\sin(\Theta)\right]|\psi^\pm\rangle_A|\psi^\pm\rangle_B \end{aligned}$$

   Hierbei ist $P_{\psi^\pm} = \sin^2(\Theta)\cos^2(\Theta)$ die Wahrscheinlichkeit für diesen Zustand. Dies wird noch in Abschnitt 8 im Detail betrachtet. Hier soll

lediglich angemerkt werden, daß Verschränkung ähnlich wie Energie nur transferiert, aber nicht erzeugt werden kann. Entsprechend ist

$$\begin{aligned} |\phi^-\rangle_A\langle\phi^-|\Psi\rangle &= |\phi^-\rangle_A \frac{1}{\sqrt{2}}\left[\cos^2(\Theta)|11\rangle_B - \sin^2(\Theta)|00\rangle_B\right] \\ \mathcal{N}^2 &= \frac{1}{2}\left[\cos^4(\Theta) + \sin^4(\Theta)\right] \qquad \text{Normquadrat} \end{aligned}$$

Es kann gezeigt werden, daß $E_{fin}(\Theta) < E$. Das Quadrat der Norm gibt zugleich die Wahrscheinlichkeit für diesen Zustand an, d.h. $P_{\phi^-} = \frac{1}{2}\left[\cos^4(\Theta) + \sin^4(\Theta)\right]$. Die Wahrscheinlichkeit für höher verschränkte Zustände ist daher klein.

Ein (experimentaltechnisches) offenes Problem ist die Frage, wie eine Bell-Messung durchgeführt werden kann. Bei den häufig verwendeten Photonen müssen nichtlineare Medien verwendet werden, die aber erst bei hohen Intensitäten nutzbar sind und nicht wie benötigt bei einzelnen Photonenpaaren. Daher kommen nur lineare optische Elemente zur Anwendung. In [21] und [22] wird das für diesen Fall (leider) relevante Theorem bewiesen:

Theorem 9 *No-Go-Theorem:*
Es ist unmöglich, komplette Bell*-Messungen bei Photonen durchzuführen, ohne nichtlineare optische Element zu benutzen.*

Hierbei stehen „lineare optische Elemente“ für eine Klasse unitärer Operationen. Es bleibt die Frage, ob es möglich ist, Messungen an teilweise verschränkten Zuständen durchzuführen.

4. A und B teilen sich zwei Singuletts (unvollständige Bell-Messung): Wie im ersten Fall teilen sich A und B zwei Singuletts:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)$$

aber in diesem Fall mißt Alice

$$\begin{aligned} \cos(\Theta)|01\rangle - \sin(\Theta)|10\rangle &= |\tilde{\psi}^-\rangle_A \\ \sin(\Theta)|01\rangle + \cos(\Theta)|10\rangle &= |\tilde{\psi}^+\rangle_A \\ \cos(\Theta)|01\rangle - \sin(\Theta)|10\rangle &= |\tilde{\phi}^-\rangle_A \\ \sin(\Theta)|01\rangle + \cos(\Theta)|10\rangle &= |\tilde{\phi}^+\rangle_A \end{aligned}$$

Hierbei handelt es sich nur um ein Beispiel! Es könnte sein, daß es noch bessere Möglichkeiten gibt. Die Verschränkung beträgt jetzt

$$\begin{aligned} E &= E(\tilde{\psi_A^{\pm}}) = E(\tilde{\phi_A^{\pm}}) \\ &= -\cos^2(\Theta)\log(\cos^2(\Theta)) - \sin^2(\Theta)\log(\sin^2(\Theta)) \end{aligned}$$

Eine Projektion auf den Singulett-Zustand ergibt nun

$$|\psi^-\rangle_A\langle\psi^-|\Psi\rangle = |\tilde{\psi^-}\rangle_A \frac{1}{2}\left[\cos(\Theta)|10\rangle_B - \sin(\Theta)|01\rangle_B\right]$$

Die Wahrscheinlichkeit für jeden Bell-Zustand beträgt auch hier $P_{\psi^\pm}{=}P_{\phi^\pm}{=}\frac{1}{4}$. Bob verfügt jetzt über einen Zustand mit der Verschränkung E. Dieses Ergebnis sollte nicht mit idealen sondern mit realen Messungen verglichen werden.

7.4 Dichtes Quantencodieren

Dichtes Quantenkodieren[30] wurde von [23] vorgestellt. Die Idee ist hierbei, in einem Qubit zwei bits zu codieren bzw. in n Qubits $2n$ bits. Alice sendet hierbei ein Teil eines verschränkten Paares an Bob, der darauf einige lokale Operationen anwendet und danach Alice das Teilchen zurücksendet. Schließlich führt Alice eine Bell-Messung durch. Die vier möglichen Ergebnisse können als die zwei übertragenen Bits verstanden werden.
Protokoll:

1. Alice präpariert ein Singulett

$$|\psi^-\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

2. Bob führt eine lokale unitäre Operation durch[31]:

$$\begin{aligned} U_B &= U_B(\alpha,\beta,\gamma) = e^{-i\alpha\sigma_z^B} e^{-i\beta\sigma_y^B} e^{-i\gamma\sigma_z^B} \qquad \text{mit} \\ |\psi(\alpha,\beta,\gamma)\rangle &= U_B|\psi^-\rangle_{A,B} \end{aligned}$$

[30] engl. Quantum Dense Coding
[31] Stimmen die Winkel ?

Insbesondere sind die Zustände

$$\begin{aligned}
|\psi(0,0,0)\rangle_{A,B} &= |\psi^-\rangle_{A,B} \\
|\psi(0,0,\frac{\pi}{2})\rangle_{A,B} &= \left((\cos\left(\frac{\pi}{2}\right)\mathbb{1} - i\sin\left(\frac{\pi}{2}\right)\sigma_z\right)|\psi^-\rangle_{A,B} \\
&= \frac{-i}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right) \sim |\psi^+\rangle_{A,B} \\
|\psi(0,\frac{\pi}{2},0)\rangle_{A,B} &= -i\sigma_y^B|\psi-\rangle_{A,B} \sim |\phi^+\rangle_{A,B} \\
|\psi(\frac{\pi}{2},\frac{\pi}{2},0)\rangle_{A,B} &= (-1)\sigma_z^B\sigma_y^B|\psi^-\rangle_{A,B} \sim \sigma_x^B|\psi^-\rangle_{A,B} \sim |\phi^-\rangle_{A,B}
\end{aligned}$$

3. Alice führt eine BELL-Messung an beiden Teilchen durch. Da bei dieser BELL-Messung vier Ergebnisse möglich sind, hat Bob ihr also zwei bit an Informationen übertragen. Ein gegebenenfalls lauschender Eve kann diese Information nicht decodieren, da sie nicht über Alice Teilchen verfügt und daher bei der Spurbildung über Alice-Raum die Information verloren geht.

8 Purifikation und Destillation

Die Gewinnung von reinen Zuständen wird als Purifikation, die Erhöhung der Verschränkung wird als Destillation bezeichnet. In der Literatur werden diese Begriffe jedoch oft vermischt.
Die grundlegende Idee besteht darin, daß für Anwendungen (z.B. Teleportation) reine und maximal verschränkte Zustände benötigt werden, experimentell jedoch nur gemischte (und damit per Definition *nicht* vollständig verschränkte) Zustände vorliegen.

8.1 Purifikation unter Benutzung von POVMs

Hierbei wird das Experiment auf lokale Operationen und klassische Kommunikation beschränkt. Wie auch im vorherigen Kapitel sind dies die einzigen erlaubten und „billigen"-Operationen.
Wird z.B. der Zustand mit der Dichtematrix

$$\rho \;=\; F|\psi^-\rangle\langle\psi^-| + (1-F)|11\rangle\langle 11| \qquad F \in [0,1]$$

betrachtet. Hierbei ist $F = \text{Spur}\,(\rho|\psi^-\rangle\langle\psi^-|)$ die *Fidelity*. Beträgt sie 1, dann handelt es sich um den maximal verschränkten Singulett-Zustand. Betrachten wir hierfür die CHSH-Ungleichungen

$$\begin{aligned} S &= |E(\vec{a},\vec{b}) + E(\vec{b},\vec{c}) + E(\vec{c},\vec{d}) - E(\vec{d},\vec{a})| \qquad \text{mit} \\ \angle(\vec{a},\vec{b}) &= \angle(\vec{b},\vec{c}) = \angle(\vec{d},\vec{c}) = \frac{\pi}{4} \end{aligned}$$

Hierbei liegen alle Winkel in einer Ebene, wobei die Benennung in mathematisch positiver Richtung erfolgt. Dann kann gezeigt werden, daß

$$S \;=\; F \cdot S(\psi^-) + (1-F)\cdot S(11) = 2\sqrt{2}F + \sqrt{2}(1-F)$$

beträgt. Der Fall $S > 2$, d.h. die Verletzung der CHSH-Ungleichung erfolgt, sobald $1 \geq F \geq \sqrt{2} - 1$ erfüllt ist.
Nicht nur aus diesem eher theoretischen Interesse heraus ist die Destillation interessant, sondern z.B. in Fällen, in denen Quantenzustände gespeichert werden sollen. Ein Zustand $|11\rangle$ entspricht z.B. einer Zweiphotonenanregung in einem System, die erheblich schneller dissipiert als die in $|\psi^-\rangle$ enthaltenen Einphotonenanregungen.

8.2 POVM aus einem abstrakten Blickwinkel

Def. 11 *POVM is ein Satz V_i von Operatoren, so daß $\sum_i V_i^\dagger V_i = \mathbb{1}$. Die V_i sind nicht notwendigerweise hermitesch, aber $V_i^\dagger V_i = O_i$ ist eine Observable.*

Insbesondere ist $\sum O_i = \mathbb{1}$. Daraus folgt $V_i = \sqrt{O_i}$ für $O_i \geq 0$. Nach der Messung beträgt die Dichtematrix

$$\rho \;=\; \frac{V_i \rho V_i^\dagger}{\text{Spur}\left(V_i \rho V_i^\dagger\right)}$$

Def. 12 *Lokale POVM für zusammengesetzte Systeme sind POVM $V_i = V_i^A \otimes V_i^B$ für jedes i.*
Fidelity:

$$F \;:=\; Spur\left(\rho|\psi^-\rangle\langle\psi^-|\right) = \langle\psi^-|\rho|\psi^-\rangle \leq 1$$

Jetzt wird eine POVM-Messung durchgeführt mittels

$$\begin{aligned}
O_1^{A,B} &= \alpha|0\rangle_{A,B}\langle 0| + (1-\alpha)|1\rangle_{A,B}\langle 1| \qquad \alpha \geq 0 \\
O_2^{A,B} &= (1-\alpha)|0\rangle_{A,B}\langle 0| + \alpha|1\rangle_{A,B}\langle 1| \\
\mathbb{1}_A &= O_1^A + O_2^A \qquad V_i^A = \sqrt{O_i^A} \qquad \text{und} \\
V_1^A &= \sqrt{\alpha}|0\rangle_A\langle 0| + \sqrt{1-\alpha}|1\rangle_A\langle 1|
\end{aligned}$$

Der Zustand nach der Messung von $O_1^A \otimes O_1^B$ wird durch die Dichtematrix

$$\rho' \;=\; \frac{V_1^A \otimes V_1^B \rho (V_1^A)^\dagger \otimes (V_1^B)^\dagger}{\text{Spur}\left(O_1^A \otimes O_1^B \rho\right)}$$

beschrieben. Hierbei ist[32]

$$\begin{aligned}
\text{Spur}\left(O_1^A \otimes O_1^B \rho\right) &= F\alpha(1-\alpha) + (1-F)(1-\alpha)^2 \qquad \text{und somit} \\
\rho' &= \frac{F\alpha(1-\alpha)|\psi^-\rangle\langle\psi^-| + (1-F)(1-\alpha)^2|11\rangle\langle 11|}{F\alpha(1-\alpha) + (1-F)(1-\alpha)^2} \\
&= \frac{F\alpha|\psi^-\rangle\langle\psi^-| + (1-F)(1-\alpha)|11\rangle\langle 11|}{F\alpha + (1-F)(1-\alpha)}
\end{aligned}$$

Damit geht die neue Fidelity

$$\begin{aligned}
F' &= \frac{F\alpha}{F\alpha + (1-F)(1-\alpha)} \to 1 \text{ falls } \alpha \to 1 \\
F' &> F \qquad \text{falls } \alpha > \frac{1}{2}
\end{aligned}$$

Dies ist klar, wenn die streng monotone Stetigkeit betrachtet wird und durch explizites Einsetzen 1 als Fixpunkt identifiziert wird. Allerdings geht die Wahrscheinlichkeit für solche Zustände

$$P \;=\; \left[F\alpha + (1-F)(1-\alpha)\right](1-\alpha) \to 0 \text{ mit } \alpha \to 1.$$

[32] hier fehlt noch was ?

8.3 Purifikation unter Benutzung von Control-NOT Operationen

Dieser Abschnitt basiert auf [24], [25] und [26]. Wir betrachten einen Zustand mit der Dichtematrix ρ, der $\langle\psi^-|\rho|\psi^-\rangle = F > \frac{1}{2}$ erfüllt. Alice und Bob teilen sich Paare einer Quelle die durch ρ beschrieben wird.
Prozedur:

1. Zufällige bilaterale Rotationen:
   A und B führen die gleichen lokalen und zufälligen Rotationen von ρ durch. Dabei bleibt $|\psi^-\rangle$ invariant während die orthogonalen Unterräume „durcheinander gewirbelt“ werden.

$$\begin{aligned}
|0\rangle &\rightarrow |0'\rangle = \cos(\Theta)|0\rangle + e^{i\varphi}\sin(\Theta)|1\rangle \\
|1\rangle &\rightarrow |1'\rangle = -\sin(\Theta)|0\rangle + e^{i\varphi}\cos(\Theta)|1\rangle \qquad \text{und damit} \\
|\psi^-\rangle &\rightarrow e^{i\varphi}|\psi^-\rangle \\
|\psi^+\rangle &\rightarrow \frac{1}{\sqrt{2}}\cos(\Theta)\sin(\Theta)\left(|00\rangle + e^{i2\varphi}|11\rangle\right) + \frac{1}{\sqrt{2}}e^{i\phi}|\psi^+\rangle \\
|\phi^-\rangle &\rightarrow \frac{1}{\sqrt{2}}\left(|00\rangle + e^{i2\varphi}|11\rangle\right) \\
|\phi^+\rangle &\rightarrow \frac{1}{\sqrt{2}}(\cos^2(\Theta) - \sin^2(\Theta))\left(|00\rangle - e^{i2\varphi}|11\rangle\right) + \frac{1}{\sqrt{2}}e^{i\varphi}|\psi^+\rangle
\end{aligned}$$

   Nach dieser Operation beträgt die Dichtematrix

$$\begin{aligned}
\rho_{\psi^-} &= F|\psi^-\rangle\langle\psi^-| + \left(\frac{1-F}{3}\right)\left[|\psi^+\rangle\langle\psi^+| + |\phi^-\rangle\langle\phi^-| + |\phi^+\rangle\langle\phi^+|\right] \\
&= \left(F - \frac{1-F}{3}\right)|\psi^-\rangle\langle\psi^-| + \frac{1-F}{3}\mathbb{1}
\end{aligned}$$

   Dieser Zustand wird WERNER-Zustand[33] genannt.

2. Unilaterale PAULI-Rotation:
   A wendet σ_y an $\Leftrightarrow |\psi^\pm\rangle \rightarrow |\phi^\mp\rangle$.

3. Bilaterale C-NOT-Operation:
   Alice und Bob nehmen zwei Paare vom Teilchenensemble und wenden auf diese Paare die C-NOT-Operation an. Bezeichnet Alice ihre Teilchen mit A_1, A_2 und Bob seine mit B_1, B_2, wobei Teilchen 1 jeweils als

[33] Deutscher Physiker aus Braunschweig

Quell-, Teilchen 2 als Zielteilchen bezeichnet wird, dann ist die Dichtematrix

$$\rho \;=\; \rho_{\phi^+}^{A_1,B_1} \otimes \rho_{\phi^+}^{A_2,B_2}.$$

Die Wirkung der Control-NOT-Operation auf Zustände beträgt

$$\begin{aligned}
\text{C-NOT}|0\rangle_{A_1}|0\rangle_{A_2} &= |0\rangle_{A_1}|0\rangle_{A_2} \\
\text{C-NOT}|0\rangle_{A_1}|1\rangle_{A_2} &= |0\rangle_{A_1}|1\rangle_{A_2} \\
\text{C-NOT}|1\rangle_{A_1}|0\rangle_{A_2} &= |1\rangle_{A_1}|1\rangle_{A_2} \\
\text{C-NOT}|1\rangle_{A_1}|1\rangle_{A_2} &= |1\rangle_{A_1}|0\rangle_{A_2}
\end{aligned}$$

Offensichtlich kann die Abbildung durch eine unitäre Transformationsmatrix beschrieben werden, sie ist also reversibel. Dies prädestiniert sie zu einem universellen Gatter für einen Quantencomputer. Für die Bell-Zustände ergibt sich:

Anfangszustände		Endzustände	
Quelle	Ziel	Quelle	Ziel
$\phi^\pm$	ϕ^+	$\phi^\pm$	ϕ^+
$\phi^\pm$	ϕ^-	$\phi^\mp$	ϕ^-
$\psi^\pm$	ψ^+	$\psi^\pm$	ϕ^+
$\psi^\pm$	ψ^-	$\psi^\mp$	ϕ^-
$\phi^\pm$	ψ^+	$\phi^\pm$	ψ^+
$\phi^\pm$	ψ^-	$\phi^\mp$	ψ^-
$\psi^\pm$	ϕ^+	$\psi^\pm$	ψ^+
$\psi^\pm$	ϕ^-	$\psi^\mp$	ψ^-

Zum Beispiel ist

$$\begin{aligned}
\text{C-NOT}|\phi^\pm\rangle_1 \otimes |\phi^+\rangle_2 &= \text{C-NOT}\frac{1}{2}\left[|0\rangle_{A_1}|0\rangle_{B_1} \pm |1\rangle_{A_1}|1\rangle_{B_1}\right] \\
&\qquad \otimes \left[|0\rangle_{A_2}|0\rangle_{B_2} + |1\rangle_{A_2}|1\rangle_{B_2}\right] \\
&= \frac{1}{\sqrt{2}}\left[|00\rangle_1|\phi^+\rangle_2 \pm |11\rangle_1|\phi^+\rangle_2\right] \\
&= |\phi^\pm\rangle_{A_1,B_1}|\phi^+\rangle_{A_2,B_2}.
\end{aligned}$$

Die anderen Kombinationen werden entsprechend berechnet.

4. Messung:
   A und B messen $\sigma_z^{A_2}$ bzw. $\sigma_z^{B_2}$ ihrer Zielteilchen. Sie teilen sich die Ergebnisse mit und behalten die Quellpaare falls das Ergebnis bei beiden

Messungen gleich ist (d.h. die Richtung des Zielteilchenspins). Andernfalls übergehen sie ihr Quellpaar. Dies bedeutet, daß sie **ihre** Dichtematrix auf den Raum $\phi^{\pm}$ des Ziels projezieren bzw. ihren Eingangszustand auf den Unterraum $\{\phi^{\pm} \otimes \phi^{\pm}, \psi^{\pm} \otimes \psi^{\pm}\}$.

Frage: Wie groß ist die Fidelity $F' = \langle\phi^+|\rho_S|\phi^+\rangle$?

- mit $P = F^2$ war der Ausgangszustand $|\phi^+\rangle_1|\phi^+\rangle_2$
- mit $P = \frac{(1-F)^2}{9}$ war der Ausgangszustand $|\phi^-\rangle_1|\phi^-\rangle_2$
- mit $P = \frac{F(1-F)}{3}$ war der Ausgangszustand $|\phi^{\mp}\rangle_1|\phi^{\pm}\rangle_2$
- mit $P = \frac{(1-F)^2}{9}$ war der Ausgangszustand $|\psi^{\pm}\rangle_1|\psi^{\pm}\rangle_2$

$$\begin{aligned} F' &= \frac{F^2 + \frac{(1-F)^2}{9}}{P_+} \qquad \text{mit} \\ P_+ &= F^2 + \frac{(1-F)^2}{9} + 2\frac{F(1-F)}{3} + 4\frac{(1-F)^2}{9} \end{aligned}$$

Hierbei ist P_+ die Wahrscheinlichkeit einer positiven Projektion. Falls $F > \frac{1}{2}$ ist $F' > F$.

5. Unilaterale PAULI-Rotation mit σ_y:

$$\rho_{\phi^+} \quad \rightarrow \quad \rho_{\psi^-} = F'|\psi^-\rangle\langle\psi^-| + \frac{1-F'}{3}(\dots)$$

Mittels Iteration kann F' nun beliebig nahe an 1 gebracht werden, d.h. eine „perfekte Fidelity“ erreicht werden.

9 Quanten-Rechnen

Dieser Abschnitt orientiert sich an [30], weitere Informationen z.B. in [28] und [29].

9.1 Klassisches Rechnen

Im folgenden sollen wichtige Begriffe des klassischen Rechnens definiert werden.

- Rechnen ist ein physikalischer Prozeß, der ein *Eingabe* in eine *Ausgabe* transformiert. Im folgenden wird mit klassischem Rechnen diejenigen Rechenvorgänge bezeichnet, die rein mit klassischen physikalischen Gesetzen beschreibbar sind und nicht quantenkohärente Prozesse benutzen.

- Algorithmen können als *langsam* oder *schnell* eingestuft werden. Dafür wird mit der Schrittanzahl n_o und der Eingabegröße N (in bits) noch die Größe $n_i = \log_2 N$ definiert. Ferner bezeichnet im folgenden

$$\text{Poly}\,(x, m) \;:=\; \sum_{i=0}^{m} a_i x^i \qquad a_i \in \mathbb{R},\, m < \infty$$

  Schnelles Rechnen: Erfüllt der Algorithmus die Bedingung

$$n_o \;\leq\; \text{Poly}\,(n_i, k) \sim O(n_i^k)$$

  für ein beliebiges aber festes k, dann heißt er schnell bzw. Mitglieder der Klasse P.

  Langsames Rechnen: Gilt für jedes $k > 0$ $n_o > \text{Poly}\,(n_i, k)$ (für $n_i \to \infty$) so heißt der Algorithmus langsam (skaliert exponentiell) oder Mitglied der Klasse NP. Der Beweis, das ein gegebender Algorithmus zur Klasse NP gehört ist im allgemeinen schwer zu führen. Algorithmen, bei denen dieser Beweis gelungen ist, werden daher als Mitglied der Klasse NP-komplett bezeichnet.

  Beispielhaft sei hier das Problem des reisenden Geschäftsmanns erwähnt. Hierbei geht es um die Frage, was der kürzeste Weg zwischen N Punkten in einer Ebene ist, wenn jeder Punkt einmal erreicht werden muß. Dieses Problem gehört zu der Klasse NP-komplett. Durch Gegenbeispiele (d.h. Algorithmen mit polynomialer Laufzeit) kann aber gezeigt werden, daß bereits bei geringen Zusatzannahmen das Problem zur Klasse P gehört.

Als weiteres Beispiel sei die sequentielle Addition (Ziffer für Ziffer) zweier Zahlen N_1 und N_2 mit n_i Ziffern betrachtet. Offensichtlich ist $n_o \lesssim O(n_i) < O(n_i^2)$.

Im Gegensatz dazu benötigen eine (naive) Faktorisierung, bei der einfach die Zahl $M = M_1 \cdot M_2$ durch $1, \ldots, \sqrt{M}$ geteilt wird,

$$n_o \sim O(\sqrt{M}) = O(2^{\frac{\log_2(M)}{2}}) = O(2^{\frac{n_i}{2}}).$$

Ist hierbei allerdings z.B. M_1 bekannt, dann kann das Problem in polynomialer Zeit gelöst werden.

Wichtig ist daher immer, zwischen der Klasse eines Problems (z.B. Travelling Salesman) und der Klasse eines Algorithmus (z.B. Faktorisierung) zu unterscheiden. Wenn ein Problem in der Klasse NP-komplett liegt, dann kann es keinen Algorithmus in der Klasse P geben. Liegt dagegen der Algorithmus in der Klasse NP, dann bedeutet dies nicht, daß alle Algorithmen in dieser Klasse liegen. Ein schönes Beispiel hierfür ist SHORs Faktorisierungsalgorithmus (s.11.1).

- *Universelle Computer* sind Rechner, die jede mögliche Rechnung durchführen können. Sie stellen eine Abstraktion von der konkreten Hardware dar; so ist der mechanische Rechner von CHARLES BABBAGE natürlich ganz anders zu programmieren als der der erste elektronische Rechner von KONRAD ZUSE, welcher sich in der Programmierung selbst wieder grundlegend von einem modernen Rechner mit z.B. einem Alpha-Prozessor unterscheidet.

  Universelle Computer verfügen über

  - bits, das sind (klassische) Register die die Werte 0 und 1 aufnehmen können. Hiermit kann jede Zahl codiert werden, z.B. $23 = 10111$ unter Benutzung des Binärsystems;
  - Gatter, z.B.

NOT	
I	O
0	1
1	0

AND	
I	O
00	0
01	0
10	0
11	1

  - universelle Gatter, die aus endlich vielen Gattern aufgebaut sind und die jede denkbare Berechnung durchführen können.

9.2 Quantenrechnen

Auch hier sollen im folgenden zuerst die Begriffe geklärt werden:

- Quantenrechnen ist ein quantenphysikalischer Prozeß, der *Eingaben* in *Ausgaben* transformiert. Hierbei können Quantenphänomene wie Superposition, Verschränkung etc. verwendet werden; da die klassische Physik als Grenzfall in der Quantenphysik enthalten ist, ist diese Definition des Rechnes weiter, ein Quantenrechner kann auch klassisch rechnen.

- Eingaben/Ausgaben werden durch Zustände eines physikalischen Systemes repräsentiert, z.B. durch Basiszustände $|0\rangle, |1\rangle, \ldots, |N\rangle, \ldots$. Eine Zahl kann dann z.B. mittels $N \rightarrow |N\rangle$ codiert werden.

- *Ideales Quantenrechnen* beschränkt sich auf diejenigen datenverarbeitende Operationen, die durch unitäre Operatoren beschrieben werden können. Dies ist natürlich eine Idealisierung. Sie ist aber insofern nützlich, als daß hiermit die prinzipiellen Vorgehensweisen beim Quantenrechnen gut beschrieben werden können.

  Problematisch ist z.B. die AND-Operation, da sie vom $\mathcal{H}_4$ auf den $\mathcal{H}_2$ abbildet. Als weiteres Beispiel sei die nicht unitäre Paritätsoperation betrachtet:

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow |1\rangle \\ |2\rangle &\rightarrow |0\rangle \\ |3\rangle &\rightarrow |1\rangle \end{aligned}$$

  Dieses Problem kann durch Hinzunahme der Umgebung umgangen werden:

$$\begin{aligned} |0\rangle|0\rangle &\rightarrow |0\rangle|0\rangle \\ |1\rangle|0\rangle &\rightarrow |1\rangle|1\rangle \\ |2\rangle|0\rangle &\rightarrow |0\rangle|1\rangle \\ |3\rangle|0\rangle &\rightarrow |1\rangle|0\rangle \end{aligned}$$

- Quantenparallelität:

$$f : \{0, \ldots, n\} \rightarrow \{0, \ldots, n\}$$

sei die betrachtete Funktion. Z.B. kann f durch die unitäre Operation

$$\begin{array}{rcl} U|0\rangle|0\rangle & \rightarrow & |0\rangle|f(0)\rangle \\ U|1\rangle|0\rangle & \rightarrow & |1\rangle|f(1)\rangle \\ \vdots & & \vdots \\ U|n\rangle|0\rangle & \rightarrow & |n\rangle|f(n)\rangle \end{array}$$

vermittelt werden. Sowohl die Anfangszustände als auch die Endzustände sind orthonormal, d.h. eine solche unitäre Transformation existiert (auch für $f = \text{const}$). Präparieren wir nun die Quantensuperposition

$$\begin{aligned} |\Psi\rangle &= \frac{1}{\sqrt{n+1}} \sum_{k=0}^{n} |k\rangle|0\rangle \qquad \text{dann ist} \\ U|\Psi\rangle &= \frac{1}{\sqrt{n+1}} \sum_{k=0}^{n} |k\rangle|f(k)\rangle, \end{aligned}$$

d.h. alle Werte werden simultan berechnet. Allerdings ist die Ausgabe nicht einfach, im Prinzip sogar unmöglich, da die Messung die Superposition zerstört.

- Bedingte Dynamik
  Einige wichtige Operationen, die auf ein Register wirken, hängen von dem anderen Register ab:

  $$U = |0\rangle\langle 0|U_0 + |1\rangle\langle 1|U_1 + \ldots$$

  Ein Beispiel hierfür ist die C-NOT-Operation aus Abschnitt 8.3.

- Langsames und schnelles Rechnen

  Da der Quantenrechner den klassischen Rechner beinhaltet, sind alle schnellen Algorithmen auch auf dem Quantenrechner schnell. Es existieren allerdings einige schnelle Quantenalgorithmen, die kein klassisches Gegenstück besitzten, z.B. SHORs-Faktorisierungsalgorithmus.

  Natürlich können nur Probleme der Klasse NP einen schnellen Quantenalgorithmus besitzten.

  Als Beispiel sei der DEUTSCH-Algorithmus betrachtet, der hier vereinfacht vorgestellt werden soll. Es werden alle möglichen Funktionen

  $$f : \{0,1\} \rightarrow \{0,1\}$$

  betrachtet. Dies sind $f_1 = \mathbb{1}$, $f_2 = \text{NOT}$, $g_1 = 0$ und $g_2 = 1$. Die logischen Tafeln lauten also:

f_1	
I	O
0	0
1	1

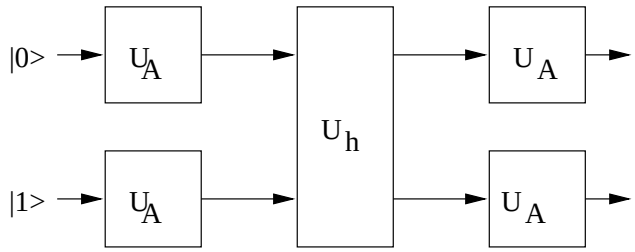
f_2	
I	O
0	1
1	0

g_1	
I	O
0	0
1	0

g_2	
I	O
0	1
1	1

Die Funktionen f_1 und f_2 sind ausgeglichen, d.h. die Funktion hat genauso häufig 0 wie 1 als Ergebnis. Bei den Funktionen g_1 und g_2 ist dies offensichtlich nicht der Fall.

Das Problem von DEUTSCH besteht nun in der Annahme, daß eine unbekannte Funktion h, deren Berechnung sehr langwierig ist (z.B. zwei Stunden), gegeben ist und innerhalb kurzer Zeit herausgefunden werden soll, ob dies eine ausgeglichene oder unausgeglichene Funktion ist. Während ein klassischer Computer die Funktion zweimal berechnen muß (einmal für 0 und einmal für 1 als Eingabe), wird ein Quantencomputer nach folgendem Schema an das Problem herangehen:



Es werden zwei Qubits $|0\rangle$ und $|1\rangle$ geladen. Diese werden zuerst einzeln (lokal) mittels der schnellen Operation (!) U_A transformiert:

$$\begin{aligned} U_A|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ U_A|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad \text{d.h.} \\ |0\rangle \otimes |1\rangle &\rightarrow U_A|0\rangle \otimes U_A|1\rangle \\ &= \frac{1}{2}\left(|0\rangle + |1\rangle\right) \otimes \left(|0\rangle - |1\rangle\right) =: |\psi_2\rangle \end{aligned}$$

U_h wird jetzt mit dieser Superposition als Eingabe durchgeführt. Dabei ist

$$\begin{aligned} U_h|i,j\rangle &= |i, j \oplus h(i)\rangle \qquad \text{mit} \\ a \oplus b &= (a+b) \mod 2. \end{aligned}$$

Wenn z.B. $h = f_1$ ist. dann ist

$$\begin{aligned}
U_h|0,0\rangle &= |0,0\rangle \\
U_h|0,1\rangle &= |0,1\rangle \\
U_h|1,0\rangle &= |1,1\rangle \\
U_h|1,1\rangle &= |1,0\rangle \qquad \text{und damit} \\
U_h|\psi_2\rangle &= \frac{1}{2}\left(|0\rangle\otimes|0\rangle - |0\rangle\otimes|1\rangle + |1\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle\right) \\
&= \frac{1}{2}\left(|0\rangle - |1\rangle\right)\otimes\left(|0\rangle - |1\rangle\right) =: |\psi_3\rangle
\end{aligned}$$

Abschließend werden die Qubits wieder lokal zurücktransformiert:

$$U_A \otimes U_A|\psi_3\rangle = |11\rangle$$

Analog kann diese Rechnung für die anderen drei möglichen Funktionen durchgeführt werden. Es ergibt sich

$$\begin{aligned}
f_1(|01\rangle) &= |11\rangle \\
f_2(|01\rangle) &= |11\rangle \\
g_1(|01\rangle) &= |01\rangle \\
g_2(|01\rangle) &= |01\rangle
\end{aligned}$$

Durch Messung des ersten Qubits kann also entschieden werden, ob die Funktion ausgeglichen ist oder nicht.

Der Originalalgorithmus ist komplizierter, da der allgemeinere Fall von Funktionen in n dimensionalen Räumen betrachtet wird. Mit einer gewissen Wahrscheinlichkeit werden die Rechnungen mit dem Quantenalgorithmus exponentiell gegenüber dem klassischen Algorithmus beschleunigt.

- *Universelle Quantencomputer* sind eine Abstraktion von der konkreten physikalischen Realisation. Sie können jede denkbare quantenphysikalische Rechnung durchführen und verfügen daher über
  - Qubits: Elementare Quantenregister, die durch Zweizustands-Systeme realisiert $\{|0\rangle, |1\rangle\}$ sind. Damit kann z.B. die Zahl 23 durch die fünf Qubits $|10111\rangle$ dargestellt werden.
  - Quantengatter: Elementare unitäre Operationen, die auf Qubits wirken. Dies können z.B. die folgenden Operationen sein:

I	V(α,φ)
$\|0\rangle$	$\cos(\alpha)\|0\rangle - ie^{i\varphi}\sin(\alpha)\|1\rangle$
$\|1\rangle$	$ie^{-i\varphi}\sin(\alpha)\|0\rangle + \cos(\alpha)\|1\rangle$

I	C-NOT
$\|0\rangle\|0\rangle$	$\|0\rangle\|0\rangle$
$\|0\rangle\|1\rangle$	$\|0\rangle\|1\rangle$
$\|1\rangle\|0\rangle$	$\|1\rangle\|1\rangle$
$\|1\rangle\|1\rangle$	$\|1\rangle\|0\rangle$

– Universelle Quantengatter: Menge von Gattern, die jede denkbare Berechnung erlauben. Hierbei sind kontinuierliche unitäre Transformationen erlaubt, d.h. die Menge der Gatter kann unendlich groß sein. V(α, φ), C-NOT realisieren eine solche Menge. Beweis in [30].

  Für Photonen werden die zwei Gatter V und C-NOT durch Rotationen der Polarisation und Phasenschieber realisiert, beide experimentell leicht realisierbar.

10 Fehlerkorrektur

10.1 Klassische Fehler

Als einer der ersten Theoretiker hat SHANNON das Problem der Übertragung von Informationen über verrauschte Kanäle untersucht. Die naive Lösungsmöglichkeit die Hardware zu verbessern scheidet oft aus Kostengründen oder technologischen Unzulänglichkeiten aus. Daher bleibt nur die Möglichkeit, gegen die Fehler „anzukämpfen“. Hierbei besteht die Möglichkeit durch redundantes Senden von Informationen eine Fehlerkorrektur zu implementieren.
Im allgemeinen werden zwei Arten von Fehlern unterschieden:

- Speicherfehler - gespeicherte Information wird im Laufe der Zeit einer zufälligen Transformation unterzogen
- Operationsfehler - Während einer (Rechen-)Operation tritt ein Fehler auf

Beide Fehlertypen sind im Ergebnis identisch (inkorrekte Daten), aufgrund der einfacheren Beschreibung wird die folgende Betrachtung aber nur für Speicherfehler durchgeführt.

10.2 Klassische Fehlerkorrektur

An einer Speicherposition sei ein bit (d.h. entweder 0 oder 1) gespeichert. Mit $P(\tau)$ wird die Wahrscheinlichkeit, das sich das betrachtete Bit nach der Zeit τ geändert hat, bezeichnet. $P(\tau)$ ist eine monoton wachsende Funktion und sollte $P(\tau) \ll 1$ erfüllen.
Im folgenden werde das redundante Codieren betrachtet. Hierbei wird jedes Bit z.B. durch drei bits beschrieben:

$$\begin{aligned} 0 &\rightarrow 000 \\ 1 &\rightarrow 111 \end{aligned}$$

Die dreibit-Sequenzen (bzw. allgemein n-bit-Sequenzen) werden Codewörter genannt.
Die Wahrscheinlichkeit, daß nach der Zeit τ ein Fehler aufgetreten ist, beträgt unter der Annahme, daß $P(\tau)$ für jedes „physikalische bit“ statistisch unabhängig ist:

- Kein Fehler: $(1 - P(\tau))^3$

- Fehler in einem bit[34]: $3P(\tau)(1-P(\tau))^2$
- Fehler in zwei bits: $3P^2(\tau)(1-P(\tau))$
- Fehler in drei bits: $P^3(\tau)$

Die Fehlerkorrektur erfolgt jetzt durch „Abstimmung“:

3 bits identisch: Keine Korrektur durchgeführt.

1 bit anders: Dieses bit wird auf den Wert der zwei anderen gesetzt.

Wie groß ist die Wahrscheinlichkeit, daß diese Mehrheitsentscheidung tatsächlich das richtige Ergebnis liefert[35]?

$$P_\tau^{\text{korr}} = (1-P_\tau)^3 + 3(1-P_\tau)^2 P_\tau = 1 - 3P_\tau^2 + 2P_\tau^3$$

Während ohne Fehlerkorrektur die Wahrscheinlichkeit für ein richtiges Ergebnis lautet

$$P_\tau^{\text{unkorr}} = (1-P_\tau) < P_\tau^{\text{korr}} \qquad \text{falls } P_\tau \leq \frac{1}{2}$$

Noch besser sieht die Situation aus, wenn häufig korrigiert und ein langer Zeitraum betrachtet wird. Wächst zum Beispiel die Fehlerwahrscheinlichkeit linear, d.h. $P_\tau = c\tau$ und korrigieren wir N mal in der betrachteten Zeit, d.h. $\tau = \frac{t}{N}$, dann ist

$$P_{t,N}^c = \left[1 - 3\left(\frac{ct}{N}\right)^2 + 2\left(\frac{ct}{N}\right)^3\right]^N \xrightarrow{N\to\infty} \exp\left(-\frac{3c^2t^2}{N}\right) \xrightarrow{N\to\infty} 1$$

10.3 Quantenfehler

Wie im klassischen Fall können Speicherfehler und Rechenfehler (Operationsfehler) unterschieden werden. Ist der Quantencomputer mit Spins realisiert, dann können die Spins umklappen, d.h. der Zustand

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

geht nach einer Zeit τ über in den Zustand

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

Auch ein Phasenverschub ist möglich. Verschiebt sich die Phase um π, dann geht $|\psi\rangle$ über in

$$\sigma_z|\psi\rangle = c_0|0\rangle - c_1|1\rangle$$

[34] es gibt drei Möglichkeiten: $000 \to 001$, 010 und 100

[35] Bei Fehlern in zwei oder drei Codierbits versagt natürlich die Korrektur

10.4 Quantenfehlerkorrektur

Codierung und Fehlerwahrscheinlichkeit

Um Umklappprozesse korrigieren zu können, kann folgende redundante Codierung verwendet werden

$$\begin{aligned} |0\rangle_L &\rightarrow |000\rangle \\ |1\rangle_L &\rightarrow |111\rangle \end{aligned}$$

während bei Phasenverschub um π folgende redundante Codierung sinnvoll ist:

$$\begin{aligned} |0\rangle_L &\rightarrow |++\!+\rangle \qquad |\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right) \\ |1\rangle_L &\rightarrow |--\!-\rangle \qquad \text{da } \sigma_z|\pm\rangle = |\mp\rangle \end{aligned}$$

Im folgenden betrachten wir zunächst nur Umklappfehler.
Die Wahrscheinlichkeit für Fehler beträgt vor der Korrektur

- $(1-P_\tau)^3$ daß kein Fehler aufgetreten ist.
- $3*(1-P_\tau)^2 P_\tau$ daß ein Spin umgeklappt ist.
- $3*(1-P_\tau)P_\tau^2$ daß zwei Spins umgeklappt sind.
- P_τ^3 daß alle drei Spins umgeklappt sind.

Die Fehlerkorrektur läuft nun in folgenden Schritten ab:

- Zuerst erfolgt eine Messung mit

  $$P = |000\rangle\langle 000| + |111\rangle\langle 111|$$

  Ist der Messausgang positiv, dann ist kein Fehler aufgetreten und das Verfahren ist beendet. *Ansonsten*

- erfolgt eine Messung

  $$P = |100\rangle\langle 100| + |011\rangle\langle 011|.$$

  Ist diese positiv, dann wird der Fehler durch Anwendung von σ_x^1 korrigiert. Bei negativem Ergebnis

- erfolgt eine Messung

$$P \;=\; |010\rangle\langle 010| + |101\rangle\langle 101|.$$

  Ist diese positiv, dann wird der Fehler durch Anwendung von σ_x^2 korrigiert ansonsten muß der Fehler im dritten Bit aufgetreten sein und daher wird σ_x^3 zur Korrektur angewendet.

Die Wahrscheinlichkeit, daß die Korrektur erfolgreich war, beträgt

$$P^{\text{korr}} \;=\; (1-P_\tau)^3 + 3P_\tau(1-P_\tau)^2 > (1-P_\tau) \qquad \text{falls } P_\tau \lesssim \frac{1}{2}.$$

Wächst die Fehlerwahrscheinlichkeit z.B. linear mit der Zeit, d.h. $P_\tau = c\tau$ und korrigieren wir N mal in der Zeit t, d.h. $\tau = \frac{t}{N}$ dann beträgt die Wahrscheinlichkeit für ein korrektes Resultat

$$\begin{aligned} P_t^{\text{korr}} \quad &= \quad (1-3P_\tau^2+2P_\tau^3)^N \simeq \left(1-3\left(\frac{ct}{N}\right)^2+2\left(\frac{ct}{N}\right)^3\right)^N \\ &\xrightarrow{N\to\infty} \quad e^{-3\left(\frac{ct}{N}\right)^2 N} = e^{-3\frac{(ct)^2}{N}} \xrightarrow{N\to\infty} 1. \end{aligned}$$

Allgemeiner Fall

Während die Fehlerkorrektur problemlos für einen der Fehlerfälle (*entweder* Spinumklapp *oder* Phasenverschub um π) funktioniert, ist der allgemeine Fall etwas komplizierter. Die Überlegungen hierzu entstammen [31], [32] und [29]. Die Idee besteht darin, das System in einen größeren HILBERTraum einzubetten, so daß die verschiedenen Fehlermöglichkeiten auf jeweils andere Unterräume abgebildet werden.
Im folgenden gibt k die Anzahl der Qubits im ursprünglichen System (im Hilbertraum $\mathcal{H}_L$ mit der Dimension 2^k) an, während n die Anzahl der zum codieren verwendeten Qubits (im Hilbertraum $\mathcal{H}$ mit der Dimension 2^n) bezeichnet.

$$k \text{ Qubits} \to n \text{ Qubits}$$

Alle möglichen Operatoren, und damit auch die Fehleroperatoren[36], lassen sich in PAULImatrizen entwickeln. Damit ist ein allgemeiner Fehler

$$\begin{aligned} A_L \;&=\; \sum_{\alpha_1\ldots\alpha_{\tilde{k}}} c_{\alpha_1}\ldots c_{\alpha_{\tilde{k}}} E^{j_1\ldots j_{\tilde{k}}}_{\alpha_1\ldots\alpha_{\tilde{k}}} \qquad \tilde{k} \le k \\ E^{j_1\ldots j_{\tilde{k}}}_{\alpha_1\ldots\alpha_{\tilde{k}}} \;&=\; \sigma^{j_1}_{\alpha_1}\sigma^{j_2}_{\alpha_2}\ldots\sigma^{j_{\tilde{k}}}_{\alpha_{\tilde{k}}} \qquad j_m \neq j_n \text{ für } n \neq m \end{aligned}$$

[36] hier werden nur unitäre Fehleroperatoren betrachtet

Hierbei ist $\sigma_0^i = \mathbb{1}^i$, $\alpha_i \in \{0,1,2,3\}$ und $c_l \in \mathbb{C}$. Die Summe läuft über alle möglichen Anordnungen von $\alpha_1 \ldots \alpha_{\tilde{k}}$.
Wie viele mögliche Fehler gibt es maximal?

$$\sum_{l=0}^{k} \underbrace{3^l}_{\text{(a)}} \underbrace{\frac{n!}{(n-l)!l!}}_{\text{(b)}} =: N(n)$$

Es wirken zwischen 0 und k Operatoren, an jeder dieser Positionen wirkt einer der PAULI-Matrizen, daher gibt es bei l Operatoren jeweils (a) 3^l Verteilmöglichkeiten der PAULI-Operatoren auf die Plätze. Da insgesamt n Plätze zur Verfügung stehen geht in (b) noch die Zahl der möglichen Anordnungen der l Fehleroperatoren auf die n Plätze ein.
Soll das Bild unter zwei verschiedenen Fehleroperationen in jeweils zwei orthogonale Unterräume von $\mathcal{H}$ abgebildet werden, muß $\mathcal{H}$ über genügend Zustände verfügen, d.h.

$$2^k N(n) \leq 2^n \quad = \quad \dim(\mathcal{H})$$

Ist z.B. $k = 1$, dann ergibt sich durch Einsetzen in die obige Formel, daß

$$2^1 * (1 + 3n) \leq 2^n$$

sein muß. Dies wird ab $n = 5$ erfüllt.
Damit ergibt sich für die Fehlerkorrektur folgendes Verfahren:

1. Das System von k Qubits wird auf $\mathcal{H}$ abgebildet: $\mathcal{H}_L \rightarrow K(\mathcal{H}_L) \subset \mathcal{H}$
2. Ein Fehler bildet $K(\mathcal{H}_L)$ mittels A_L auf einen anderen Unterraum von $\mathcal{H}$ ab. Nach Konstruktion ist der Unterraum eindeutig einem Fehleroperator A_L zugeordnet.
3. Durch sukzessive Projektion auf die einzelnen Unterräume von $\mathcal{H}$ wird der Unterraum ermittelt, in dem sich das System befindet. Da alle Unterräume orthogonal zueinander sind, wird nur in einem Unterraum ein positives Meßergebnis erzielt.
4. Da alle PAULI-Operatoren idempotent sind, kann durch erneute Anwendung des (jetzt bekannten) Fehleroperators der Fehler rückgängig gemacht werden (d.h. es wird wieder in den ursprünglichen Unterraum zurückprojeziert).

Schematisch:

$$|\psi\rangle \xrightarrow{\text{Einbettung}} K(|\psi\rangle) \xrightarrow{\text{Fehler}} A_L K(|\psi\rangle) \xrightarrow{\text{Korrektur}} A_L^2 K(|\psi\rangle) = K(|\psi\rangle)$$

11 Quantenalgorithmen

11.1 Shors Faktorisierungsalgorithmus

Neben der Originalarbeit von SHOR wird in [28] sowie in [36] der Algorithmus vorgestellt. Die mathematischen Beweise können gängigen Lehrbüchern über Zahlentheorie entnommen werden, z.B. [33] oder dem eher populärwissenschaftlichen [34].

Theorem 10 *Sind p, q Primzahlen mit $N = pq$ und $a \in \mathbb{N}$, $a < N$ eine Zufallszahl die $1 = ggT(a, N)$ erfüllt*[37] *und*

$$f_{a,N}(x) \;:=\; a^x \mod N \qquad x \in \mathbb{N}$$

eine (offensichtlich) periodische Funktion mit der Periode r, dann gilt:
Ist r gerade und $a^{\frac{r}{2}} \mod N \neq N-1$

$$\Rightarrow \qquad p, q \;=\; ggT\left(a^{\frac{r}{2}} \pm 1, N\right)$$

Hierbei sind folgende Punkte anzumerken:

- Zur Ermittlung des ggT existiert seit EUCLID ein Algorithmus mit polynomialer Laufzeit.
- Die Zahlentheorie liefert die (nicht triviale) Aussage, daß bei zufälliger Wahl $P(r \text{ gerade}) > \frac{1}{2}$ ist.
- Für klassische Computer liefert das Theorem keinen Vorteil, da für die Ermittlung der Periode nur klassische Algorithmen mit exponentieller Laufzeit bekannt sind. Die besten Algorithmen haben eine Laufzeit von $O\left(\exp(\log_2 N)^{\frac{1}{3}}\right)$.

Beispiel

Es soll die Zahl $N = 15 = 3 * 5$ faktorisiert werden. Wähle a coprim mit N, d.h. $a \in \{2, 4, 7, 8, 11, 13, 14\}$, z.B. $a = 7$. Damit ergibt sich für $f_{7,15}(x) = 7^x \mod N$ folgende Wertetabelle:

x	0	1	2	3	4	5
$f(x)$	1	7	4	13	1	7

[37] diese Eigenschaft wird als Coprim bezeichnet

Die Periode r ist also 4 und insbesondere gerade. Ferner ist $a^{\frac{r}{2}} = 7^2 = 49$ coprim mit $N = 15$. Damit sind die Primfaktoren

$$5, 3 \quad = \quad \text{ggT}\,(49 \pm 1, 15)$$

Analog lassen sich auch die anderen möglichen Werte für a verwenden:

a	2	4	7	8	11	13	14
r	4	2	4	4	2	4	2

Offensichtlich sind alle r gerade, allerdings eignet sich 14 wegen $14^{\frac{r}{2}} = 14 \mod 15 = 14$ nicht als Startwert.

Quantenmechanisches Ermitteln der Periode

Ist $N \sim O(2^L)$ dann wird der Algorithmus mit Hilfe von $2L$ Qubits, jeweils in zwei Registern, wie folgt durchgeführt:

1. Durch eine unitäre Transformation[38] wird in dem ersten Register eine Überlagerung aller Eingaben erzeugt:

$$|0\rangle|0\rangle \quad \rightarrow \quad \frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} |x\rangle|0\rangle$$

2. Als nächstes wird die zu $f_{a,N}$ gehörende unitäre Transformation U_f angewendet:

$$U_f \frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} |x\rangle|0\rangle = \frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} |x\rangle|f_{a,N}(x)\rangle$$

   Ist wie oben $N = 15$, $a = 7$ und damit $L = 4$ dann liegt nach diesem Schritt der Zustand

$$\frac{1}{64}\left(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + |5\rangle|7\rangle + \cdots + |255\rangle|13\rangle\right)$$

   vor.

3. Durch Messung des zweiten Registers wird ein Zustand herausprojeziert. In unserem Beispiel kann beim Messen des zweiten Zustandes $|1\rangle$, $|7\rangle$, $|4\rangle$ oder $|13\rangle$ auftreten. Wird z.B. $|4\rangle$ gemessen, so lautet der Zustand:

$$\left(|2\rangle + |6\rangle + |10\rangle + |14\rangle + \cdots + |254\rangle\right)|4\rangle$$

[38] s. unten für die Beschreibung dieser Transformation

Hätten wir stattdessen $|13\rangle$ erhalten, so lautete der Gesamtzustand nach der Messung

$$(|3\rangle + |7\rangle + |11\rangle + |15\rangle + \cdots + |255\rangle)\,|13\rangle$$

Offensichtlich ist die Periode jetzt im ersten Register kodiert. Als nächstes wird das erste Register gemessen und danach erneut ein Zustand präpariert usw.

Nach einigen Durchläufen ist dreimal das gleiche zweite Register gemessen worden, z.B. $|13\rangle$. Ist bei der jeweils darauf folgenden Messung des ersten Registers zudem in allen drei Fällen eine verschiedenes Qubit gemessen worden, z.B. $|23\rangle$, $|11\rangle$ und $|3\rangle$ dann kann die gesuchte Periode ermittelt werden, indem der ggT der *Differenzen* der Ergebnisse im ersten Register ermittelt werden, in unserem Beispiel ist

$$\mathrm{ggT}\,(23-11, 11-3) \;=\; \mathrm{ggT}\,(12,8) = 4$$

Der Nachteil dieser Methode besteht darin, daß mindestens dreimal der gleiche Wert im zweiten Register gemessen werden muß und in den dazugehörigen Messungen des ersten Registers jeweils ein anderer Wert im ersten Register gemessen werden muß[39]. Damit wächst die Rechenzeit wieder exponentiell mit N.

Das Problem besteht konkret darin, daß für jeden möglichen Wert im zweiten Register, die Werte im ersten Register nicht identisch, sondern um einen Startwert[40] verschoben sind, d.h.

$$|\psi\rangle \;=\; \xi \sum_{j=0}^{[\frac{2^{2L}}{r}]} |jr + l\rangle$$

Hierbei ist ξ eine für diese Betrachtung unwesentliche Normierungskonstante und l der Offset. Mit $[x]$ wird der ganzzahlige Anteil von x bezeichnet.

In unserem Beispiel ergibt sich also

Zweites Reg.	Erstes Register	Startwert
1	$\|0\rangle+\|4\rangle+\|8\rangle+\ldots+\|252\rangle$	0
4	$\|2\rangle+\|6\rangle+\|10\rangle+\ldots+\|254\rangle$	2
7	$\|1\rangle+\|5\rangle+\|9\rangle+\ldots+\|253\rangle$	1
13	$\|3\rangle+\|7\rangle+\|11\rangle+\ldots+\|255\rangle$	3

[39] Ein weiterer Nachteil besteht darin, daß bei der ggT-Bildung auch ein Vielfaches der Periode r gemessen werden kann

[40] engl. Offset

Wäre der Startwert immer 0, dann könnte schon nach wenigen Messungen die Periode ermittelt werden.

4. Diskrete Fourier-Transformation

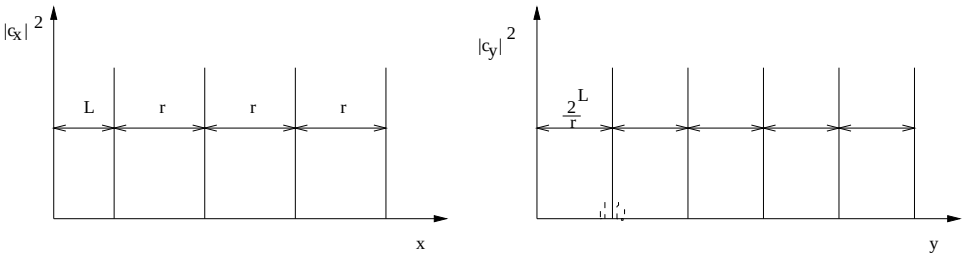
   Durch die DFT wird der Startwert in eine irrelevante Phase umgewandelt. Die unitäre Transformation der DFT ergibt sich zu

$$\begin{aligned} U_{\mathrm{DFT}}|x\rangle &= \frac{1}{2^L}\sum_{y=0}^{2^{2L}-1}\exp\left(i\frac{2\pi xy}{2^{2L}}\right)|y\rangle \\ U_{\mathrm{DFT}}\sum_x c_x|x\rangle &= \sum_y \tilde{c}_y|y\rangle \qquad \text{mit} \\ \tilde{c}_y &= \frac{1}{2^L}\sum_{x}^{2^{2L}-1}\exp\left(i\frac{2\pi xy}{2^{2L}}\right)c_x \end{aligned}$$

   Teilt r 2^{2L}, dann ergibt die DFT bei unserem Zustand[41]

$$U_{\mathrm{DFT}}|\psi\rangle = \frac{1}{\sqrt{r}}\sum_{r=1}^{r-1}\exp\left(i\frac{2\pi lj}{r}\right)|j\frac{2^{2L}}{r}\rangle$$

   Wenn r nicht 2^{2L} teilt, dann ergeben sich exponetiell abklingende Seitenbänder (s. dazu [36]).



Effizienz des Algorithmus

An zwei Stellen im Algorithmus werden zufällige Werte betrachtet:

1. Die Wahl von a. Dies ist unproblematisch, da $p_{a\,\mathrm{ok}} \geq \frac{1}{2}$ unabhängig von N.

2. Die Periode r teilt 2^{2L} nicht (der Normalfall). Die entstehenden Seitenbänder bedeuten, daß die richtige Periode nur mit einer bestimmten Wahrscheinlichkeit p_r ermittelt wird. Da p endlich ist kann durch wiederholte Messung auch hier r bestimmt werden.

[41] rechts im Ket hoch $2L$ oder hoch L ?

Da die Berechnung von $f_{a,N} \sim O(L^3)$ skaliert und für die DFT Algorithmen mit DFT$\sim O(L\log(L))$ existieren (via Fast Fourier Transformation (FFT)) läuft also SHORs Quantenfaktoriesiralgorithmus in QFT$\sim O(L^3)$. Verglichen mit der klassischen Laufzeit $O(\exp(L^{\frac{1}{3}}))$ bedeutet dies also eine exponentielle Beschleunigung.

11.2 Grovers Suchalgorithmus

Auch wenn dieser Algorithmus weniger spektakulär als SHORs Algorithmus ist, so lohnt es sich dennoch, den von GROVER in [35] vorgestellten Suchalgorithmus näher zu betrachten.
Das Problem besteht darin, ein Element aus einer Menge zu finden. Als Beispiel kann hier die sogenannte Bierdeckelfunktion betrachtet werden: einer Telephonnummer soll der zugehörige Name zugeordnet werden. Der Quantenalgorithmus benötigt hier $O(\sqrt{N}) = O(2^{\frac{L}{2}})$ Schritte, wobei N die Mächtigkeit der zu durchsuchenden Menge ist (Anzahl der Einträge im Telephonbuch). Ein klassischer Algorithmus skaliert mit $\frac{N}{2}$.
Im folgenden werden die Einträge $x = 0, \ldots, N-1$ betrachtet. Jeder Eintrag trägt eine Bezeichnung S_v ($\nu = 0, \ldots, N-1$). Diese Bezeichnung entspricht den Namen. Jedem Eintrag ist zudem eine Eigenschaft C_v (die Telephonnummer) zugeordnet. Die Funktion C_v ist also der Gestalt, daß

$$C_\nu(S_x) = \begin{cases} 1 & \text{falls} \quad x = \nu \\ 0 & \text{falls} \quad x \neq \nu \end{cases}$$

Grovers Algorithmus: Überblick

Zuerst soll in einem Überblick erläutert werden, wie der Algorithmus *arbeitet*, der Beweis für das Funktionieren folgt unten. Bei dem im folgenden verwendeten L-qubit-Register entspricht jeder mögliche $|x\rangle$ einem S_x.

1. Zuerst wird das L-qubit-Register in dem Zustand $|0\rangle$ präpariert.
2. Als nächstes wird die sogenannte HADAMARD-Transformation durchgeführt, d.h. auf jedes Qubit wird die Operation U_A (s. S. 68 für Definition) angewendet.

$$\begin{aligned} |\psi\rangle &= U_A \otimes \cdots \otimes U_A |0 \ldots 0\rangle \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{2^{\frac{L}{2}}} \sum_{x=0}^{2^L - 1} |x\rangle \end{aligned}$$

Nach dieser Operation[42] befindet sich im Register eine lineare Überlagerung aller möglichen Zustände, wobei zudem bei einer Messung alle Zustände gleichwahrscheinlich sind.

3. Ungefähr $\sqrt{N}$ mal (die genaue Zahl wird unten ermittelt) müssen jetzt die folgende Operationen durchgeführt werden:

   (a) Zuerst wird der Operator U_{C_ν} angewendet:

   $$\begin{aligned} U_{C_\nu}|\nu\rangle &= -|\nu\rangle \\ U_{C_\nu}|x\rangle &= |x\rangle \text{ für } x \neq \nu \end{aligned}$$

   Dieser Operator ist „gegeben“, d.h. es gibt keine Möglichkeit, ihn zu analysieren.

   (b) Danach wird der Operator U_D angewendet:

   $$U_D = -U_H^\dagger U_{C_0} U_H$$

   Hierbei ist U_H die obige HADAMARD-Transformation und $U_{C_0} = U_{C_\nu}$ mit $\nu = 0$.

4. Nach diesen Operationen wird das Register gemessen. Mit einer Wahrscheinlichkeit von ca. 50 % befindet sich der Zustand $|\nu\rangle$ im Register.

Beweis des Algorithmus

Nach Konstruktion haben alle Anfangszustände reelle Phasen, durch die angewendeten Operatoren U_D und U_{C_ν} bleiben sie reell (was nicht unbedingt bedeutet, daß sie *während* einer Operation nicht doch komplex sein können) was die Betrachtungen erheblich vereinfacht.
Die Wirkung von U_{C_ν} ist offensichtlich während die Wirkung von U_D eine genauere Betrachtung erfordert. Dafür ist es sinnvoll, den Mittelwert der

[42] Die allgemeine HADAMARD-Transformation wird auf einen beliebigen Anfangszustand $|x\rangle$ angewendet:

$$U_H|x\rangle = \frac{1}{2^{\frac{L}{2}}} \sum_y (-1)^{xy}|y\rangle$$

Die Summe läuft hierbei über alle möglichen Kombinationen von x und y.**Stimmt das so ??**

Koeffizienten der Basiskets zu betrachten:

$$\begin{aligned} |\psi\rangle &= \sum_{i=0}^{2^L-1} \alpha_i |i\rangle \qquad \text{und damit} \\ \alpha &= \frac{1}{2^L} \sum_{i=0}^{2^L-1} \alpha_i \end{aligned}$$

Die Wirkung von U_D besteht nun in einer Inversion um den Mittelwert, d.h. die Koeffizienten α_i gehen unter U_D wie folgt in α_i' über:

$$\alpha_i = \alpha + (\alpha_i - \alpha) \quad \xrightarrow{U_D} \quad \alpha_i' = \alpha - (\alpha_i - \alpha) = 2\alpha - \alpha_i$$

Dies läßt sich durch explizites Betrachten der Schritte zeigen:

$$\begin{aligned} U_D|\psi\rangle &= -U_H^\dagger U_{C_0} \sum_{i=0}^{2^L-1} \sum_{k=0}^{2^L-1} \alpha_i \frac{(-)^{ik}}{\sqrt{2^L}} |k\rangle \\ &= -U_H^\dagger U_{C_0} \left(\sum_{i=0}^{2^L-1} \alpha_i \frac{1}{\sqrt{2^L}} |0\rangle + \sum_{i=0}^{2^L-1} \sum_{k=1}^{2^L-1} \alpha_i \frac{(-)^{ik}}{\sqrt{2^L}} |k\rangle \right) \\ &= -U_H^\dagger (-\sqrt{2}^L \alpha |0\rangle + U_H|\psi\rangle - \sqrt{2}^L \alpha |0\rangle) \\ &= 2\alpha \sum_{i=0}^{2^L-1} |i\rangle - |\psi\rangle \end{aligned}$$

Damit gilt also für jedes i das $\alpha_i' = 2\alpha - \alpha_i$ ist.
Beim ersten Schritt wird $|\nu\rangle$ deutlich unter den Mittelwert abgesenkt um dann bei der Inversion um den Mittelwert deutlich überhöht zu werden. Somit ist bereits nach dem ersten Schritt die Wahrscheinlichkeit $|\nu\rangle$ zu messen, größer als für alle anderen Zustände.
Um die Entwicklung der Zustände unter iterativer Anwendung der Operationen U_{C_ν} und U_D zu verstehen, ist es sinnvoll zu bemerken, daß sich der Zustand $|\psi(n)\rangle$ immer als

$$|\psi(n)\rangle = \sum_{i \neq \nu} \alpha(n)|i\rangle + \alpha_\nu(n)|\nu\rangle$$

schreiben läßt, da die Operatoren auf alle $i \neq \nu$ stets identisch wirken. Bei der Operation U_D bleibt zudem der Mittelwert erhalten, denn

$$\alpha = \frac{1}{2^L} \sum_{i=0}^{2^L-1} \alpha_i = \frac{1}{2^L} \sum_{i=0}^{2^L-1} \alpha_i' = \frac{1}{2^L} \sum_{i=0}^{2^L-1} (2\alpha - \alpha_i) = 2\alpha - \alpha = \alpha.$$

Nun läßt sich eine Rekursionsformel für den Mittelwert $\alpha(n)$ (der unter der Gesamttransformation *nicht* erhalten ist da er durch U_{C_ν} geändert wird) und $\alpha_\nu(n)$ aufstellen:

$$\begin{aligned}\alpha(n+1) &= \alpha(n) - 2\epsilon\alpha_\nu(n) \quad \text{mit } \epsilon := \frac{1}{2^L} \\ \alpha_\nu(n+1) &= 2(\alpha)_{U_{C_\nu}} - (\alpha_\nu)_{U_{C_\nu}} = 2\alpha(n) - 4\epsilon\alpha_\nu(n) + \alpha_\nu(n)\end{aligned}$$

Einfacher läßt sich diese lineare Gleichung in Matrixschreibweise schreiben:

$$\begin{pmatrix} \alpha(n+1) \\ \alpha_\nu(n+1) \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & -2\epsilon \\ 2 & 1-4\epsilon \end{pmatrix}}_{:=A} \begin{pmatrix} \alpha(n) \\ \alpha_\nu(n) \end{pmatrix}$$

Um die Wirkung der Iteration berechnen zu können, muß eine Basis gewählt werden, in der A diagonal ist. Wird der Startvektor entsprechen gedreht, folgt damit:

$$\begin{aligned}\begin{pmatrix} \alpha(0) \\ \alpha_\nu(0) \end{pmatrix} &= \begin{pmatrix} \sqrt{\epsilon} \\ \sqrt{\epsilon} \end{pmatrix} = \alpha_1\vec{e}_1 + \alpha_2\vec{e}_2 \\ A^M \begin{pmatrix} \sqrt{\epsilon} \\ \sqrt{\epsilon} \end{pmatrix} &= \alpha_1\lambda_1^M\vec{e}_1 + \alpha_2\lambda_2^M\vec{e}_2\end{aligned}$$

Hierbei sind $\vec{e}_i$ die Eigenvektoren und λ_i die Eigenwerte von A. Physikalisch machen weder Eigenwerte größer 1 Sinn, da damit der Mittelwert beliebig groß werden kann, noch der Fall, das beide Eigenwerte kleiner als 1 sind, da dann sowohl Mittelwert als auch α_ν gegen 0 gingen, was aber nicht der Fall sein kann, da alle Operationen unitär und mithin eigenwerterhaltend sind.
Die Eigenwerte von A sind

$$\lambda_j = 1 - 2\epsilon \pm 2i\sqrt{\epsilon - \epsilon^2} = 1 \pm iO(\sqrt{\epsilon}) \approx e^{i\varphi} \qquad \varphi \approx O(\sqrt{\epsilon})$$

Eine genauere Betrachtung in [37] zeigt, daß

$$a_\nu(n) = \sin((2n+1)\Theta) \qquad \text{mit} \qquad \sin^2\Theta = \epsilon$$

ist. Das Maximum von a_ν wird also erreicht, wenn $(2n+1)\Theta = \frac{\pi}{2}$ ist; weitere Iterationen verringern die Wahrscheinlichkeit, den gesuchten Zustand $|\nu\rangle$ zu messen, wieder. Somit muß die Operation optimalerweise

$$n = \frac{\pi}{4}\frac{1}{\Theta} \approx \frac{1}{\sqrt{\epsilon}} = \sqrt{N}$$

mal durchgeführt werden. Da das Ergebnis zudem nur mit einer gewissen Wahrscheinlichkeit gemessen wird, sind u.U. mehrere Durchläufe notwendig, so daß wie behauptet der Algorithmus eine Laufzeit von $O(\sqrt{N})$ besitzt.

11.3 Weitere Algorithmen

Neben diesen zwei grundlegenden Algorithmen gibt es noch eine Reihe von weiteren quantenmechanischen Berechnungsmöglichkeiten wie z.B. das Summenproblem der Zahlentheorie (auch als Diskrete Logarithmen bezeichnet), das SHOR allerdings auf die Periodenfindung zurückführte. Auch viele andere Algorithmen sind lediglich Varianten entweder von SHORs oder GROVERs Algorithmus.

12 Experimentelle Realisation

Zur experimentellen Verwirklichung von Quantencomputern werden verschiedene Ansätze verfolgt. Ein Möglichkeit besteht darin, daß die Kernspins die Zustände repräsentieren und man mittels Verfahren der NMR[43]-Spektroskopie gezielt Zustände besetzt und ausliest. Trotz des Vorteils der schwachen Störung des Kernes von außen ist diese Möglichkeit noch nicht weit verfolgt worden. Eine Grund dafür ist die Begrenzung der Anzahl der Qubits. Das Register würde aus einem Molekül bestehen, dessen Atomkerne die Zustände darstellen. Dies begrenzt die Ausdehnung des Registers.

12.1 Ionenfalle

In einer Ionenfalle hingegen werden einzelne Ionen gefangen und in einer linearen Falle aneinandergereiht. Die Ionen müssen dazu sehr tief herunter gekühlt werden, aber für einzelne Ionen ist dies mit Fallen machbar. Der Prototyp einer solchen Falle ist auch als Paul-Falle bekannt, der dafür einen Nobelpreis erhielt. Mehrere Ionen in einer Falle sind der Coulomb-Abstoßung untereinander ausgesetzt. Cirac und Zoller haben in [38] eine einführende Darstellung einer solchen Falle gegeben. Es empfiehlt sich, z.B. diesen Text als Referenz heranzuziehen.
Eine Ionenfalle besteht aus einem schnell oszillierendem Wechselfeld, das ein harmonisches anziehendes Potential in einer Raumrichtung und ein harmonisches abstoßendes in der anderen Raumrichtung erzeugt. Durch die zeitliche Mittelung dieses schnell oszillierenden Feldes entsteht ein effektives harmonisches Potential. Das darin gefangene Atom läßt sich darum bezüglich seiner Bewegung als harmonischer Oszillator beschreiben (Nullpunktsenergie, gleiche Abstände der Niveaus etc.). Wenn die Ausdehnung des Potentials relativ gering ist, spricht man von „steifem Potential“. Das „Lamb-Dicke-Limit“ kennzeichnet genau diese Situation: Das Atom ist auf einen Raumbereich eingeschnürt, der viel kleiner ist als die Wellenlänge des eingestrahlten Laserlichtes. Die gleiche Tatsache wird durch die Bedingung $h\nu \gg E_{\text{Photonrückstoß}}$ beschrieben. Die Frequenz ν ist dabei die Frequenz des Modes.
Dieses Bild aus der Festkörperphysik kann so weit ausgedehnt werden, daß man von Phononen spricht, deren Anzahl den Energieinhalt einer bestimmten Mode bestimmt. (Viele Phononen $\sim$ große Auslenkung des Atoms um den Gleichgewichtspunkt mit Modenfrequenz).
In diesem Bild sagt die Bedingung aus, daß die Phononenenergie größer sein muß als die Aufprallenergie eines Laserphotons, damit die Lamb-Dicke-

[43]Nuclear Magnetoresistance Spectroscopy

Näherung gilt. Da sich die Aufprallenergie eines Laserphotons zu

$$E_R = \frac{\hbar^2 k^2}{2\mu} \qquad \frac{E_R}{\hbar} \sim 1 \ldots 10\text{kHz}$$

ergibt (μ ist die reduzierte Masse des Ions) und $\nu \sim 10^2$ kHz, ist dieses Limit sicher gegeben.
Der LAMB-DICKE-Parameter η ergibt sich zu

$$\eta = \frac{2\pi}{\lambda_{\text{Laser}}} \cdot \underbrace{a}_{\text{Fallengröße}} \ll 1$$

Wie kühlt man so tief?
Eine Art der fortgeschrittenen Kühlung ist das sog. „sideband-cooling“, bei dem mit zwei verschiedenen elektronischen Zuständen gearbeitet wird. Der Laser ist relativ zum Übergang leicht ins Rote verschoben, und wenn ein Atom in Richtung Laserstrahl fliegt, bewirkt die Dopplerverschiebung, daß das Licht nun genau auf der Resonanz des Atoms liegt. Das Photon wird absorbiert, und das Atom hat einen Impuls entgegen der Bewegungsrichtung erfahren. Kurze Zeit später wird ein Photon emittiert, das Atom kehrt in seinen Grundzustand zurück. Im Mittel wird diese spontane Emisssion in alle Richtungen stattfinden, und daher erhält das Atom hier im Mittel keinen Rückstoß. Das Atom ist dann wieder aufnahmefähig für ein weiteres Photon aus dieser Laserrichtung. Dieser Prozeß wiederholt sich, bis das Atom nahezu zum Stillstand kommt. Da der Laser auf einer Seite der Resonanzlinie liegt, spricht man auch von „Seitenband-Kühlung“.
Zur mathematischen Behandlung der Falle soll nur der 1D-Fall betrachtet werden, da sich die anderen Dimensionen separieren lassen. Das Atom befindet sich im Knoten des stehenden Laserfeldes (auf der anderen Seite steht auch ein Laser, und beide Wellen bilden zusammen die stehende Welle). Wir benutzen den semiklassischen Formalismus (E-Feld nicht quantisiert), mit den atomaren Zuständen $|g\rangle$, $|f\rangle$ und der RABI-Frequenz $\Omega = \underbrace{d}_{\text{Dipoloperator}} \underbrace{E}_{\text{Feldstärke}}$. Die Wechselwirkungsfunktion lautet (in Rotating-Wave Approximation, die Grundzustandsenergie sei 0, daher kein $|g\rangle$-Term):

$$H = \underbrace{-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + \mu\frac{\nu^2 x^2}{2}}_{Bewegung} + \hbar\omega_0 |f\rangle\langle f|$$
$$+ \frac{\Omega}{2} \underbrace{\sin(kx)}_{stehendeWelle} \left(|f\rangle\langle g| e^{-i\omega_2 t} + |g\rangle\langle f| e^{i\omega_2 t}\right)$$

Es soll nun auch die Bewegung des Atoms quantisiert werden (⇒ Phononen). Anstatt die Auslenkung des Atoms festzulegen („x^2“), wird ein „Phononenzähloperator“ $a^\dagger a$ eingeführt:

$$kx \sim \eta(a^\dagger + a) \quad \sin(kx) \approx kx, \quad x^2 \approx a^\dagger a$$

Terme höherer Ordnung werden vernachlässigt, so daß

$$H \approx k\nu a^\dagger a + \hbar\omega_0 |f\rangle\langle f| + \frac{\Omega}{2}\eta(a + a^\dagger)\left(|f\rangle\langle g| e^{-im\omega t} + \text{h.c.}\right)$$

h.c. = hermitisch konjugiert. Da wir spontane Emission vernachlässigen (verbotene Dipolübergänge), können wir ins Wechselwirkungsbild übergehen und allein die Wechselwirkung betrachten:

$$H_{WW} = \frac{\eta\Omega}{2}(a^\dagger e^{i\nu t} + a e^{-i\nu t})\left(|f\rangle\langle g| e^{-i\delta t} + |g\rangle\langle f| e^{i\delta t}\right)$$

wobei die Verstimmung (detuning) $\delta = \omega_L - \omega_0$ verstellbar und $\delta \approx \nu$ ist. Das gesamte Atom läßt sich nun z.B. durch den Zustand $|g, 2\rangle$ beschreiben: Grundzustand, leichte Schwingung. Der Vorgang der Laserkühlung läßt sich nun als kaskadenförmiges Schema veranschaulichen. Das Atom fällt von hohen Phononenzuständen immer tiefer, bis es den Grundzustand erreicht (Nullpunktsschwingung). Diese Prozedur ist schon zweidimensional experimentell verwirklicht worden, man siehe dazu Arbeiten von Wineland am NIST oder Toschek & Blatt. Das Abkühlen bis in den Grundzustand kann auch für Präzisionspektroskopie und Zeitstandards Anwendung finden. Nachdem das Atom so herunter gekühlt wurde, werden die Qubits durch die inneren Zustände des Atoms repräsentiert. Betrachten wir den Fall mit zwei Ionen.

12.2 2 Ionen in der Falle

Die Falle kann nun in einer Dimension (x-Richtung) ausgedehnt werden. Ion für Ion wird in immer gleichem Abstand hinzugefügt, bis die gewünschte Fallengröße mit N Ionen erreicht ist. Die Falle ist nun asymmetrisch, es gilt $\hbar\nu_y, \hbar\nu_z \gg \hbar\nu_x \gg E_k$. Wir betrachten hier nur den Fall 2 Ionen, N Ionen bringen konzeptionell nichts neues.
Zur Herleitung verwenden wir klassiche Größen, d.h. die Schwingungsmoden der Atome in der Falle werden noch nicht quantisiert. Dann ergibt sich für das Potential

$$\begin{aligned} V(x_1, x_2) &= \frac{M\nu^2}{2}x_1^2 + \frac{M\nu^2}{2}x_2^2 + \frac{\alpha}{|x_1 - x_2|} \\ E_{kin} &= \frac{p_1}{2M} + \frac{p_2}{2M} \end{aligned}$$

mit einer Transformation ins Schwerpunktssystem (CM-Trafo):

$$x_{CM} = \frac{x_1 + x_2}{2}, \quad x_{rel} = x_1 - x_2, \quad p_{CM} = \frac{p_1 + p_2}{2}, \quad p_{rel} = p_1 - p_2$$

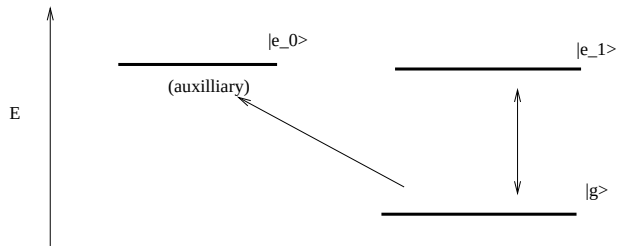
$$H = \frac{1}{2\mu} p_{CM}^2 + \frac{\mu \nu^2 x_{CM}^2}{2} + \frac{\mu_R \nu^2 x_R^2}{2} + \underbrace{\frac{\alpha}{|x_R|}}_{Coulomb} + \frac{p_R^2}{2\mu_R}$$

Mit der Bezeichnung $\bar{x}_R = x_{r,GG}$ für den Ionenabstand am Gleichgewichtspunkt gilt:

$$\mu_r \nu^2 \bar{x}_R - \frac{\alpha}{\bar{x}_R^2} = 0, \quad x_R = x + \bar{x}_R$$

$$\frac{\mu_R \nu^2}{2}(x + \bar{x}_R)^2 + \underbrace{\frac{\alpha}{\bar{x}_R + x}}_{\approx \text{const.}} + \frac{\mu_R \nu^2}{2} x^2 + \underbrace{\frac{\alpha}{\bar{x}_R^3}}_{\mu_R \nu^2} x^2 + \frac{\mu_R 3\nu^2}{2} x^2 \quad \Rightarrow \nu_1 = \sqrt{3}\nu$$

Mit ν_1: Frequenz 1. CM-Mode. Für N Ionen existieren (aufgrund der Kopplung) N Moden des Schwerpunktes. Eine bemerkenswerte Eigenschaft der Ionenfalle ist, daß die Frequenzabstände unabhängig von der Anzahl der Ionen sind.
Experimente verwenden z.B. Be^+-Ionen auf dem (verbotenem Dipol-)Übergang $S_{\frac{1}{2}} \to D_{\frac{1}{2}}$, der eine Halbwertszeit von $\gamma^{-1} \approx 45$ s besitzt. Da $\bar{x}_R \approx 10\mu$m $> \lambda$, sind die einzelnen Ionen bequem durch einen Laser adressierbar. Dabei gilt das Lamb-Dicke-Limit.
Die gemeinsamen Phononenmoden sorgen für eine Verschränkung der Ionen (jedes Ion hatte ja eine zusätzliche Quantenzahl, die die Besetzung des Modes angab). Dies erlaubt Datentransfer untereinander.
Das einzelne Ion befindet sich in einem Knoten der stehenden EM-Welle und stellt nun mit seinen beiden Zuständen ein Qubit dar. Meist wird noch ein dritter Zustand (auxilliary) genutzt. Dieser kann z.B. ein (energetisch entarteter) Zustand $|e_0\rangle$ sein (mit m_j verschieden von $|e_1\rangle$). Dadurch lassen sich die Zustände durch verschiedene Polarisationen (links, rechts-) ansprechen.



Betrachte nun den Fall N Ionen:
Die Wechselwirkungs-HAMILTONfunktion ist

$$H_{WW} = \frac{\eta}{\sqrt{N}} \frac{\Omega}{2} \left(|e_q\rangle\langle g| a \underbrace{e^{-i\phi}}_{\text{Laserphase}} + |g\rangle\langle e_q| a^\dagger e^{i\phi} \right)$$

mit dem LAMB-DICKE-Parameter $\eta = \sqrt{\frac{\hbar k^2 \cos^2(\theta)}{2M\nu_x}}$.
θ gibt den Winkel zwischen Einstrahlrichtung des Lasers und x-Richtung, ϕ die Phasendifferenz zwischen den Lasern an. Der Faktor $\sqrt{N}$ erscheint, weil die effektive Masse des Schwerpunktes NM beträgt, die Amplitude der Schwerpunktsschwingung jedoch mit $\frac{1}{\sqrt{NM}}$ skaliert. Der Index q in $|e_q\rangle$ bezeichnet die magnetische Quantenzahl. Er wird auch für die Polarisation des Lasers verwendet, die den entsprechenden Zustand bevölkert. So ergibt sich dann die Kurzschreibweise Polarisation = 1. Wird ein $k\pi$-Puls auf das $n$te Ion angewendet, so erfordert dies die Zeit $t = \frac{k\pi\sqrt{N}}{\Omega\eta}$, so daß der Operator wie folgt aussieht ($a, a^\dagger$: Phonon-Erzeuger/Vernichter):

$$\hat{U}_n^{k,q}(\phi) = \exp(-iHt) = \exp\left(\frac{-ik\pi}{2} \left(|e_q\rangle\langle g| a e^{-i\phi} + |g\rangle\langle e_q| a^\dagger e^{i\phi} \right) \right)$$

Die Wirkung auf die Zustände $|g\rangle|0\rangle$, $|g\rangle|1\rangle$, $|e_q\rangle|0\rangle$:

$$\begin{aligned}
|g\rangle|0\rangle &\longrightarrow |g\rangle|0\rangle, \quad (\text{da} \quad H|g\rangle|0\rangle = 0 \Rightarrow \hat{U}|g\rangle|0\rangle = \mathbb{1}|g\rangle|0\rangle) \\
|g\rangle|1\rangle &\longrightarrow \cos(\frac{k\pi}{2})|g\rangle|1\rangle - ie^{i\phi}\sin(\frac{k\pi}{2})|e_q\rangle|0\rangle \\
|e_q\rangle|0\rangle &\longrightarrow \cos(\frac{k\pi}{2})|e_q\rangle|0\rangle - ie^{-i\phi}\sin(\frac{k\pi}{2})|g\rangle|1\rangle
\end{aligned}$$

Dies erlaubt die Realisierung von 2-bit Gattern mittels folgender Prozedur:

1. Ein π-Puls mit Polarisation $q = 0$ und $\phi = 0$ regt das $m$te Ion an. Der Zeitentwicklungsoperator ist $\hat{U}_m^{1,0}(0)$.

2. Der Laser auf Ion n wird für die Dauer eines 2π-Pulses angeschaltet. Polarisation ist 1 und Phase ist $\phi = 0$. Der Operator $\hat{U}_n^{2,1}(0)$ ändert das Vorzeichen von $|g\rangle|0\rangle$ durch eine Rotation über $|e_q\rangle|0\rangle$, ohne die anderen Zustände zu beeinflussen.

3. wie Schritt 1.

Die gesamte unitäre Operation $\hat{U}_{m,n} = \hat{U}_m^{1,0}(0)\hat{U}_n^{2,1}(0)\hat{U}_m^{1,0}(0)$ wirkt wie folgt:

$$\begin{aligned}
|g\rangle_m|g\rangle_n|0\rangle &\xrightarrow{\hat{U}_m^{1,0}} |g\rangle_m|g\rangle_n|0\rangle \xrightarrow{\hat{U}_n^{2,1}} |g\rangle_m|g\rangle_n|0\rangle \xrightarrow{\hat{U}_m^{1,0}} |g\rangle_m|g\rangle_n|0\rangle \\
|g\rangle_m|e_0\rangle_n|0\rangle &\longrightarrow |g\rangle_m|e_0\rangle_n|0\rangle \longrightarrow |g\rangle_m|e_0\rangle_n|0\rangle \longrightarrow |g\rangle_m|e_0\rangle_n|0\rangle \\
|e_0\rangle_m|g\rangle_n|0\rangle &\longrightarrow -i|g\rangle_m|g\rangle_n|1\rangle \longrightarrow i|g\rangle_m|g\rangle_n|1\rangle \longrightarrow |e_0\rangle_m|g\rangle_n|0\rangle \\
|e_0\rangle_m|e_0\rangle_n|0\rangle &\longrightarrow -i|g\rangle_m|e_0\rangle_n|1\rangle \longrightarrow -i|g\rangle_m|e_0\rangle_n|1\rangle \longrightarrow -|e_0\rangle_m|e_0\rangle_n|0\rangle
\end{aligned}$$

Der Zustand ändert sein Vorzeichen, falls beide Teilzustände sich im angeregten Zustand befinden. Dies ist äquivalent zum C-NOT-Gatter. Betrachte dazu die Zustände

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left(|g\rangle \pm |e_0\rangle\right)$$

Auf diese wirkt der Operator wie folgt:

$$\begin{aligned}
|g\rangle_m|\pm\rangle_n &\longrightarrow |g\rangle_m|\pm\rangle_n \\
|e_0\rangle_m|\pm\rangle_n &\longrightarrow |e_0\rangle_m|\mp\rangle_n
\end{aligned}$$

Mit einer entsprechenden (ein-bit) Drehung auf das n-te Ion ergibt sich ein C-NOT. Das Problem hierbei ist, daß sich eine unerwünschte Änderung der Phononenzahl einstellt. Um lokale Rotationen ohne Phononenzahländerung zu bewirken, muß $\delta = 0$ (keine Verstimmung) und $q = 0$ erfüllt sein. Der Laser wird so eingestellt, daß sich das Ion in einem Wellenbauch befindet (?). Die Hamilton-Funktion lautet nun:

$$\begin{aligned}
\hat{H}_n &= \frac{\Omega}{2}\left(|e_0\rangle\langle g|e^{-i\phi} + |g\rangle\langle e_0|e^{i\phi}\right) \\
&\Rightarrow \hat{V}_n^k(\phi) = \exp(-i\hbar\hat{H}_n t) = \exp\left(-i\frac{k\pi}{2}\left(|e_0\rangle\langle g|e^{-i\phi} + |g\rangle\langle e_0|e^{i\phi}\right)\right)
\end{aligned}$$

Damit gilt:

$$\begin{aligned}
|g\rangle_n &\longrightarrow \cos(\frac{k\pi}{2})|g\rangle_n - i\sin(\frac{k\pi}{2})e^{i\phi}|e_0\rangle_n \\
|e_0\rangle_n &\longrightarrow \cos(\frac{k\pi}{2})|e_0\rangle_n - i\sin(\frac{k\pi}{2})e^{-i\phi}|g\rangle_n
\end{aligned}$$

Für den Fall $k = \frac{1}{2}$ ergibt sich:

$$\begin{aligned}
\hat{V}_n^{\frac{1}{2}}(\phi = -\frac{\pi}{2})|g\rangle_n = |+\rangle_n \hat{V}_n^{\frac{1}{2}}(\phi = -\frac{\pi}{2})|e\rangle_n = |-\rangle_n \\
\Rightarrow \quad \hat{C}_{m,n} = \hat{V}_n^{\frac{1}{2}}(\phi = -\frac{\pi}{2})\hat{U}_{m,n}\hat{V}_n^{\frac{1}{2}}(\phi = -\frac{\pi}{2})
\end{aligned}$$

Das durch $\hat{C}_{m,n}$ repräsentierte C-NOT ist wichtig, da mit dem C-NOT und $V_n^k(\phi)$ prinzipiell ein beliebiges Gatter gebastelt werden kann. Experimentell ist die Gruppe um D. Wineland z.Zt. sehr „erfolgreich“, sie haben 3 Ionen bis in den Grundzustand gekühlt und bereits 2-bit Gatter realisiert. J. Kimble ist mit einer Gruppe am Caltech dabei, das Verfahren in Cavity-QED umzusetzen (Resonatoren extrem hoher Güte, so daß nur noch einzelne Moden darin auftreten). Das erlaubt auch Rydberg-Atom-ähnliche Zustände zu erzeugen. Aufgrund der hohen Lebensdauern dieser Systeme (keine spontane Emission) sollte das auch in Cavity-QED arbeiten. Auf weitere Ergebnisse darf man gespannt sein.

13 Quantencodier-Theorem

Dieser Abschnitt befaßt sich mit der Möglichkeit, Information möglichst platzsparend zu codieren und sollte daher exakter Quanteninformationskompression heißen.
Die klassische Codier-Theorie wurde von SHANNON begründet und hängt eng mit den Begriff der Entropie zusammen. Zuerst sollen die Grundzüge der klassischen Theorie dargelegt und danach das Quantenanalogon aufgezeigt werden.

13.1 Klassische Informationskompression

Betrachte eine gedächtnislose Quelle, die Worte ($\hat{=}$ Symbole) aus dem Alphabet w_i, $i = 1, \ldots, N$ mit der Wahrscheinlichkeit p_i generiert. Die Entropie beträgt dann

$$S \;=\; -\sum p_i \log(p_i),$$

wobei wie üblich $\log := \log_2$. Ferner bezeichnen wir im folgenden eine Sequenz von Wörtern synonym mit Nachricht und Block. Symbole hingegen sind synonym mit Signal und Wort.

Theorem 11 *Nachrichten können mit einer beliebigen Genauigkeit mit maximal* $\log Sn$ *bits pro Wort codiert werden, wenn n nur hinreichend groß ist, mathematisch: Für* $\varepsilon > 0, \delta > 0$ *und n hinreichend groß, existiert eine Untermenge* $TYP(n) \subset SEQ(n) = Sequenzen(n)$ *der Größe* $\leq 2^{n(S+\delta)} < 2^{n \log N}$, *mit einer Gesamtwahrscheinlichkeit* $\geq 1 - \varepsilon$, *also beliebig nahe an 1.*

Die Mächtigkeit der Menge SEQ(n) ist $|\text{SEQ}(n)| = N^n = 2^{n \log(N)}$
Beweis des Theorems:
Vorbemerkung:
Wir erinnern an die ČEBYČEV-Ungleichung:

$$P(|X - E(X)| > a) \leq \frac{\sigma_X}{a^2}, \quad \text{mit Varianz} \quad \sigma_X = E(X^2 - E(X)^2)$$

Sei $\Sigma = \{w_1, \ldots, w_N\}$ die Menge der Quellensymbole, (die bei der Codierung in Wörtern dargestellt werden), und $\bar{x}_n = \{x_1, \ldots, x_n\}$ die Menge aller Nachrichten bis einschließlich der Länge n. Im folgenden wird statt von Nachrichten oder Sequenzen nur noch von Blöcken gesprochen. Weiter sei $f_i(\bar{x}_n)$ die Häufigkeit des Symbols w_i in $\bar{x}_n$.
Wenn nun $\bar{x}_n$ ein typischer Block ist, d.h. $\bar{x}_n \in \text{TYP}(n)$, gilt (per def.)

$$\left| \frac{f_i(\bar{x}_n) - np_i}{(np_iq_i)^{\frac{1}{2}}} \right| \leq W \quad \text{mit} \quad W \text{ bel.}, \quad 1 < i < N, \quad q_i = 1 - p_i$$

Nennen wir außerdem die Menge der Blöcke, für die obige Gleichung nicht erfüllt ist, die *atypischen* Blöcke: ATYP(n). Es gilt also

$$\mathrm{TYP}(n) \cup \mathrm{ATYP}(n) = \mathrm{SEQ}(n)$$

Beweisbeginn:
Sei $\bar{x}_n \in \mathrm{ATYP}(n)$. Dann gilt für die Wahrscheinlichkeit

$$\begin{aligned} P(\bar{x}_n \in \mathrm{ATYP}(n)) &= P(\bigcup_{i=1}^{N} |\frac{f_i(\bar{x}_n) - np_i}{\sqrt{np_iq_i}}| > W) \\ &\overset{P(A\cup B)\leq P(A)+P(B)}{\leq} \sum_{i=1}^{N} P(|\frac{f_i(\bar{x}_n) - np_i}{\sqrt{np_iq_i}}| > W) \\ &= \sum_{i=1}^{N} P(|f_i(\bar{x}_n) - np_i| > W\sqrt{np_iq_i}) \end{aligned}$$

da $\sqrt{np_iq_i} > 0$. Die Čebyčev-Ungleichung liefert:

$$\leq \sum_{i=1}^{N} \frac{\sigma_{f_i}^2}{(W\sqrt{np_iq_i})^2}$$

Betrachten wir nun die Zufallsgröße $X = f_i(\bar{x}_n)$ genauer: Sie gibt an, wie oft das Symbol w_i in $\bar{x}_n$ auftritt. Da w_i an jeder Stelle unabhängig von den anderen Stellen im Block auftritt, ist die Wahrscheinlichkeitsverteilung $f_i(\bar{x}_n) = k$ für k-faches Auftreten im Nachrichtenblock eine Binomialverteilung, also:

$$P(f_i(\bar{x}_n) = k) = \left(\begin{array}{c} n \\ k \end{array} \right) p_i^k q_i^{n-k}$$

Für den Erwartungswert und die Varianz einer Binomialverteilung gelten:

$$E(f_i(\bar{x}_n)) = np_i \qquad \sigma_{f_i}^2 = np_iq_i$$

Damit ist

$$\sum_{i=1}^{N} \frac{\sigma_{f_i}^2}{(W\sqrt{np_iq_i})^2} = \sum_{i=1}^{N} \frac{np_iq_i}{W^2np_iq_i} = \frac{N}{W^2} =: \varepsilon$$

Damit ist die Wahrscheinlichkeit, daß der Block untypisch ist, beliebig klein wählbar:

$$P(\bar{x}_n \in \mathrm{ATYP}(n)) \leq \varepsilon$$

Damit sind (für hinreichend große n) fast alle Blöcke typische Blöcke. N.B.: Im Allgemeinen muß dafür die Blocklänge n recht groß werden.
Betrachten wir nun einen typischen Block $\bar{x}_n \in \mathrm{TYP}(n)$. Die Häufigkeit ($= f_i(\bar{x}_n)$) des Wortes w_i in diesem typischen Block weicht von dem Mittelwert ($E(f_i(\bar{x}_n)) = np_i$) der Häufigkeit von w_i in allen Blöcken nur noch um einen geringen Betrag ab:

$$np_i - W\sqrt{np_iq_i} \leq f_i(\bar{x}_n) \leq np_i + W\sqrt{np_iq_i} \quad \forall i$$

Die Wahrscheinlichkeit für einen Block, bei dem alle w_i mit ihrer mittleren Häufigkeit auftreten, ist:

$$P = p_1^{np_1} p_2^{np_2} p_3^{np_3} \dots p_N^{np_N}$$

Ein typischer Block hat die Wahrscheinlichkeit

$$P(\bar{x}_n \in \mathrm{TYP}(n)) = p_1^{f_1(\bar{x}_n)} p_2^{f_2(\bar{x}_n)} \dots p_N^{f_N(\bar{x}_n)} = 2^{\sum_i f_i(\bar{x}_n)\log(p_i)}$$

Damit ist $P(\bar{x}_n \in \mathrm{TYP}(n))$ durch die Gleichung oben begrenzt:

$$p(\bar{x}_n) = 2^{-nS-A\sqrt{n}} \leq p(\bar{x}_n \in \mathrm{TYP}(n)) \leq 2^{-nS+A\sqrt{n}}$$
$$A := \sum_i W\sqrt{p_iq_i}\log(p_i), S = \sum_i p_i \log(p_i)$$

(Fast) alle Blöcke sind typisch, und jeder hat die (gleiche) Wahrscheinlichkeit $P(\bar{x}_n \in \mathrm{TYP}(n)) \approx 2^{-nS}$. Daher ist die Anzahl der typischen Blöcke (=Mächtigkeit von $\mathrm{TYP}(n)$) gleich

$$|\mathrm{TYP}(n)| < 2^{n(S+\delta)} < 2^{n\log N}$$

Ein einzelner Block ist damit mit Sn bits codierbar.

13.2 Klassisches Informationskompression-Protokoll

Beachte: die hier vorgestellte Kompressionsart ist eine Codierung mit *fester* Codewortlänge (z.B. arithmetische Codierung), im Gegensatz z.B. zum Huffman-Code von Kapitel 2, bei dem *einzelne* Symbole Nachrichteneinheiten gebildet haben. Hier sind die Blöcke die Einheiten. Die Blöcke haben alle feste Länge (Huffman-Wortlänge für ein Symbol war variabel). Je genauer die Blöcke die Wahrscheinlichkeitsverteilung der Symbole der Quelle widerspiegeln, desto besser ist die Codierung: daher wird diese Codierung gut für große Blocklängen.
Protokoll:

1. A,B stellen eine gemeinsame Liste aller typischen Sequenzen (Blöcke, Nachrichten) auf. Für jede Sequenz benötigen sie dazu $n(S+\delta)$ bits.

2. Für eine gegebene Sequenz $\bar{x}_n$ überprüft A, ob es eine typische Sequenz ist.

   - falls ja: A sendet den Namen von $\bar{x}_n$ an B
   - falls nein: A sendet ein festes $\bar{x}_n^*$ an B. Dieses Protokoll nennt man - warum auch immer - „faithful block coding“

13.3 Quanteninformationskompression

Dieser Abschnitt kann nur eine kurze Skizze der vorgeschlagenen Möglichkeiten sein[44], daher ist das weitere Literaturstudium dringend angeraten, z.B. [39] oder [40].
Wir betrachten nun eine quantenmechanische Quelle. Jedem der Zustände entspricht nun ein Symbol. Da nicht bekannt ist, welches Symbol die Quelle sendet, emittiert sie in der quantenmechanischen Beschreibung Dichtematrizen. Die Dichtematrix für ein gesendetes Signal ist z.B.:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Die Folge der gesendeten Signale läßt sich damit beschreiben als:[45]

$$\rho^{\otimes n} := \rho_1 \otimes \cdots \otimes \rho_n$$

Die Eigenwerte von $\rho^{\otimes n}$ sind die Produkte der Eigenwerte der einzelnen ρ_j, z.B. für dim $\mathcal{H} = N$:

$$\lambda_{\text{tot}} = \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_n} \quad \text{für } i = 1,\ldots,(N-1)$$

Den typischen Sequenzen entspricht nun ein Unterraum von $\mathcal{H}$, nämlich

$$\begin{aligned} \Lambda(n) &\subset \mathcal{H}^{\otimes n} \\ \Lambda(n) &= \text{span}\{|\lambda_{i_1}\ldots\lambda_{i_n}\ldots\rangle\} \text{ so daß } \{\lambda_{i_1},\ldots,\lambda_{i_n}\} \in \text{TYP}(n) \end{aligned}$$

Damit wird

$$S_{\text{SHANNON}} = -\sum_i \lambda_i \log(\lambda_i) = S_{vN}$$

[44] das Skript ist an dieser Stelle noch nicht ausgereift

[45] (Für eine stationäre Quelle sollte $\rho_1 = \rho_n$, oder ? Dann würde auch die VON-NEUMANN-Entropie $S(\rho) = \text{Spur}\,(\rho\log(\rho))$ mit der klassischen übereinstimmen).

Damit folgt für die Dimension des Unterraums:

$$\dim(\Lambda(n)) \quad \leq \quad 2^{n(S(\rho)+\delta)}$$

Wenn wir den Projektor auf $\Lambda(n)$ mit Π bezeichnen, dann folgt (analog zum klassischen):

$$\text{Spur}\left(\rho^{\otimes n}\Pi\right) \quad \geq \quad 1-\varepsilon$$

13.4 Jozsa-Schumacher-Protokoll

Das quantenmechanische Verfahren läuft analog zu klassischen:

1. A häuft eine Menge von Ausgangszuständen an (dies entspricht der zu komprimierenden Sequenz im klassischen Fall):

$$|\psi_{\text{ein}}\rangle = |\psi_{i_1}\rangle \otimes \ldots |\psi_{i_n}\rangle$$

2. A überprüft, ob die Sequenz $|\psi_{\text{ein}}\rangle$ zu $\Lambda(n)$ gehört oder nicht (Projektion)

   - falls ja:
     A sendet $n(S(\rho)+\delta)$ Qubits an B [46]
   - falls nicht:
     A schickt B irgendeinen Zustand $\in \Lambda(n)$

Mit der Wahrscheinlichkeit

$$P \quad = \quad \langle\psi_{\text{ein}}|\Pi|\psi_{\text{ein}}\rangle$$

erhält A ..(?). Der Zustand nach der Messung ist

$$\rho_{\text{aus}} \quad = \quad P\frac{\Pi|\psi_{\text{ein}}\rangle\langle\psi_{\text{ein}}|}{\langle\psi_{\text{ein}}|\Pi|\psi_{\text{ein}}\rangle} + (1-P)|\tilde{\psi}\rangle\langle\tilde{\psi}|$$

Wie ähnlich ist $\langle\psi_{\text{ein}}|\rho_{\text{aus}}|\psi_{\text{ein}}\rangle$ zum Zustand von B?
Wenn wir über alle Zustände mitteln, erhalten wir:

$$\begin{aligned}\langle\psi_{\text{ein}}|\bar{\rho}_{\text{aus}}|\psi_{\text{ein}}\rangle \quad &\geq \quad (\langle\psi_{\text{ein}}|\bar{\rho}_{\text{aus}}|\psi_{\text{ein}}\rangle)^2 \geq (\langle\psi_{\text{ein}}|\bar{\rho}_{\text{aus}}|\psi_{\text{ein}}\rangle)^2 \\ &= \quad (\text{Spur}\left(\rho^{\otimes n}\Pi\right))^2 \geq (1-\varepsilon)^2\end{aligned}$$

Kapitel zuende ?

[46] Begründung?

14 Quantenklonen und Zustandsabschätzung

14.1 Quantenklonen

Die Grundlage des Quantenklonens ist das in [41] vorgestellte

Theorem 12 *No-Cloning*
Ein unbekannter Quantenzustand $|\psi\rangle$ kann nicht perfekt geklont werden, d.h. $\nexists$ *unitäre Operation U, für die gilt*

$$U|\psi\rangle|i\rangle = |\psi\rangle|\psi\rangle$$

Hierbei ist $|i\rangle$ ein bekannter Anfangszustand (Initialzustand).

Beweis:
Angenommen, es existiere eine unitäre Operation U die klonte, d.h.

$$U|0\rangle|i\rangle = |0\rangle|0\rangle \qquad \text{und} \qquad U|1\rangle|i\rangle = |1\rangle|1\rangle$$

Wird U nun auf den allgemeinen Zustand $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ angewendet, ergibt sich

$$U|\psi\rangle|i\rangle \;\; = \;\; \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq |\psi\rangle|\psi\rangle$$

Eine solche Operation würde zudem die Unitarität verletzen, d.h. das Skalarprodukt zweier Vektoren wäre nicht erhalten. Wird die Behauptung (s. obiges Theorem) mit z.B. der Gleichung für $\langle 1|\langle i|U^\dagger$ multipliziert, ergibt sich

$$\begin{aligned} \langle 1|\langle i|U^\dagger U|\psi\rangle|i\rangle &= \beta 1 = \beta \\ &\neq \langle 1|\psi\rangle\langle 1|\psi\rangle = \beta^2 \end{aligned}$$

Dies ist ein wichtiges Ergebnis, da klassisch kopieren möglich ist. Auf der einen Seite ist die Unmöglichkeit, Quantenzustände zu kopieren, sehr vorteilhaft, z.B. bei der Quantenkryptographie (s.Abschnitt 6), andererseits basiert Fehlerkorrektur oft auf Redundanz; solche Verfahren erzwingen im Quantenfall kompliziertere Schemata (s.Abschnitt 10).
Daher ist nur approximatives Quantenklonen möglich. Das erste Beispiel aus [42] beschreibt einen isotropen 1→2-Kloner:

$$U|0\rangle|i\rangle|a\rangle = \sqrt{\frac{2}{3}}|00\rangle|0\rangle_a + \sqrt{\frac{1}{6}}(|01\rangle + |10\rangle)|1\rangle_a$$
$$U|1\rangle|i\rangle|a\rangle = \sqrt{\frac{2}{3}}|11\rangle|1\rangle_a + \sqrt{\frac{1}{6}}(|01\rangle + |10\rangle)|0\rangle_a$$

Hierbei ist $|a\rangle$ ein weiterer, beliebiger Freiheitsgrad des Systems[47]. Um zu beschreiben, wie gut der Kloner einen beliebigen Zustand $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kopiert, wird wieder die Fidelity

$$F = \langle\psi|\rho^{\text{out}}|\psi\rangle = \text{Spur}\left(\rho^{\text{in}}\rho^{\text{out}}\right) \qquad \text{mit } \rho^{\text{out}} = \text{Spur}\left(\rho^{\text{total}}\right)_{2,a}$$

betrachtet. Ausgeschrieben lauten die Dichtematrizen

$$\begin{aligned}
\rho^{\text{in}} &= |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \\
\rho^{\text{out}} &= {}_{2,a}\langle 00|\rho^{\text{total}}|00\rangle_{2,a} + {}_{2,a}\langle 01|\rho^{\text{total}}|01\rangle_{2,a} \\
&\quad + {}_{2,a}\langle 10|\rho^{\text{total}}|10\rangle_{2,a} + {}_{2,a}\langle 11|\rho^{\text{total}}|11\rangle_{2,a} \\
&= \begin{pmatrix} \frac{5}{6}|\alpha|^2 + \frac{1}{6}|\beta|^2 & \frac{2}{3}\alpha\beta^* \\ \frac{2}{3}\alpha^*\beta & \frac{5}{6}|\beta|^2 + \frac{1}{6}|\alpha|^2 \end{pmatrix}
\end{aligned}$$

betrachtet. Die Fidelity beträgt hier

$$F = |\alpha|^2\left(\frac{5}{6}|\alpha|^2 + \frac{1}{6}|\beta|^2\right) + \frac{4}{3}|\alpha|^2|\beta|^2 + |\beta|^2\left(\frac{5}{6}|\beta|^2 + \frac{1}{6}|\alpha|^2\right) = \frac{5}{6} = \text{const}$$

Hier wird offensichtlich, daß die Qualität der Klonung unabhängig von $|\psi\rangle$ ist.
Eine andere Beschreibung sind die in Abschnitt 3.3 eingeführten BLOCHvektoren. Hierbei werden die spurlosen PAULImatrizen, die z.B.

$$\sigma_k\sigma_l = i\epsilon_{klm}\sigma_m \text{ und } \text{Spur}\left(\sigma_i\sigma_j\right) = 2\delta_{ij}$$

erfüllen, als Basis verwendet. Damit ist

$$\rho = S_0\mathbb{1} + S^i\sigma_i$$

Da $\text{Spur}\left(\rho\right) = 1$ und $\text{Spur}\left(\mathbb{1}\right) = 2$ ist, muß also $S_0 = \frac{1}{2}$ betragen. Damit ist

$$\rho = \frac{1}{2}\left(\mathbb{1} + \vec{S}\cdot\vec{\sigma}\right)$$

Der Vektor $\vec{S}$ wird BLOCHvektor genannt. Seine Länge ergibt sich aus der Bedingung, daß für reine Zustände $\text{Spur}\left(\rho\right) = \text{Spur}\left(\rho^2\right) = 1$ sein muß. Durch einsetzen und ausquadrieren ergibt sich sofort, daß der BLOCHvektor die Länge (Norm) 1 besitzt, d.h. reine Zustände liegen auf der Oberfläche der BLOCHkugel.

[47]Der Zustand/die Quantenzahl wird mit „a“ bezeichnet, da in der Literatur dieser Hilfszustand oft als Ancilla bezeichnet wird

Um den BLOCHvektor aus einer gegebenen Dichtematrix zu bestimmen, ist es sinnvoll, die Definition auszunutzen:

$$\rho = \frac{1}{2}\left(\mathbb{1} + \vec{S}\cdot\vec{\sigma}\right) \quad = \quad \frac{1}{2}\begin{pmatrix} 1+S_z & S_x - iS_y \\ Sx + iS_y & 1-S_z \end{pmatrix}$$

Diese Gleichungen lassen sich nach den Komponenten von $\vec{S}$ auflösen:

$$S_x = 2\Re(\rho_{01}) \qquad S_y = -2\Im(\rho_{01}) \qquad S_z = \rho_{00} - \rho_{11}$$

In unserem Beispiel ist

$$\begin{aligned} S_x^{\text{in}} &= 2\Re(\alpha\beta^*) & S_x^{\text{out}} &= \frac{2}{3}\cdot 2\Re(\alpha\beta^*) \\ S_y^{\text{in}} &= -2\Im(\alpha\beta^*) & S_x^{\text{out}} &= -\frac{2}{3}\cdot 2\Im(\alpha\beta^*) \\ S_z^{\text{in}} &= |\alpha|^2 - |\beta|^2 & S_z^{\text{out}} &= \frac{2}{3}\left(|\alpha|^2 - |\beta|^2\right) \end{aligned}$$

d.h. $\vec{S}^{\text{out}} = \frac{2}{3}\vec{S}^{\text{in}}$ oder anders formuliert, die BLOCHkugel ist geschrumpft. Dies bedeutet nichts anderes, als daß aus dem reinen Ursprungszustand ein gemischter, verschränkter Zustand eines Teilsystems geworden ist; der Gesamtzustand ist damit verschränkt.
Nach dieser Vorbetrachtung stellt sich die Frage nach dem „besten“ universellen Quantenkloner. Universell bedeutet hier, daß jeder Zustand gleich gut geklont wird. Als erstes haben dies [43] für den 1→2-Kloner untersucht. Die Bedingungen an diesen Kloner bedeuten formal

$$\begin{aligned} \rho_1 &= \rho_2 && \text{Ausgangszustände identisch} \\ \forall|\psi\rangle\ F = \text{const} &\Leftrightarrow \vec{S}_1 = \eta\vec{S}_\psi && \text{Universalität} \end{aligned}$$

Beweis für die Äquivalenz der letzten Zeile:
⇐

$$F \quad = \quad \frac{1}{4}\text{Spur}\left(\left(\mathbb{1} + \vec{S}_\psi\cdot\vec{\sigma}\right)\left(\mathbb{1} + \eta\vec{S}_\psi\cdot\vec{\sigma}\right)\right) = \frac{1}{4}\left(2 + 2\eta|\vec{S}_\psi|^2\right) = \frac{1}{2}(1+\eta)$$

⇒
Da die Fidelity unabhängig vom Zustand sein soll, kann es sich nicht um eine reine Drehung auf der BLOCHkugel handeln, da dort zwei Fixpunkte existieren[48]. Diese Tatsache ist auch unter Begriffen wie „haariger Ball“ und

[48] Jede Transformation der BLOCHkugel läßt sich in eine Drehung und eine Streckung (Schrumpfung) zerlegen

„Igel können nicht gekämmt werden“ bekannt. Somit muß der Vektor geschrumpft sein. Da kein Punkt auf der Kugel ausgezeichnet sein soll, muß diese „Schrumpfung“ unabhängig vom Zustand sein. □
Um den optimalen Klonoperator zu finden, wird eine allgemeine unitäre Operation angesetzt:

$$\begin{aligned} U|0\rangle|i\rangle|a\rangle &= a|00\rangle|A\rangle + b_1|01\rangle|B_1\rangle + b_2|10\rangle|B_2\rangle + c|11\rangle|C\rangle \\ U|1\rangle|i\rangle|a\rangle &= \tilde{a}|11\rangle|\tilde{A}\rangle + \tilde{b}_1|10\rangle|\tilde{B}_1\rangle + b_2|01\rangle|\tilde{B}_2\rangle + \tilde{c}|00\rangle|\tilde{C}\rangle \end{aligned}$$

Jetzt werden eine Reihe von Zwangsbedingungen ausgenützt, um die Parameter zu bestimmen:

Unitärität d.h. Erhalt des Skalarprodukts, z.B. $|a|^2 + |b_1|^2 + |b_2|^2 + |c|^2 = 1$

Symmetrie der reduzierten Dichtematrizen, liefert z.B. $|b_1| = |b_2|$

Isotropie liefert Bedingungsgleichungen für η, die unter den Nebenbedingungen zu maximieren sind (mittels LAGRANGE-Multiplikatoren)

Die Rechnung liefert schließlich, daß $c = \tilde{c} = 0$ ist. Ferner zeigt die Rechnung, daß der zusätzliche Freiheitsgrad nötig ist, aber ein qubit dafür ausreicht. Die maximale Fidelity liegt bei $\frac{5}{6}$, dies entspricht $\eta^{\max} = \frac{2}{3}$. Das Beispiel war bereits ein optimaler Kloner. Möglich sind noch Rotationen im Ancilla-Raum und Phasen.
Die Möglichkeit der Verallgemeinerung auf N (identische) Eingänge und M Ausgänge ($M > N$) wurde von [44] untersucht. Der optimale Operator wurde „geraten“ und numerisch bis $N = 7$ explizit auf seine Extremaleigenschaft hin untersucht.

$$U_{N,M}|N \cdot \psi\rangle|\chi\rangle = \sum_{j=0}^{M-1} \alpha_j S\{|(M-j)\psi, j\psi^{\perp}\rangle\} \otimes |A_j(\psi)\rangle$$

Hierbei sind

$$\begin{aligned} S\{|2\cdot 0, 1\cdot 1\rangle\} &= \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right) \\ |A_j(\psi)\rangle &= S\{|(M-1-j)\psi^*, j(\psi^*)^{\perp}\rangle\} \\ \alpha_j &= \sqrt{\frac{N+1}{M+1}}\sqrt{\frac{(N\cdot M)!(M-j)!}{(M-N-j)!M!}} \end{aligned}$$

Damit erhalten die Autoren den Skalierfaktor

$$\eta_{N,M} = \frac{N}{N+2} \cdot \frac{M+2}{M}$$

Wird mehrfach hintereinander kopiert, entspricht dies der Multiplikation der Skalierfaktoren. Natürlich wird bei jeder Kopie ein verschränkter Zustand erzeugt, dieser ist aber symmetrisch und linear in seinen Basiselementen

$$\rho_{\text{sym}} = \sum \gamma_i |\psi_i\rangle\langle\psi_i|^{\otimes M}$$

und daher ist diese Betrachtung möglich (*dies ist keine triviale Aussage*). Damit ist

$$\eta_{N,M} \cdot \eta_{M,L} = \frac{N}{N+2} \cdot \frac{M+2}{M} \frac{M}{M+2} \cdot \frac{L+2}{L} = \eta_{N,L}$$

Zwei Randbemerkungen sind hier noch angebracht:

1. Die gesamte Betrachtung untersuchte ausschließlich *reine* Eingangszustände. Quantenklonen von gemischten Zuständen ist Thema aktueller Forschung.

2. Ist (entgegen den Voraussetzungen) $M < N$ und sind die Eingangszustände gemischt, dann betrachten wir die Purifikation und „Dehnen“ den BLOCHvektor aus, d.h. mit $\eta > 0$ liegt der neue Zustand näher an einem reinen als der ursprüngliche.

14.2 Zustandsabschätzung

Ein Satz von M identischen reinen Zuständen wird gemessen. Gesucht ist hierbei ein Satz von Operatoren P_μ derart, daß der Zustand $|\psi_\mu\rangle$, der mit der Wahrscheinlichkeit

$$p_\mu(\psi) = \text{Spur}\left(P_\mu |\psi\rangle\langle\psi|^{\otimes M}\right)$$

auftritt, eine im Durchschnitt maximale Fidelity

$$\begin{aligned} \bar{F}_{\text{mess}} &= \sum_\mu p_\mu |\langle\psi|\psi_\mu\rangle|^2 =: \langle\psi|\bar{\rho}|\psi\rangle \qquad \text{mit} \\ \bar{\rho} &= \sum_\mu p_\mu |\psi_\mu\rangle\langle\psi_\mu| = \frac{1}{2}\left(\mathbb{1} + \eta_{\text{mess}} \vec{S}^{\text{in}} \vec{\sigma}\right) \end{aligned}$$

besitzt. Auch hier wird wieder Universalität verlangt.
Die beste Vorschrift ([45]) liefert

$$\bar{F}^{\max}_{\text{mess}}(M) = \frac{M+1}{M+2} \;\rightsquigarrow\; \bar{\eta}^{\max}_{\text{mess}}(M) = \frac{M}{M+2},$$

d.h. eine kollektive Messung ist besser als eine einzelne Messung. Da die Operatoren P_μ bekannt sind ist $\bar{\rho}$ konstruierbar.

Zusammenhang mit Klonen

1. $\eta_{\text{mess}} \leq \eta_{\text{clone}}^{\text{opt}}(M, L)$ da ansonten das Klonen durch Zustandsmessung und Neuerzeugung effektiver wäre als das direkte Klonen (Widerspruch).

2. Werden zuerst M identische Quantenzustände auf L Zustände geklont und diese danach gemessen, multiplizieren sich die Skalierfaktoren ebenfalls.

Da die optimale Messung nicht verbessert werden kann, muß gelten

$$\begin{aligned} \eta_{\text{clone}}(M, L) \cdot \eta_{\text{mess}}(L) &\leq \eta_{\text{mess}}^{\text{opt}}(M) \qquad \text{bzw.} \\ \eta_{\text{clone}}(M, \infty) \cdot 1 &\leq \eta_{\text{mess}}^{\text{opt}}(M) \qquad \text{für } L \to \infty \end{aligned}$$

Da die Ungleichung für $L \to \infty$ in beiden Richtungen gilt, ergibt sich damit

$$\eta_{\text{clone}}^{\text{opt}}(M, \infty) = \eta_{\text{mess}}^{\text{opt}}(M)$$

A Das direkte Produkt

Ergänzend zu Kapitel 4.2 soll hier kurz das direkte Produkt zweier Vektoren aus dem $\mathcal{H}_2$ angegeben werden. Hierbei wird der allgemeinste Fall betrachtet:

$$|0\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$$

mit $a, b, c, d \in \mathbb{C}$ und $\langle 0|1\rangle \neq 1$, d.h. die Vektoren schließen einen von Null verschieden Winkel ein. Wie in der Quantenmechanik üblich, sollen die Vektoren zudem auf 1 normiert sein. Damit ist

$$\begin{aligned} |0\rangle \otimes |1\rangle &= \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} \\ &= \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} =: |\psi\rangle. \end{aligned}$$

Wird dieser Zustand als Dichtematrix geschrieben, ergibt sich

$$\begin{aligned} |\psi\rangle\langle\psi| &= \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \left((ac)^* \, (ad)^* \, (bc)^* \, (bd)^*\right) \\ &= \begin{pmatrix} |a|^2|c|^2 & |a|^2cd^* & ab^*|c|^2 & ab^*cd^* \\ |a|^2c^*d & |a|^2|d|^2 & ab^*c^*d & ab^*|d|^2 \\ a^*b|c|^2 & a^*bcd^* & |b|^2|c|^2 & |b|^2cd^* \\ a^*bc^*d & a^*b|d|^2 & |b|^2c^*d & |b|^2|d|^2 \end{pmatrix} =: \rho \end{aligned}$$

Bei der Spurbildung z.B. über den Unterraum B werden jetzt für das Element ρ_A^{ij} alle Elemente, die in ρ_A an der Position (i, j) stehen *und* die Diagonalelemente aus dem Unterraum B enthalten (d.h. entweder $|c|^2$ oder $|d|^2$), aufsummiert. Damit ist

$$\begin{aligned} \rho_A &= \text{Spur}\,(\rho)_B = (|c|^2 + |d|^2) \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} \\ \rho_B &= \text{Spur}\,(\rho)_A = (|a|^2 + |b|^2) \begin{pmatrix} |c|^2 & cd^* \\ c^*d & |d|^2 \end{pmatrix} \end{aligned}$$

Entsprechend wird bei höherdimensionalen zusammengesetzten Systemen verfahren; jedoch ist hierbei eine Indexschreibweise sinnvoller als die „Berechnung“ der $2n \times 2n$-Matrix.

B RSA-Codierung

Die RSA-Kodierung[49] ist die wahrscheinlich populärste Public-Key-Verschlüsselungsmethode, neben Banken wird sie auch vielfach im privaten Mailverkehr als PGP/GPG eingesetzt. Details dazu in Kapitel 6.4. Ein weiteres Verfahren, auf das hier nicht eingegangen werden soll, ist das „Rucksackverfahren“ von MERKLE und HELLMAN[50], das ebenfalls 1978 vorgestellt wurde.

B.1 Prinzip

Im folgenden soll kurz das allgemeine Prinzip von Public-Key-Systemen, dann konkret das Vorgehen bei der RSA-Verschlüsselung erläutert werden. Ein Beispiel folgt in B.2 während dann in B.3 auf die mathematischen Hintergründe von RSA eingegangen wird.
Bei den folgenden Betrachtungen habe ich mich an Kapitel 11 aus [1] sowie den lesenswerten Artikel [46] orientiert. Dort werden auch weitere Quellen zitiert. Das Beispiel habe ich selbst durchgerechnet (mit übernommenen Schlüsseln).

Allgemeines Prinzip

Jeder Teilnehmer A_i am System verfügt über ein Schlüsselpaar (k_i, l_i). Daneben ist allen Teilnehmern der Codier-Algorithmus C sowie der Decodieralgorithmus D bekannt. Diese Algorithmen erfüllen für jedes Schlüsselpaar (k_i, l_i) und jede Nachricht m die Bedingung

$$m \;=\; D(C(m, k_i), l_i)$$

Der Schlüssel k_i wird nun allen anderen Teilnehmern bekanntgegeben (er wird daher *öffentlicher Schlüssel* genannt), während der Schlüssel l_i geheim bleibt.
Will B_j nun eine verschlüsselte Nachricht an A_i senden, läuft folgendes ab:

1. B_j ermittelt den öffentlichen Schlüssel k_i von A_i.
2. B_j berechnet das Kryptogramm $c = C(m, k_i)$.
3. Das Kryptogramm c wird über öffentliche Kanäle an A_i übertragen.

[49] RIVEST, SHAMIR und ADELMAN realisierten 1978 die Public Key Verschlüsselung mithilfe des nach Ihnen benannten RSA-Algorithmus, nachdem die prinzipielle Idee 1976 von DIFFIE und HELLMAN vorgestellt worden war.
[50] Mathematiker reden hier vom „Super-increasing Subset-Sum“-Problem

4. A_i gewinnt mittels $m = D(c, l_i)$ die Nachricht zurück.

Damit ein solches Verfahren sicher und in großem Maßstab praktisch ist, müssen folgende Voraussetzungen erfüllt werden:

1. Es muß leicht sein, zufällige Paare (k_i, l_i) zu generieren.
2. Das Kryptogramm $c = C(m, k_i)$ muß leicht berechenbar sein.
3. *Ohne* l_i muß das decodieren von c sehr aufwendig sein.
4. *Mit* l_i muß $m = D(c, l_i)$ leicht berechenbar sein[51].

Konkret: RSA

A generiert zwei große Primzahlen p und q. Im folgenden ist

$$n = p * q.$$

Als nächstes berechnet A

$$z = (p-1) * (q-1)$$

und wählt zwei natürliche Zahlen e und d, die der Bedingung

$$d * e = 1 \mod z$$

genügen, aus. Wenn d (bzw. e) relativ Prim[52] zu z ist, d.h. d und z haben keine gemeinsamen Primfaktoren, dann liegt e fest.
Die Zahlen p und q werden im folgenden nicht mehr benötigt und von A sicherheitshalber vernichtet. A hat jetzt zwei Schlüssel:

öffentlicher Schlüssel (e, n)**:** Dieser Schlüssel wird möglichst weit verbreitet, insbesondere erhält B eine Kopie hiervon[53].

privater Schlüssel d**:** A sichert den Schlüssel, da er unbedingt geheim, d.h. nur ihm bekannt sein darf.

[51] Daher werden solche Verfahren gelegentlich auch als Hintertür-Verfahren (engl. Trapdoor) bezeichnet

[52] wird auch als Coprim bezeichnet

[53] Dieser Schritt ist nicht unproblematisch, da die Übergabe sicher erfolgen muß. Bei PGP ist dies über ein „Web of Trust“ realisiert, d.h. ich vertraue jemandem der jemandem vertraut, der usw. Eine Alternative sind Keyserver, d.h. Institutionen, die auf sicherem Wege (z.B. durch persönlichen Kontakt) Schlüssel sammeln und sie anderen nur im Lesezugriff zugänglich machen.

Damit sind die Vorbereitungen von A abgeschlossen.
Möchte B eine codierte Nachricht an A senden, dann bildet B die Nachricht auf eine Ziffernfolge ab, zerlegt diese Folge in Blöcke der Größe k (ggf. füllt er den letzten Block mit Nullen auf) und berechnet für jeden Block (hier mit x bezeichnet):

$$C(x) \quad = \quad x^e \mod n$$

Die so codierte Nachricht sendet B an A. Um die Nachricht zu decodieren, berechnet A für jeden Ziffernblock $y = C(x)$

$$D(y) \quad = \quad y^d \mod n \qquad \text{mit } D(y) \equiv x$$

Ein potentieller Lauscher (E) müßte zuerst n faktorisieren, um d zu ermitteln.

B.2 Beispiel

Erzeugung des Schlüssels

A wählt $p = 47$ und $q = 71$ und damit $n = 3337$ und $z = 3220$. Als nächstes wählt A $d = 1019$ aus und prüft, ob d und z teilerfremd (coprim) sind. Da dies der Fall ist, berechnet A die eindeutige (!) Zahl c, die $c * d = 1 \mod z$, d.h. $c * 1019 = 1 \mod 3220$, erfüllt. Dies wird von $c = 79$ geleistet. Damit ist

- der öffentliche Schlüssel $(c, n) = (79, 3337)$,
- der private Schlüssel $d = 1019$.

Erzeugung und Übertragung der Nachricht

B möchte nun A die Nachricht

STRENG GEHEIM?

übermitteln. Dazu codiert B diese Nachricht numerisch (unter Verwendung der Übersetzungstabelle aus 6.3) und gruppiert diese dann in vierziffern-Folge:

S	T	R	E	N	G		G	E	H	E	I	M	?
19	20	18	05	14	07	27	07	05	08	05	09	13	28

Nun wendet B auf jeden Block x die Codierfunktion $C(x) = x^c \mod n = x^{79} \mod 3337$ an:

x	1920	1805	1407	2707	508	509	1328
$C(x)$	3211	2675	1910	1179	416	1470	384

Das Cryptogramm

$$32112675191011790416147003 84$$

wird nun über einen öffentlichen Kanal an A übertragen, der es wieder in vierziffer-Blöcke y zerlegt und $D(y) = y^d \mod n = y^{1019} \mod 3337$ berechnet:

y	3211	2675	1910	1179	0416	1470	0384
$C(x)$	1920	1805	1407	2707	0508	0509	1328

Schließlich kann A nun die Ziffernfolge wieder in Text zurückübersetzen und weiß daher, daß diese Nachricht *streng geheim* war.

B.3 Mathematische Betrachtung

Generation der großen Primzahlen p und q

Oft wird die Anzahl der binären Stellen k von $n = p * q$ vorgegeben, z.B. $k = 1024$. Da es kein mathematisches Verfahren zum Erzeugen von großen Primzahlen gibt, werden im allgemeinen zwei große Zahlen mit gewünschtem k gewählt und mit Hilfe eines geeigneten Verfahrens auf Primzahleigenschaft geprüft. Häufig verwendet wird das Verfahren von Miller-Rabin und das Verfahren von Solovay-Strassen. Bei beiden Verfahren wird mit einer *gewissen Wahrscheinlichkeit* ermittelt, ob p bzw. q eine Primzahl ist. Dies erhöht die Geschwindigkeit der Prüfroutine erheblich.

Beweis von $x = D(C(x))$

Lemma 3 $\forall\ p, q\ p \neq q$ *und* p, q *Primzahlen sowie* $\forall\ x, u \in \mathbb{N}_{>0}$ *gilt:*

$$x^u = x \mod p \wedge x^u = x \mod q \Rightarrow x^u = x \mod (p * q)$$

Beweis:

Lemma 4 $x, p \in \mathbb{N}$, $x > 0$, $p > 1$ *dann gilt:*

$$x^{p-1} = 1 \mod p$$

Beweis:

Lemma 5 *Für jedes Schlüsselpaar* $(d, (e, n))$ *des RSA-Systems und für jede Nachricht* m *gilt*

$$m = ((m^e) \mod n)^d \mod n$$

Beweis:
Folgt noch

Muß E wirklich n Faktorisieren ?

Wenn E die Zahl n faktorisiert hat, kann sie $z = (p-1) * (q-1)$ und damit d leicht ermitteln (e und n sind ja bekannt).

C Revisionen

In dieser Sektion sind die Änderungen der einzelnen Versionen dieser Mitschrift festgehalten. Diese Sektion wird im endgültigen Dokument entfernt.

0.01 Erste Version, enthält Kapitel 1,2 und 3; Noch einige Unklarheiten/Fehlerkorrekturen notwendig; Beweis von McMillan fehlt, Beispiel Huffmann-Codierung fehlt; Beweis der Entropie fehlt (wird aber u.U. bis auf weiteres nicht gesetzt), Kapitel 3 ist noch nicht gegengelesen, Literaturliste ist unvollständig und ihr Layout wird wahrscheinlich noch überarbeitet. Der Satz von $\mathbb{C}$,$\mathbb{R}$,$\mathbb{Z}$,$\mathbb{N}$, $\mathbb{1}$ ist wg. fehlender Fonts momentan defekt (wird behoben).

0.02 Vorübergehender Fix der Fonts wg. $\mathbb{C}$,$\mathbb{N}$,$\mathbb{R}$,$\mathbb{Z}$ und $\mathbb{1}$

0.03 Jetzt richtiger Font für $\mathbb{C}$,$\mathbb{N}$,$\mathbb{R}$,$\mathbb{Z}$ und $\mathbb{1}$

0.04 Kapitel 1, 2 und 3 Teil 1 fast fertig; einige Formulierungen müssen noch überarbeitet werden; ein Bild liegt mir noch nicht vor (Ende Kapitel 2). Bitte um Feedback; insbesondere wg. der Ergänzungen gegenüber der Vorlesung. Literaturverzeichnis (leider) immer noch im Aufbau. Leerseite am Anfang ergänzt, damit Inhaltsverzeichnis zweiseitig werden kann. Subsection Plan ergänzt. Kleine Typos behoben. Beweis McMillan ergänzt (ok ?). Huffmann-Codierung ergänzt inkl. Beispiel. Hier ggf. noch Überarbeitung der Formulierung. Text bei Information (Ende Kapitel 1) überarbeitet.

0.1 Anfang nochmals leicht überarbeitet (Plan ist jetzt hinten). Sorry. Am Anfang sollte sich jetzt nicht mehr viel tun. Huffmann gegengelesen und leicht ergänzt. Beweis McMillan ok ? (→ Feedback ?). Kapitel 3 ist ist zu ca. $\frac{2}{3}$ dabei. Der Rest wird (inkl. Kapitel 4) bereits gegengelesen. Kleine Typos behoben. Literaturverzeichnis bereits aktualisiert aber noch im Aufbau. Kapitel 1 und 2 (bis auf ggf. Beweis McMillan) sollten jetzt in ihrer vorläufig endgültigen Fassung vorliegen. Diese Seite leicht bearbeitete :-)

0.11 Zwischenrelease. Anführungszeichen im ganzen Text gefixt. Namenssatz (Pauli statt Pauli) gefixt. Teil 3 (fast) fertig (ist jetzt dabei). Die Kapitelnummerierung könnte sich noch ändern. Im Satz könnten sich noch Kleinigkeiten ändern. Anfang von Kapitel 4 beigefügt (Rest ist fertig, folgt in Kürze). In Kapitel 3 sind noch Fragen offen ! (→ Feedback ?)

0.12 Kapitel 4 jetzt komplett. Keine Vollversion, da noch immer Kleinigkeiten in Kapitel 3 offen sind. Viele kleine Fixes (wieder) (in Kapitel 3). Ich hoffe, die Nummerierung in Kapitel 3 bleibt jetzt. *Feedback* wie immer sehr willkommen.

0.2 Korrektur von Fehlern in Abschnitt 3.7, dennoch könnten dort noch Fehler sein. Kapitel 5 und 6 eingefügt (wir sind somit fast wieder up to date). Da in der heutigen (4.Dezember) Vorlesung noch Teile für Kapitel 6 hinzukommen, können sich die Seitenzahlen dort noch ändern. Es zeichnet sich ab, daß wir zudem mehr Seiten für das Inhaltsverzeichnis benötigen.

0.21 Kleine Typos behoben; kleine Korrektur in Section 3.6.1.

0.22 Wieder viele kleine Typos behoben (in jedem Kapitel noch welche gefunden). Ich hoffe, daß bis auf die bekannten Schwachstellen alles bis vor Seite 49 jetzt ok ist. Neu hinzugekommen ist nur Section 6.7. Im Aufbau ist z.Z. (neben den aktuellen Kapiteln) Anhang B, ich werde dort nach und nach die PGP-Erläuterung einfügen.

0.23 Jetzt bis 7.3 bzw. 8.2 Anfang der Subsectionen geTEXt. Kleine Fehler behoben, auch Seite 49 sollte jetzt ok sein. Fehler entdeckt ? → Feedback !

0.24 Kapitel 7 bis 10 komplett. Satz weiter überarbeitet (Overfull/Underfull boxes etc.). Interne Verbesserungen, z.B. Entfernung von nicht-LATEX 2ϵ-Befehlen (lies: aus `{\sc` wird `\textsc{`). In Section 7.4 und 8.3 noch ggf. Fehler/Unsicherheiten. Ferner etwas unter Zeitdruck, daher könnten die letzten Absätze noch Flüchtigkeitsfehler enthalten. Zwei weitere Leerseiten am Anfang ergänzt (Sorry, aber das Inhaltsverzeichnis wächst unerbittlich) und (ebenfalls Sorry) leider die Zitate etwas verschoben, die Nummerierung sollte jetzt bleiben. Kleinere Ergänzungen auch auf dieser Seite.

0.3 (Weihnachtsausgabe) Nur Section 7.4 bearbeitet.

0.4 Viele Satzüberarbeitungen. Korrektur in Theorem 6, Section 3.7, 7.3, 8.3, 4.2 und B überarbeitet, Section A ergänzt. Bitte um *Feedback*, insbesondere bei den mit Fußnoten angemerkten Stellen.

0.41 Section 6.7, 10 ergänzt (!) sowie 11 angefangen.

0.42 Kleinere Korrekturen (Rechtschreibung etc.) in 7, 8, 9, 10 und B; an 11 weitergeschrieben. Versionsnummer stimmt wieder :)

0.43 Section 12 ergänzt (Reine Mitschrift).

0.44 Rest (d.h. 11, 13 und 14) gesetzt. Kleine Korrekturen in 12. Achtung: Auch in dieser Version wurde relativ wenig ergänzt/gerechnet, bitte *Feedback*. Index ergänzt.

0.9 Titelseite leicht überarbeitet, Vorwort ergänzt. In Kapitel 4 eine Namenskorrektur (Greenberger). Rechtschreibkorrektur in 5.4. Korrektur der CHSH-Ungleichung in Kapitel 5.5. In Kapitel 6 viele kleine Rechtschreibkorrekturen, die Kryptographie heißt korrekt Einmalschlüssel-Kryptographie (6.3), die Namensgeber der Protokolle wurden ergänzt. Auch in 8.2 die CHSH-Ungleichung korrigiert und leicht die Erklärung ergänzt. Kleiner Typo sowie Satz am Ende von 9.2 korrigiert. Ein Rechtschreibfehler in Kapitel 11 gefunden und behoben. Satzkorrekturen in Abschnitt 13.3. Die Namen in der Überschrift von 13.4 korrigiert. Das Kapitel 14 hat viele kleine Änderungen und Ergänzungen erfahren. Die Zitate sind alle geprüft und korrigiert. Der Abschnit „Plan“ ist entfernt worden. Eine Bitte an alle Leser: die Version 1.0 wird wohl in Bälde erscheinen, daher bitten wir um Feedback - auch die Korrektur von so „kleinen“ Dingen wie Rechtschreibung und Satzbau verbessert dieses Dokument.

0.91 Im wesentlichen wurden die Kapitel 1 und 2 um Erläuterungen ergänzt und einige Formulierungen klarer gefaßt. Da wir hier noch Diskussionsbedarf sehen, bitten wir um *Feedback*; Hinweise, Ergänzungen usw. werden gerne angenommen. Darüberhinaus viele kleine Satzverbesserungen.

0.92 Viele kleine Korrekturen und Satzüberarbeitungen.

Literatur

[1] D. Welsh: *Codes and Cryptography*, Clarendon Press [1988]

[2] C.E.Shannon and W.Weaver: *The Mathematical Theory of Communication* [1949]

[3] R.Ash: *Information Theory*, Dover Publications [1990]

[4] A. Peres: *Quantum Theory: Concepts and Methods*, Dordrecht [1993]

[5] J.A. Wheeler and W. Zurek (eds.): *Quantum Theory and Measurement*, Prnceton University Press [1983]

[6] R. Feynmann: *Feynmann's Lectures on Computing*, articles in Scientific American

[7] A. Peres: *Separability criterion for density matrices* PRL **77**, p. 1413 [1996]

[8] R. + M. Horodecki: *Information-theoretic aspects of inseparability of mixed states*, PRA **54**, p. 1838 [1996]

[9] z.B. Vorlesungsskript Statistische Methoden der Nachrichtentechnik, Uni Hannover, SS 98

[10] W. Wootters: *Entanglement of formation of inseparability*, `quant-ph/9709029`

[11] E.A. Poe, *The gold-bug*

[12] Alexander Foote: *Handbuch für Spione*, C.W.Leske Verlag, Darmstadt 1954

[13] D. Bruß, N.Lütkenhaus: *Quantum Key Distribution: from Principles To Practicalities*, `quant-ph/9901061`

[14] C Bennett, G. Brassard: *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proceedings of the IEEE International Conference on Computer Systems and Signal Processing, Bangalore, India, 1984. (IEEE, New York 1984) p. 175-179

[15] A. Ekert : *Quantum cryptography based on Bells theorem*, PRL **67**, p. 661 [1991]

[16] C. Bennett: *Quantum cryptography using any two nonorthogonal states*, PRL **68**, p.3121 [1992]

[17] P. Kwiat, R.Hughes: *Practical free-space quantum key distribution over 1 km* PRL **81**, p. 3283 [1998]

[18] N. Gisin, S. Massar: *Optimal quantum cloning machines*, PRL **79**, p. 2153 [1997]

[19] M. Zukowski, A. Zeilinger, M. Horne, A. Ekert: *"event-ready detectors" Bell-Experiment via entanglement swapping* PRL **71**, p. 4287 [1993]

[20] S. Bose, G. Verdral, P. Knight: *A multiparticle generalization of entanglement swapping*, `quant-ph/9708004`

[21] N. Lütkenhaus, J. Calsamiglia, K.-A. Suominen: *On Bell measurements for teleportation*, `quant-ph/9809063` (to appear in PRA 7/99)

[22] L. Vaidman, N. Yoram *Methods for reliable teleportation*, `quant-ph/9808040`

[23] C. Bennett, S. Wiesner: *Communications via one- and two-particle operation on EPR-states* PRL **69**, p. 2881 [1992]

[24] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera: *Quantum privacy amplification and the security of quantum cryptography*, PRL **77**, p.2818 [1996]

[25] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W. Wootters: *Purification of noisy entanglement and faithful teleportation via noisy channels* PRL **76**, p. 722 [1996]

[26] C. Bennett, H. Bernstein, S. Popescu, B. Schumacher: *Concentrating partial entanglement by local operations* `quant-ph/9511030`

[27] Star Trek, `Technical Manual`

[28] A. Ekert, R. Jozsa: *Quantum computation and Shors factoring algorithm* Rev.Mod.Physics **68**, p. 733 [1996]

[29] A. Steane: *Multiple particle interference and quantum error correction* Proc. Royal Society 452, p. 2551 [1996] und `quant-ph/9601029`; *Quantum computing* Repts. Prog. Phys **61**, p. 117 [1995] und `quant-ph/9708022`

[30] A.Barenco: *Quantum physics and computers*, `quant-ph/9612014`

[31] P.Shor: *Scheme for reducing decoherence in quantum computer memory* PRA **52**, p. R2493 [1995]

[32] A.Steane: *Error correcting codes in quantum theory* PRL **77**, p. 793 [1996]

[33] G. Hardy, E. Wright: *Introduction to the Theory of Numbers*, Oxford Clarendon Press [1993]

[34] M. Schröder: *Number Theory in Science and Communications and Applications*, Springer [1993]

[35] L. Grover: *Quantum Computers can search arbitrarily large databases by a single query* PRL **79**, p.4709 [1997]; *Quantum mechanics helps in searching for a needle in a haystack* PRL **79**, p.325 [1997]

[36] A.Barenco: *Quantum physics and computers*, Contemp. Physics **37**, p.375 [1996] [introductory text]

[37] M.Boyer, G.Brassard, P.Høyer und A.Tapp: *Tight bounds on quantum searching* `quant-ph/9605034`

[38] I. Cirac, P. Zoller: *Quantum computations with cold trapped ions*, PRL **74**, p. 4091 [1995]

[39] B. Schumacher: *Quantum coding* PRA **51**, p. 2738 [1995]

[40] R. Jozsa, M.+P.+R. Horodecki: *Universal quantum information compression* PRL **81**, p. 1714 [1998]

[41] W. Wootters und W. Zurek: *A single quantum cannot be cloned* Nature **299**, p. 802 [1982]

[42] V. Buzek, M. Hillery: *Quantum copying: beyond the no-cloning theorem* PRA **54**, p.1844 [1996]

[43] D. Bruß, D. DiVincenzo, A. Ekert, C. Fuchs, C. Macchiavello, J. Smolin: *Optimal universal and state dependent quantum coding* PRA **57**, p. 2368 [1998]

[44] N. Gisin, S. Massar: *Optimal quantum cloning machines* PRL **79**, p. 2153 [1997]

[45] S. Massar, S. Popescu: *Optimal extraction of information from finite quantum ensembles* PRL **74**, p. 1259 [1995]

[46] R. Gehring: *Asymetrisches*, Linux Magazin 10/98, Seite 42ff. [1995]

© 1998/1999 by Prof. M.Lewenstein, Helge Kreutzmann und Christian Trump