Über die Struktur von verschränkten Zuständen

Von dem Fachbereich Physik der Universität Hannover
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
– Dr. rer. nat. –

genehmigte Dissertation

von
Dipl.-Phys. Siniša Karnas
geboren am 03. Dezember 1971 in Nienburg/Weser

2001

Referent:Prof. Dr. Maciej Lewenstein
Korreferent:Prof. Dr. Olaf Lechtenfeld
Tag der Promotion:13. Dezember 2000.

Zusammenfassung
Über die Struktur von verschränkten Zuständen

In der vorliegenden Arbeit werden mehrfach zusammengesetzte quantenmechanische Systeme auf ihre Separabilität hin untersucht.

Nach einer kurzen Einleitung wird auf die “beste separable Approximation” (im weiterem Verlauf BSA [1]) eingegangen. Bei der BSA handelt es sich um eine optimale Zerlegung von quantenmechanischen Zuständen in sogenannte separable und verschränkte Anteile. Die Existenz solch einer BSA-Zerlegung wird dabei durch das BSA-Theorem [1] bewiesen. Auch die Eindeutigkeit solch einer BSA-Zerlegung wird gezeigt. Ebenfalls wird die analytische Beschreibung der Menge aller separablen Dichtematrizen präsentiert, welche die Eigenschaft besitzen, daß ihre Differenz zu einem gegebenen quantenmechanischen Zustand positiv definit ist. Aufbauend auf diese Untersuchungen wird die BSA-Zerlegung von $C^2 \otimes C^2$-Zuständen betrachtet. Dabei wird eine Ungleichung geliefert, die die Aussage darüber macht, wann die BSA-Zerlegung unter gegebenen Voraussetzungen keinen maximal verschränkten Zustand als Rest enthält. Als natürliche Fortsetzungen der bisherigen BSA-Untersuchungen ergab sich eine Verallgemeinerung dieser Theorie auf PPT-Zustände, d.h. Zustände, welche nach einer sogenannten partiellen Transposition auch weiterhin Zustände bleiben. Diese verallgemeinerte Theorie wurde PPT-BSA-Theorie genannt und lieferte die Möglichkeit der Konstruktion von Witness-Operatoren bzw. Bellschen Ungleichungen für jeden verschränkten Zustand. Ebenfalls ergab sich aus den Untersuchungen ein neues Verschränktheitsmaß.

Die mathematischen Methoden, die bis zur PPT-BSA-Theorie entwickelt wurden, erwiesen sich besonders bei der Untersuchung der Separabilität von quantenmechanischen $C^2 \otimes C^N$- und $C^2 \otimes C^2 \otimes C^N$-Zuständen als erforderlich. Das Resultat dieser Untersuchungen sind zahlreiche Separabilitätskriteria sowie konstruktive Methoden, um Zustände mathematisch nach deren Separabilität hin zu prüfen.

Schlagworte: Verschränktheit, Quanteninformationstheorie,
Verschränkheitsmaß, Separabilität
PACS: 03.67.−a, 03.65.Bz, 03.65.Ca, 03.67.Hk

Abstract
About the Structure of Entangled States

In this dissertation states of multi-composite quantum systems are investigeted with regard to their separability property.

After a short introduction, the best separable approximation (BSA [1]) will be considered. The BSA is an optimal decomposition of a quantum state in so called separable and entangled states. The existent of such BSA decomposition is proven by the BSA theorem ([1]). The analytical description of the set of all separable states, with the property that their difference from a given entangled state is positive defined, will be presented. After that, it will be shown that the BSA decomposition is unique and can be used to define an entanglement measure. Ased on this result, the BSA decomposition of $C^2 \otimes C^2$ quantum states will be studied. The result of this investigation will be a inequality for so called generic entangled states. This inequality gives us information, under which circumstances, the entangled state in the BSA decomposition will not be maximally entangled. As a natural continuation of the previous studies of BSA, the BSA theory will be generalized to PPT states (i.e. the states which after a so called partial transpositionäre still physical states). This theory is called PPT-BSA theory. Using this we have the possibility to construct so called Witness operators or Bell's inequalities for a given quantum entangled state.

The mathematical methods which has been developed in the PPT-BSA theory, turn out to be very useful for the investigation of quantum states in $C^2 \otimes C^N$ and $C^2 \otimes C^2 \otimes C^N$ Hilbertspace. This research allows to formulate several separability criteria and constructive method's for checking the separability of quantum states in such Hilbert spaces.

Keywords: Entanglement, Quantuminformation, Entanglement Measure, Separability
PACS: 03.67.−a, 03.65.Bz, 03.65.Ca, 03.67.Hk

Inhaltsverzeichnis

Kapitel 1

Einleitung

In den letzten zehn Jahren kam es zu einer rasanten Entwicklung auf dem Gebiet der Quanteninformationsverarbeitung und der Quanteninformationstheorie.

Ein Grund für diese Entwicklung war der Vorstoß der Halbleitertechnologie zu immer kleineren Größenordnungen, die aber bei der Miniaturisierung auf atomarer Ebene auf ihre Grenzen stoßen wird. In diesen Bereichen sind es die Gesetze der Quantenmechanik, die relevant werden, und es ergibt sich dabei die Frage, wie sich Informationsverarbeitung innerhalb der Quantenmechanik verhält.

Die ersten Untersuchungen zu diesem Thema wurden Mitte der 80-er Jahre von R. Feynman vorgenommen [2]. Mitte der 90-er kam es dann zu einer ausschlaggebenden Wende auf dem Gebiet der Quanteninformationsverarbeitung. P. W. Shor [3] fand einen polynomialen Quantenalgorithmus für die Primfaktorisierung. Kurz nach Shors Entdeckung fand Grover [4] einen Quantensuchalgorithmus. Diese Arbeiten führten zu einer explosionsartigen Forschungswelle auf dem Gebiet der Quantenalgorithmen und der Quantencomputer ([5], [6], [7], [8], [9] und [10]). In der praktischen Verwirklichung von Quantenalgorithmen durch Quantencomputer sah man sich allerdings mit dem Problem der Dekohärenz ([11], [12], [13], [14], [15] und [16]) konfrontiert. Dies führte wiederum zur Entwicklung von Quanten-Fehlerkorrektur-Codes ([17], [18] und [19]).

Ein weiterer Grund für die rasante Entwicklung waren Anwendungen der Quantenmechanik in der Kryptographie (Für Leser, welche an der klassischen Kryptographie interessiert sind, empfehle ich das ausgezeichnete Buch von Bruce Schneier [20] sowie [21] und [22]). Durch die Quantenkryptographie ([23], [24], [25] und [26]) war es mit den Gesetzen der Quantenmechanik möglich, sichere Nachrichtenübertragung zu gewährleisten. Dies führte zu einem wachsenden Interesse zahlreicher Unternehmen an der Quantenkryptographie.

Um Quantenkryptographie betreiben zu können, müssen Quantenzustände natürlich auch transportiert werden. Wie in der Nachrichtentheorie ergab sich daher die Notwendigkeit nach einer mathematischen Beschreibung von quantenmechanischen Kanälen ([27], [28] und [29]). Desweiteren fand man für die Quantenkommunikation noch zahlreiche weitere Anwendungen wie die Teleportation [30], Purifikation [31], Pseudo/Destillation ([32],[33] und [34]) und Quantenkatalyse ([35] und [36]).

Außer der Quantenkommunikation ergab sich durch die Untersuchungen von quantenmechanischen Systemen die Möglichkeit, Messungen an einem System durchzuführen, ohne es zu beeinflussen. Diese faszinierende Vorstellung wurde unter den Namen "Wechselwirkungsfreie Messung" (Interactions-Free Measurments) bekannt ([37] und [38]). Zahreiche Experimente ([39], [40], [41], [42] und [43]) zu diesem Thema führten ebenfalls zu einer Forschungswelle auf dem Gebiet der quantenmechanischen Messungen. Oftmals wird die quantenmechanische wechselwirkunsfreie Messung mit der quantenmechanischen zerstörungsfreien Messung ("Quantum non-demolition Measurment" [44], [45], [46], [47], [48] und [49]) verwechselt. Bei der quantenmechanischen zerstörungsfreien Messung handelt es sich um solch eine Messung an einem quantenmechanischen System, welche das quantenmechanische System nach der Messung "unversehrt" läßt. Es ist noch weiterhin offen in wie weit die letzteren beiden Begriffe zusammenhängen.

Alle aufgezählten Anwendungen der Quanteninformationsverarbeitung besitzen ein enormes Potential und können unsere Informationsgesellschaft im neuen Jahrhundert grundlegend verändern.

Der Begriff eines "verschränkten Zustandes" [50] taucht in allen diesen Anwendungen der Quanteninformationsverarbeitung auf. Aus diesem Grund sind die Untersuchungen zur mathematischen Beschaffenheit von verschränkten Zuständen nicht nur von rein akademischer sondern auch von anwendungsbezogener Natur. Dies war auch der Grund, weshalb ich gerade dieses Thema für meine Dissertation gewählt habe.

Bevor aber auf die Resultate in dieser Arbeit eingegangen wird, folgt noch eine kurze Beschreibung der Inhalte der Kapitel. Diese spiegelt auch den chronologischen Verlauf meiner Untersuchungen in den letzten drei Jahren wieder.

Die beiden folgenden Kapitel beschäftigen sich mit den verwendeten mathematischen Konventionen und einer Einführung in die Grundlagen der Quanteninformationstheorie.

Gefolgt von einer kurzen Einleitung in die BSA-Theorie [1] wird in Kapitel 4 eine Beschreibung der sogenannten BSA-Mannigfaltigkeit geliefert. Danach wird

die Eindeutigkeit der BSA-Zerlegung bewiesen. Die Untersuchungen in diesem Kapitel sind von allgemeiner Natur.

Kapitel 5 beschäftigt sich mit der BSA-Zerlegung von zwei $q-$Bit-Dichtematrizen. Dort werden notwendige Bedingungen dafür geliefert, daß die BSA-Zerlegung für sogenannte generische Zustände keinen maximal verschränkten Zustand als BSA-Rest enthält.

Inspiriert durch die BSA-Theorie wird in Kapitel 6 eine BSA-Theorie für PPT-Zustände (PPT-BSA) entworfen. Zu dieser PPT-BSA-Theorie wird auch der dazugehörige Zerlegungsalgorithmus präsentiert. Dieser Algorithmus wird durch Anhang B ergänzt und verdeutlicht. Desweiteren wird der Zusammenhang zu den Witness-Operatoren erläutert.

In Kapitel 7 wird aus der BSA-Zerlegung ein Verschränktheitsmaß vorgeschlagen und untersucht.

Aufbauend auf den gewonnenen mathematischen Untersuchungen der letzteren Kapitel wird in Kapitel 8, entstanden durch die Zusammenarbeit von Prof. Dr. J. I. Cirac und Frau B. Kraus aus der Arbeitsgruppe in Innsbruck und meinem Mentor Prof. Dr. M. Lewenstein, die Separabilität von niedrigrängigen $C^2 \otimes C^N$-Zuständen untersucht ([51] und [52]). Desweiteren wurden Separabilitätstests für solche Zustände vorgeschlagen und anhand zahlreicher Beispiele verdeutlicht.

Eines der Herzstücke der hier vorliegenden Arbeit ist Kapitel 9. Dort werden alle vorherigen Resultate für die Untersuchung der Separabilität von niedrigrängigen $C^2 \otimes C^2 \otimes C^N$-Zuständen benutzt. Desweiteren werden wie in Kapitel 8 Separabilitätstests für PPT-Zustände in $C^2 \otimes C^2 \otimes C^N$ vorgeschlagen und speziell für $C^2 \otimes C^2 \otimes C^2$-Zustände erläutert.

Anschließend wird als Ausblick in Kapitel 10 auf mögliche zukünftige Untersuchungen von verschränkten PPT-Zuständen eingegangen.

Kapitel 2

Mathematische Konventionen

In diesem Kapitel werden die mathematischen Schreibweisen und Konventionen beschrieben, die in dieser Arbeit verwendet werden.

Quantenmechanische Zustände sind normierte $(\mathrm{tr}(\rho) = 1)$ positiv definite Operatoren $\rho \geq 0$, welche auf einen abzählbaren, mehrfach zusammengesetzten Hilbertraum $H = C_1^{N_1} \otimes C_1^{N_2} \otimes \ldots \otimes C_1^{N_M}$ der Dimension $\dim H = \prod_{i=1}^{M} N_i$ wirken. Der Einfachheit halber hat es sich in der Informationstheorie eingebürgert, Hilberträumen Namen statt Numerierungen zu geben. Das bedeutet z.B. für ein zweifach zusammengesetztes System $H = C_1^N \otimes C_2^M$, daß man $H = C_A^N \otimes C_B^M$ schreibt und von Alices und Bobs zusammengesetztem System redet. Dies macht es einfacher, komplexere Vorgänge nachzuvollziehen. Gilt die Beziehung, daß $\rho^2 = \rho$ ist, so spricht man von einem reinen Zustand. Ist diese Bedingung nicht erfüllt, so spricht man von einem gemischten Zustand. Dies bedeutet, daß wenn man nur über "den Zustand" redet, damit keinen Unterschied zwischen einem reinen oder einem gemischten Zustand macht.

Mit $R(\rho)$, $K(\rho)$, $r(\rho)$ und $k(\rho)$ bezeichnet man das Bild, den Kern, die Dimension des Bildes und die Dimension des Kerns von ρ. Das Bild eines Operators O ist definiert als die Menge $\mathrm{R}(O) = \{ |\psi\rangle |\ \ |\psi\rangle = O|\phi\rangle \ \ \forall |\phi\rangle \in H \}$ und der Kern ist definiert als die Menge $\mathrm{K}(O) = \{ |\phi\rangle |\ \ 0 = O|\phi\rangle, \ \ |\phi\rangle \in H \}$. Desweiteren bezeichnet $\mathrm{tr}(O)$ die Spurbildung eines Operators O. Die Abkürzung "O.B.d.A" steht für "Ohne Beschränkung der Allgemeinheit" und taucht mehrfach in dieser Arbeit auf. $|\hat{e}\rangle$ bezeichnet einen Hilbertvektor, der zum Hilbervektor $|e\rangle \in C^2$ orthogonal ist.

Messungen bzw. Operationen auf den jeweiligen quantenmechanischen Systemen werden durch sogenannte vollständige positive Abbildungen POVM (positive

operator valued measurement) beschrieben ([53], [54] und [55]). Die POVMs sind die allgemeinsten Messungen, die an einem quantenmechanischen System durchgeführt werden können. Dies sind Messungen, die nicht nur auf dem gewünschten System durchgeführt werden, sondern zusätzlich auch auf einem weiteren System, welches man Ancilla nennt. Die Ancilla kann ein System sein, welches man kennt und über das man Kontrolle besitzt oder aber auch die äußere Umgebung des Systems, die man nie vollständig vom System abkoppeln kann.

Gegeben sei ein zusammengesetztes quantenmechanisches System $|\Psi\rangle = |\psi\rangle \otimes |A\rangle \in H = H_A \otimes H_{\text{Ancilla}}$. Nun wird eine vollständige Messung mittels der Projektoren $\{P_i\}$ durchgeführt. Vollständig bedeutet, daß $\sum_i^{\dim H} P_i = 1$ gilt. Dies führt zu

$$\begin{aligned} |\Psi\rangle\langle\Psi| &\mapsto \sum_i P_i|\psi\rangle\langle\psi| \otimes |A\rangle\langle A|P_i \\ &= \sum_i P_i|A\rangle|\psi\rangle\langle\psi|\langle A|P_i. \end{aligned}$$

Nun bildet man die Spur über die Ancilla und entledigt sich dadurch der Information über dieses Teilsystem:

$$\text{tr}_{\text{Ancilla}} \sum_i P_i|A\rangle|\psi\rangle\langle\psi|\langle A|P_i = \sum_i \sum_\alpha \langle a_\alpha|P_i|A\rangle|\psi\rangle\langle\psi|\langle A|P_i|a_\alpha\rangle,$$

wobei $\sum_\alpha |a_\alpha\rangle\langle a_\alpha| = 1_{\text{Ancilla}}$ ein vollständiges System bzgl. H_{Ancilla} ist. Nun definiert man $V_I \equiv \langle a_\alpha|P_i|A\rangle$, wobei I für eine weitere Nummerierung steht, welche durch die Beziehung $I \equiv (i,\alpha)$ definiert wird. Somit erhält man

$$|\Psi\rangle\langle\Psi| \mapsto \sum_I V_I|\psi\rangle\langle\psi|V_I^\dagger \equiv \rho. \tag{2.1}$$

Offensichtlich erfüllen die $\{V_I\}$'s folgende wichtige Beziehung:

$$\sum_I V_I V_I^\dagger = 1, \tag{2.2}$$

welche man Vollständigkeit nennt. Die $\{V_I\}$'s sind die schon erwähnten POVMs. Offensichtlich bildet die Menge aller POVMs eine viel mächtigere Menge von Messungen als die üblichen Projektionsmessungen, da sie diese als Untermenge schon enthalten. Wird nun auf einem System ρ eine POVM-Messung durchgeführt, und ist der Ausgang der Messung I, so geht ρ über in

$$\rho \mapsto \frac{V_I \rho V_I^\dagger}{\text{tr}(V_I \rho V_I^\dagger)}, \tag{2.3}$$

wobei $\mathrm{tr}(V_I \rho V_I^\dagger)$ die Wahrscheinlichkeit für den Ausgang der Messung I ist.

Nun lassen sich auch POVMs durch klassische Kommunikation korrelieren (local quantum operation and classical communication (LOCC)). Dies wird bewerkstelligt, indem z.B. Alice und Bob nur bei ganz bestimmten Ausgängen von Messungen ihren quantenmechanischen Zustand behalten. Es ist klar, daß in diesem Fall die Ausgänge der Messungen jeweils übertragen werden müssen:

$$\rho \mapsto \frac{A_I \otimes B_J \rho A_I^\dagger \otimes B_J^\dagger}{\mathrm{tr}(A_I \otimes B_J \rho A_I^\dagger \otimes B_J^\dagger)} \equiv \rho_{IJ}. \tag{2.4}$$

Die Wahrscheinlichkeit dafür ist durch $\mathrm{tr}(A_I \otimes B_J \rho A_I^\dagger \otimes B_J^\dagger)$ gegeben.

Desweiteren redet man von einem Quantenkanal (z.B. der Pauli-Kanal [29]) wenn man nicht die Möglichkeit besitzt, den Ausgang I der "Messung" zu detektieren.

Wie schon erwähnt, ist eine weitere Möglichkeit, die Messung nur auf der Ancilla durchzuführen. Man besitzt wiederum einen Zustand $|\psi\rangle \otimes |A\rangle$ und läßt diesen wechselwirken:

$$|\psi\rangle\langle\psi| \otimes |A\rangle\langle A| \to U_{\psi A} |\psi\rangle\langle\psi| \otimes |A\rangle\langle A| U_{\psi A}^\dagger. \tag{2.5}$$

Nun wird eine vollständige Messung auf der Ancilla durchgeführt:

$$\begin{aligned} U_{\psi A} |\psi\rangle\langle\psi| \otimes |A\rangle\langle A| U_{\psi A}^\dagger &\sim \sum_a \langle a| U_{\psi A} |\psi\rangle\langle\psi| \otimes |A\rangle\langle A| U_{\psi A}^\dagger |a\rangle, \\ &= \sum_a \langle a| U_{\psi A} |A\rangle |\psi\rangle\langle\psi| \langle A| U_{\psi A}^\dagger |a\rangle, \\ &= \sum_a V_a[A] |\psi\rangle\langle\psi| V_a[A]^\dagger. \end{aligned}$$

Auf diese Art und Weise lassen sich insbesondere zerstörungsfreie Messungen ("Quantum non-demolition measurements" s. [44], [45], [46], [47], [48] und [49]) auf $|\psi\rangle$ durchführen. Der Grund dafür ist, daß auf dem Zustand $|\psi\rangle$ nicht direkt gemessen wird.

Für einen tieferen mathematischen Einblick in die Quanteninformationstheorie empfehle ich das Buch von Asher Peres [56], sowie weitere Literatur zu diesem Thema (z.B. [57], [58] und [59]).

Kapitel 3

Grundlagen der Quanteninformationstheorie

3.1 Inhalt dieses Kapitels

Es wird eine kurze Einleitung in die Grundlagen der heutigen Quanteninformationstheorie gemacht. Nach einem kurzen Unterkapitel über die Bellsche Ungleichung wird auf die Definition von separablen und verschränkten Zuständen, sowie deren Separabilitätskriterien eingegangen. Es folgen Erläuterungen zum Thema Teleportation, Pseudo-Destillation, Quantenkatalyse und Verschränktheitsmaße. Das Ziel dieses Kapitels ist, unerfahreren Lesern einen schnellen und sachlichen Einstieg in die Quanteninformationstheorie zu ermöglichen.

3.2 Bellsche Ungleichung

Seit der Formulierung der Quantenmechanik gibt es, trotz ihrer überwältigenen Erfolge in der Vorhersage und Erklärung von Experimenten, noch immer Skeptiker, die behaupten, daß die Quantenmechanik **keine vollständige** Theorie sei [60] und daß dies der Grund für ihre probabalistische Eigenschaft wäre.

Was bedeutet “keine vollständige Theorie”? Nun, es bedeutet, daß die Anzahl der Parameter, die gebraucht wird, um eine gegebene physikalische Situation zu beschreiben, größer ist als die Anzahl der Parameter, die die Theorie besitzt. Dies hat zur Folge, daß die Theorie zwangsweise verschiedenen physikalischen Anfangsbedingungen die gleichen Anfangsbedingungen bezüglich der Theorie zuordnet.

Daraus ergibt sich dann, daß die Theorie wahrscheinlichkeitsartige Eigenschaften haben muß, da sie nicht mehr in der Lage ist, deren weiteren Ablauf zu beschreiben. Deswegen sollte dies der Grund sein, weshalb man in der Quantenmechanik nur Aussagen über Mittelwerte von Observablen machen kann. Im Grunde genommen sollte die Welt also einen deterministischen Charakter besitzen.

Das Argument, was diese Meinung bestätigen sollte, letzten Endes doch zum Fall der Theorie der verschteckten Variablen führte, war der Begriff eines **verschränkten Zustandes**, welcher in der Quantenmechanik auftaucht. Ein verschränkter Zustand ist ein Zustand, welcher sich nicht als Produkt von zwei Zuständen schreiben läßt ($|\psi\rangle \neq |A\rangle \otimes |B\rangle$).

Der wohl am bekannteste verschränkte Zustand ist ein Spin$\frac{1}{2}$−Singuellet $|s\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$[60]. Man spricht auch von einem Photonensingulet, obwohl dieses ein Spin-1-Teilchen ist. Der Grund dafür ist, daß man die nullte Komponente des Spins wegen der Eichinvarianz immer wegeichen kann. Dadurch besitzt das Photon nur zwei Spinausrichtungen. Die Argumentation gegen die Quantenmechanik verlief wie folgt: Angenommen zwei räumlich getrennte Beobachter (im weiteren Verlauf Alice und Bob) teilen sich den verschränkten Zustand $|s\rangle$. Nun macht Alice eine Spinmessung an ihrem Teilchen. Die Wellenfunktion kolabiert je nach Ausgang ihrer Messung in den Zustand $|\uparrow\downarrow\rangle$ oder $|\downarrow\uparrow\rangle$. Laut Quantenmechanik liegt der Ausgang einer Messung nicht vor der Messung fest, sondern erst während der Messung. Dies bedeutet aber dann auch, daß der Zustand auf Bobs Seite momentan durch Alices Messung beinflusst wurde, obwohl die beiden räumlich getrennt sind. Die Quantenmechanik hätte somit einen **nicht-lokalen** Charakter.

Da dies nicht möglich sein konnte, mußte schon vor der Messung feststehen, wie der Ausgang der Messung verlaufen sollte. Die Parameter, die dies beschreiben sollten, nannte man **versteckte Variablen**. Es sollte also möglich sein, eine Theorie mit versteckten Variablen zu formulieren, welche in der Lage wäre alle Mittelwerte von Observablen in der Quantenmechanik vorherzusagen.

Was aber, wenn solch eine Theorie nicht existiert? Dann würde man als theoretischer Physiker einer “Geistertheorie” hinterherjagen. Zum Glück lieferte Bell [61] ein notwendiges Kriterium, welches jede Theorie mit versteckten Variablen erfüllen sollte und welches sich empirisch nachprüfen läßt.

Wir definieren nun $A(\vec{\alpha}, \lambda) = \pm 1$ als eine Funktion, die uns den Ausgang von Alice Spinmessung in $\vec{\alpha}$ Richtung vorhersagt, falls die versteckte Variable λ vorliegt. λ steht für eine ganze Klasse von versteckten Variablen. Ebenso wird für Bob ein $B(\vec{\beta}, \lambda)$ definiert.

Da wir nun nichts von den versteckten Variablen wissen, sollten die Mittelwerte

der Observablen beschrieben werden durch:

$$\langle A(\vec{\alpha})\rangle = \int d\lambda p(\lambda) A(\vec{\alpha},\lambda), \tag{3.1}$$

wobei $p(\lambda)$ die statistische Verteilung der versteckten Variablen beschreibt. Wir sind nun an Korrelationsmessungen am Zustand $|s\rangle$ zwischen Alice und Bob interessiert. Dieser wird beschrieben durch:

$$\langle A(\vec{\alpha})B(\vec{\beta})\rangle = \int d\lambda p(\lambda) A(\vec{\alpha},\lambda))B(\vec{\beta},\lambda). \tag{3.2}$$

Aus der Definition von $A(\vec{\alpha},\lambda)$ folgt, daß $A(\vec{\alpha},\lambda)^2 = 1$ und aus der Struktur von $|s\rangle$ folgt, daß $A(\vec{\alpha},\lambda) = -B(\vec{\alpha},\lambda)$.

Nun schreiben wir

$$\begin{aligned}\langle A(\vec{\alpha})B(\vec{\beta})\rangle - \langle A(\vec{\alpha})B(\vec{\gamma})\rangle &= -\int d\lambda p(\lambda)[A(\vec{\alpha},\lambda)A(\vec{\beta},\lambda) - A(\vec{\alpha},\lambda)A(\vec{\gamma},\lambda)] \\ &= \int d\lambda p(\lambda) A(\vec{\alpha})A(\vec{\beta})[1 - A(\vec{\beta},\lambda)A(\vec{\gamma},\lambda)].\end{aligned}$$

Da nun $A(\vec{\alpha},\lambda), B(\vec{\beta},\lambda) \in \{-1,+1\}$, ergibt sich folgende Ungleichung:

$$|\langle A(\vec{\alpha})B(\vec{\beta})\rangle - \langle A(\vec{\alpha})B(\vec{\gamma})\rangle| \leq 1 - \langle A(\vec{\beta})B(\vec{\gamma})\rangle. \tag{3.3}$$

Diese Ungleichung nennt man **Bellsche Ungleichung**. Die Bellsche Ungleichung setzt ein notwendiges Kriterium für die Mittelwerte fest, die eine Theorie mit versteckten Variablen erfüllen muß.

Was bedeutet nun die Verletzung von (3.3)? Es bedeutet, daß sich die Mittelwerte von Observablen **nicht** durch eine lokale Theorie von versteckten Variablen in der Form (3.2) beschreiben lassen. In Worten bedeutet (3.2), daß der Ausgang von Alice Messung nicht vor der Messung vorlag. Dies führt dann zur Schlußfolgerung, daß Alice Messung den Zustand von Bob beeinflußt hat.

Man sieht also, daß es quantenmechanische Zustände gibt, die nicht durch ein Modell von versteckten Variablen beschrieben werden können. Solche Zustände besitzen eine neue Art von Korrelation, die mit der klassischen nicht verglichen werden darf. Dieser physikalische Sachverhalt führte zu einer generischen Charakterisierung von korrelierten quantenmechanischen Zusänden in verschränkte (nicht klassisch korrelierte) und separable (klassisch korrelierte) quantenmechanische Zustände.

3.3 Separable und verschränkte Zustände

Es werden nun die Begriffe von separablen und verschränkten Zuständen mathematisch definiert.

Definition 1 *Ein Quantenzustand* ρ_s *heißt* **separabel** *[69], wenn er sich schreiben läßt als:*

$$\rho_s = \sum_\alpha p_\alpha |\psi_\alpha^1\rangle\langle\psi_\alpha^1| \otimes |\psi_\alpha^2\rangle\langle\psi_\alpha^2| \otimes \ldots \otimes |\psi_\alpha^N\rangle\langle\psi_\alpha^N|, \tag{3.4}$$

wobei $|\psi_\alpha^1\rangle, |\psi_\alpha^2\rangle \ldots |\psi_\alpha^N\rangle \in H_1 \otimes H_2 \otimes \ldots \otimes H_N$.

Ein separabler Zustand ist also ein Zustand, welcher von N räumlich getrennten Parteien allein nur durch lokale Operationen und klassische Kommunikation zusammengesetzt werden kann. Dies geschieht so, daß sich die N Parteien als erstes auf einen Zufallsgenerator einigen (klassische Kommunikation) und dann, je nach Ergebnis des Zufallsgenerators, die jeweiligen Zustände $|\psi_\alpha^1\rangle, |\psi_\alpha^2\rangle \ldots |\psi_\alpha^N\rangle$ bei sich lokal präparieren. Der Zufallsgenerator spielt offensichtlich die Rolle einer versteckten Variable, so daß jeder separable Zustand den Bellschen Ungleichungen genügen muß.

Nun kommen wir zur Definition von verschränkten Zuständen:

Definition 2 *Einen Quantenzustand, welcher* **nicht separabel** *ist, nennt man* **verschränkt**.

Dies bedeutet, daß verschränkte Quantenzustände **nicht** durch lokale Operationen und klassische Kommunikation präpariert werden können.

Der nächste natürliche Schritt ist nun eine generische Charakterisierung von Quantenzuständen nach Verschränktheit und Separabilität. Dies führt zur fundamentalsten Frage in der heutigen Quanteninformationstheorie:

> **Gegeben sei ein Quantenzustand ρ. Ist dieser Quantenzustand separabel oder verschränkt ?**

Was auf anhieb sehr trivial klingt, erweist sich als das krasse Gegenteil von Trivialität.

Im nächstem Kapitel gehen wir auf einige wichtige Separabilitätskriterien ein, die im Verlauf dieser Arbeit für Untersuchungen zwingend erforderlich werden. Auserdem liefern die Separabilitätskriterien weitere natürliche Unterteilungen von verschränkten Zuständen.

3.4 Separabilitätskriteria

Das wohl am bekannteste und wichtigste Separabilitätskriterium ist das Peres-Horodeckis Kriterium [70] für Separabilität. Es wird im nächsten Abschnitt behandelt.

3.4.1 Peres-Horodeckis Kriterium für Separabilität

Das erste notwendige Separabilitätskriterium wurde von Asher Peres [70] und der Horodecki Familie [71] formuliert. Um dieses Kriterium zu formulieren, muß der Begriff der partiellen Transposition erläutert werden. Der Einfachheit halber geschieht dies für zweifach zusammengesetzte Systeme.

Sei ρ ein positiv definiter Operator, welcher auf $C_A^M \otimes C_B^N$ wirkt. Gegeben sei eine vollständige reelle orthonormalbasis $\{|\,i\rangle\} \in C_A^M$. Dann ist die partielle Transposition in bezug auf Alices Raum definiert durch:

$$\rho^{t_A} = \sum_{i.j=0}^{M-1} \langle i\,|\rho|\,j\rangle|\,j\rangle\langle i\,| \tag{3.5}$$

Sei $\{|\,e_i\rangle = \sum_{j=0}^{M-1} e_{ij}|\,j\rangle\}$ eine weitere vollständige orthonormale Basis in Alices Raum. Daraus ergibt sich mit Hilfe von (3.5) folgende nützliche Eigenschaft:

$$\langle e_i\,|\rho|\,e_j\rangle = \langle e_j^*\,|\rho^{t_A}|\,e_i^*\rangle, \tag{3.6}$$

wobei $|\,e_i^*\rangle = \sum_{j=0}^{M-1} e_{ij}^*|\,j\rangle$ ist. Die partielle Transposition kann nun dementsprechend auf M-fach zusammengesetzte Systeme verallgemeinert werden.

Die Peres-Horodecki Bedingung besagt, daß jeder separable Zustand nach einer **partiellen Transposition** (in Bezug auf alle möglichen Subsysteme) wieder ein separabler Zustand sein muß und damit positiv definit. Für ein zweifach zusammengesetztes System bedeutet dies:

$$\rho = \rho_s \Rightarrow \rho^{t_B} \geq 0, \tag{3.7}$$

wobei die partielle Transposition mit Hilfe von (3.5) und (3.6) wie folgt definiert ist:

$$\rho^{t_B} := \sum_{\alpha} \lambda_\alpha|\,e_\alpha\,f_\alpha^*\rangle\langle e_\alpha\,f_\alpha^*\,|. \tag{3.8}$$

Allerdings erwies sich dieses Kriterium nur in 2×2 und 2×3 zusammengesetzten Systemen als hinreichend [71]. Dies bedeutet daß es auch verschränkte Zustände

gibt welche nach partiellen Transpositionen wiederum positiv definit sind, aber denoch verschränkt. Dieser Sachverhalt führte zu einer weiteren generischen Charakterisierung von verschränkten Zuständen.

Verschränkte Zustände, welche nach einer partiellen Transposition keine positiven Operatoren mehr sind, nennt man NPPT-verschränkte Zustände (non positive partial transposition) und dementsprechend heißen verschränkte Zustände, welche die Positivität nach einer partiellen Transposition bewahren, PPT-verschränkte Zustände. Sowohl PPT- als auch NPPT-verschränkte Zustände besitzen bestimmte physikalische Eigenschaften. Diese werden im Abschnitt über Destillation und Pseudodestillation noch genauer erörtert und sie liefern eine tiefere physikalische Sichtweise in die mathematische Struktur von verschränkten Zuständen. Man erkennt sofort, daß die vollständige Charakterisierung von verschränkten Zuständen gelöst würde, wenn man wüßte, wie die kanonische Struktur von PPT-verschränkten Zuständen auszusehen hätte. Zahlreiche Arbeiten ([73], [74], [75], [76] und [77]) wurden zu diesem Thema geschrieben. In meiner Arbeit werde ich im Kapitel über die PPT-BSA auf diese Problematik noch genauer eingehen.

Eine etwas komplexere aber dafür auch hinreichende Bedingung, bildet die Bildbedingung, welche von Pawel Horodecki [72] formuliert wurde und mehrfach in dieser Arbeit benutzt werden wird.

3.4.2 Die Bildbedingung

Sei $V \equiv \{|e,f\rangle : \quad |e,f\rangle \in R(\rho), |e^*,f\rangle \in R(\rho^{t_A})\}$, so daß die Anzahl der Elemente der Menge V endlich ist und $P_i \equiv |e_i f_i\rangle\langle e_i f_i|$. Es gilt folgendes Lemma:

Lemma 1 *Der Zustand* ρ *ist genau dann separabel wenn es als konvexe Kombination der* $\{P_i\}$ *geschrieben werden kann.*

Beweis: Die erste Richtung des Beweises ist trivial und folgt aus der Definition eines separblen Zustandes. Gegeben sei also ein separabler Zustand $\rho = \sum_i^N \lambda_i |e_i f_i\rangle\langle e_i f_i|$. Dann gilt $|e_i f_i\rangle \in R(\rho)$. Für jeden Hilbertvektor $|\psi\rangle \in K(\rho)$ gilt nun daß $0 = \langle\psi|\rho|\psi\rangle$ sein muß und damit $\langle\psi|e_i f_i\rangle = 0$. Also sind die $|e_i f_i\rangle$ orthogonal zu jedem $|\psi\rangle \in K(\rho)$ und damit in $R(\rho)$.$_{q.e.d.}$

Seien nun alle $\{P_i\}$ linear unabhängig. Diese Projektoren gehören zur Menge $L[R(\rho)]$ aller linearen Operatoren, welche auf $R(\rho)$ wirken. $L[R(\rho)]$ besitzt demnach die Dimension $r(\rho)^2$. Auf der anderen Seite wiederum sind die Projektoren $\{P_i^{t_A}\}$ ebenfalls linear unabhängig. Dies folgt aus der Invertierbarkeit der partiellen Transposition. Demnach gehören die $\{P_i^{t_A}\}$ zu $L[R(\rho^{t_A})]$. $L[R(\rho^{t_A})]$

besitzt die Dimension $r(\rho^{t_A})^2$. Daraus ergibt sich, daß $L \leq \min(r(\rho)^2, r(\rho^{t_A})^2)$ gelten muß. Nun ist es möglich die Menge $\{P_i\}$ so durch weitere Operatoren $\{P_i, i = L+1, \ldots, r(\rho)^2\}$ zu erweitern, daß sie eine Basis in $L[R(\rho)]$ bilden. Da nun auf $L[R(\rho)]$ ein Hilbertraum mit dem Skalarprodukt $(A,B) \equiv \mathrm{tr}(A^\dagger B)$ definiert ist, kann man auch eine biorthogonale Basis $Q_i \in L[R(\rho)]$ finden, so daß $(Q_i, P_j) = \delta_{ij}$ gilt. Daraus ergibt sich eine notwendige und hinreichende Bedingung für die Separabilität.

Lemma 2 *Sind die $\{P_i\}$ linear unabhängig, dann ist ρ genau dann separabel, wenn $(Q_i, \rho) \geq 0$ für alle $i \leq L$ und $(Q_i, \rho) = 0$ für alle $i > L$ ist.*

Beweis: Da die $\{P_i\}$ eine Basis bilden, kann ρ geschrieben werden als

$$\rho = \sum_{i=1}^{r(\rho)^2} c_i P_i, \tag{3.9}$$

wobei $c_i = (Q_i, \rho)$. Da nun $c_i \geq 0$, folgt, daß ρ separabel ist. Andererseits gilt daß wenn ρ separabel ist dann kann es auch wie (3.9) geschrieben werden, wobei $c_i \geq 0$ für alle $i \leq L$ und $c_i = 0$ für alle $i > L$ ist. Damit wäre der Beweis abgeschlossen.$_{q.e.d.}$

Was aber, wenn man mehr Produktvektoren als $L_0 = \min(r(\rho)^2, r(\rho^{t_A}))$ erhält? In diesem Fall müssen alle möglichen Mengen von linear unabhängigen Projektoren $|e_i f_i\rangle\langle e_i f_i|$ mit mindestens $L_0 = \min(r(\rho)^2, r(\rho^{t_A}))$ Elementen gebildet werden, welche die Bedingung $|e_i f_i\rangle \in R(\rho)$ und $|e_i^* f_i\rangle \in R(\rho^{t_A})$ erfüllen. Für jede Menge wird dann ρ als Linearkombination dieser Projektoren ausgedrückt und dann nachgeprüft, ob in einer Kombination die Koeffizienten alle positiv sind. Dies kann unter Umständen bei einer große Anzahl von Produktvektoren unpraktisch werden. Für diesen Fall kann man die lineare Programmiertheorie anwenden [78]. In dieser Arbeit wird aber im Gegensatz zu der linearen Programiertheorie die PPT-BSA Zerlegungsmethode vorgestellt. Diese Zerlegungsmethode benutzt die von P. Horodecki entwickelte Bildbedingung [72], welche mit Hilfe von Lemma 1 und 2 wie folgt zusammengafasst werden kann:

Allgemeine Bildbedingung: Sei $\rho = \sum_i^N |e_i f_i\rangle\langle e_i f_i|$ ein separabler Zustand. Dann existiert es eine Menge V von Produktvektoren $|e_i f_i\rangle \in R(\rho)$, so daß V das Bild $R(\rho)$ und $\tilde{V} = \{|e^* f\rangle \mathrm{mit} |ef\rangle \in V\} R(\rho^{t_A})$ aufspannt.

Im nächsten Unterkapitel wird auf eine weitere Untersuchungsmethode eingegangen, welche ebenfalls von der Horodecki Familie maßgebend geprägt wurde. Dies sind die positiv linearen Abbildungen.

3.4.3 Positive lineare Abbildungen

Die Horodecki Familie [71] fand heraus, daß zwischen der Klassifizierung von verschränkten Zuständen und der Theorie von sogenannten positiven linearen Abbildungen ein Zusammenhang besteht. Eine positive lineare Abbildung ist wie folgt definiert:

Definition 3 *Eine positive lineare Abbildung S ist eine lineare abbildung $S : L[H_n] \to L[H_m]$, die alle positiv semidefiniten Matrizen $\rho \in L^+[H_n] \subset L[H_n]$ wiederum auf positiv definiten Matrizen $\sigma \in L^+[H_m] \subset L[H_m]$ abbildet.*

Sei id_k nun die Identitätsabbildung auf einen Hilbertraum H_k. Die Abbildung $\mathrm{id}_k \otimes S : L[H_k \otimes H_n] \to L[H_k \otimes H_m]$ für $k = 1, 2, \ldots$ ist definiert durch

$$(\mathrm{id}_k \otimes S)\left(\sum_i \tau_i \pi_i\right) = \sum_i \tau_i \otimes S(\pi_i), \tag{3.10}$$

wobei $\tau_i \in L[H_k]$ und $\pi_i \in L[H_n]$ ist. Die Abbildung S heißt nun $k-$positiv, wenn die Abbildung $\mathrm{id}_k \otimes S$ positiv ist, und heißt dementsprechend vollständig positiv, wenn S positiv für alle $k = 1, 2, \ldots$ ist. Ebenso heißt eine Abbildung k-positiv, falls $\mathrm{id}_k \otimes (ST)$ positiv ist, wobei T die Transposition ist. Nun bezeichnet man eine linear positive Abbildung S als zerlegbar, wenn sie sich schreiben läßt als

$$S = S_1 + S_2 T, \tag{3.11}$$

wobei S_1 und S_2 vollständige positive Abbildungen sind.

Woronowicz [80] konnte beweisen, daß alle positiv linearen Abbildungen $S : L[H_2] \to L[H_2]$ und $S : L[H_2] \to L[H_3]$ zerlegbar sind. Aufbauend auf dieser Arbeit formulierten die Horodeckis [71] das folgende Theorem:

Theorem 1 *Ein Zustand ρ auf $H_A \otimes H_B$ ist verschränkt, falls eine lineare positive Abbildung $S : L[H_B] \to L[calH_B]$ existiert, so daß*

$$(\mathrm{id}_A \otimes S)(\rho) \tag{3.12}$$

nicht mehr positiv semidefinit ist.

Faßt man die Resultate von Woronowicz und den Horodeckis zusammen, so folgt für $H_2 \otimes H_2-$ und $H_2 \otimes H_2-$Zustände ρ, daß diese verschränkt sind, falls $(\mathrm{id}_A \otimes [S_1 + S_2 T])(\rho)$ nicht mehr positiv definit sind. Da nun Lindblad [81] zeigen konnte,

daß es sich bei den S_1 und S_2 um vollständige POVMs handelt, konnte man sich auf $\mathrm{id} \otimes T$ beschränken. Dies ist die “partielle Transposition”.

Doch bevor auf die mathematischen Eigenschaften von verschränkten Zuständen eingegangen wird, müssen noch einige wichtige physikalischen Eigenschaften und Anwendungen von ihnewn beschrieben werden, um ein tieferes Verständnis für den Begriff der Verschränktheit zu erlangen. Eine davon ist die Teleportation.

Zuerst müssen aber noch einige wichtige physikalische Eigenschaften und Anwendungen von verschränkten Zuständen beschrieben werden, um ein tieferes Verständnis für den Begriff der Verschränktheit zu erlangen. Daher wird im nächsten Abschnitt nächer auf die Teleportation eingegangen.

3.5 Teleportation

Eines der wohl sowie in der Quanteninformationstheorie als auch in der breiten Öffentlichkeit interessantesten Phänomene ist der Begriff der **Teleportation** [30], welche auch experimentell ([82], [83], [84] und [85]) verwirklicht wurde. Die Teleportation hat in der Quanteninformationsverarbeitung, wegen ihrer breiten Anwendungsmöglichkeiten, eine wichtige zentrale Bedeutung. Dies wird besonders Einleuchtend wenn man bedenkt wie stark ein quantenmechanischer Zustand während seines transportes zwischen Alice und Bob verrauscht werden kann. Diese Problematik wird auf eine sehr elegante Art und Weise von der Teleportation gelößt, wenn die Parteien einen maximal verschränkten Zustand teilen.

Gegeben sei ein verschänkter Zustand $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ zwischen Alice und Bob. Alice besitzt nun einen unbekannten Quantenzustand $|\phi\rangle = a|0\rangle + b|1\rangle$, den sie zu Bob teleportieren möchte. Es liegt also folgende physikalische Situation vor:

$$\begin{aligned} |\phi\rangle \otimes |\psi\rangle &= (a|0\rangle_A + b|1\rangle_A) \otimes (\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \\ &= \frac{1}{\sqrt{2}}(a|00\rangle_A|0\rangle_B + a|01\rangle_A|1\rangle_B + b|10\rangle_A|0\rangle_B + b|11\rangle_A|1\rangle_B). \end{aligned}$$

Nun macht Alice eine sogenannte Bellsche Messung an dem zu teleportierenden Zustand $|\psi\rangle$ und an ihrer Hälfte des verschränkten Zustandes $|\phi\rangle$. Die Bellsche Messung sind Projektionen auf die Bellschen Zustände welche wie folgt definiert sind:

$$|b_1\rangle_A = \frac{1}{\sqrt{2}}(|00\rangle_A + |11\rangle_A), \tag{3.13}$$

$$|b_2\rangle_A = \frac{1}{\sqrt{2}}(|00\rangle_A - |11\rangle_A), \tag{3.14}$$

$$|b_3\rangle_A = \frac{1}{\sqrt{2}}(|01\rangle_A + |10\rangle_A), \tag{3.15}$$

$$|b_4\rangle_A = \frac{1}{\sqrt{2}}(|01\rangle_A - |10\rangle_A). \tag{3.16}$$

Entwickeln wir nun den Zustand $|\phi\rangle \otimes |\psi\rangle$ nach diesen Bellschen Basen, so erhalten wir folgende Konfiguration:

$$\begin{aligned} |\phi\rangle \otimes |\psi\rangle &= |b_1\rangle_A(a|0\rangle_B + b|1\rangle_B) + |b_2\rangle_A(a|0\rangle_B - b|1\rangle_B) \\ &+ |b_3\rangle_A(a|1\rangle_B + b|0\rangle_B)|b_4\rangle_A(a|1\rangle_B - b|0\rangle_B). \end{aligned}$$

Alice teilt Bob nun ihren Ausgang der Messung mit, wobei Bob durch das folgende Protokoll den unbekannten Quantenzustand wiederherstellen kann:

1. Für den Fall, daß Alice $|b_1\rangle$ gemessen hat, braucht Bob nichts an seinem Zustand $|\phi\rangle$ zu unternehmen.

2. Für den Fall, daß Alice $|b_2\rangle$ gemessen hat, muß Bob die unitäre Operation σ_z ausführen, um den Zustand $|\phi\rangle$ wiederherzustellen.

3. Für den Fall, daß Alice $|b_3\rangle$ gemessen hat, muß Bob die unitäre Operation $i\sigma_y$ ausführen, um den Zustand $|\phi\rangle$ wiederherzustellen.

4. Für den Fall, daß Alice $|b_4\rangle$ gemessen hat, muß Bob die unitäre Operation σ_x ausführen, um den Zustand $|\phi\rangle$ wiederherzustellen.

Es fällt auf, daß ohne die Mitteilung des Ausganges der Bellschen Messung von Alice an Bob keine Teleportation möglich ist. Wäre dem so, so könnte man Informationen mit Überlichtgeschwindigkeit übertragen.

Interessant an Teleportation sind nun vier Aspekte:

1. Die Teleportation ermöglicht es, Quantenzustände zu transportieren, ohne daß sie während des Transportes verrauscht werden. Das setzt natürlich vorraus, daß Alice und Bob schon einen “sauberen” verschränkten Zustand besitzen.

   Dieses läßt sich durch ein **Destillierungsprotokoll** [32] verwirklichen. Auf den Begriff der Destillierung gehe ich später noch ausführlicher ein.

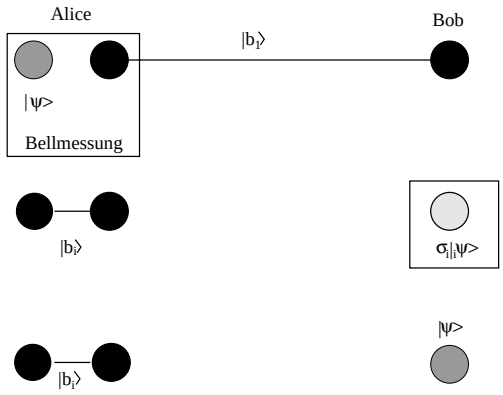

Abbildung 3.1: Teleportation

2. Um einen Zustand zu teleportieren, werden 2−Bit an Informationen ausgetauscht. Ein Zustand ist aber isomorph zu einer S^2−Sphäre. Man weiß aber, daß 2−Bit nicht vollständig eine S^2−Sphäre parametrisieren können. Wie ist dann diese “Information” übertragen worden?

3. Nach der Teleportation ist der verschränkte Zustand $|\psi\rangle$ zwischen Alice und Bob “vernichtet” oder besser gesagt “verbraucht” worden. Dies bedeutet, daß Verschränktheit eine verbrauchbare Ressource ist. Man kann also nicht mehr verschränkbare Zustände durch lokale Operationen und klassische Kommunikation als schon vorhanden erzeugen. Gäbe es ein Teleportationsprotokoll (und solch eines existiert nicht), welches dies bewerkstelligt, dann könnte man Verschränktheit wie folgt erzeugen:

   Alice erzeugt bei sich lokal ein zweites verschränktes Paar. Sie teleportiert nur eine Hälfte zu Bob. Nun besitzen beide zusätzlich zu dem schon bestehende einen neuen verschränkten Zustand. Beide haben also Verschränktheit erzeugt.

4. Der unbekannte Zustand $|\psi\rangle$, welcher zu Bob teleportiert wurde, wurde vernichtet und durch einen der Bellschen Zustände ersetzt. Dieser Sachverhalt ist verträglich mit dem **No-Cloning-Theorem** ([86], [87] und [88]). Das No-Cloning-Theorem besagt, daß man einen unbekannten Quantenzustand nicht klonen kann. Würde also auf Alices Seite der Zustand $|\psi\rangle$ erhalten bleiben, so würde dies dem No-Cloning-Theorem widersprechen (s. Abbildung 3.2).

Alle diese physikalischen Eigenschaften der Quanteninformationtheorie, wel-

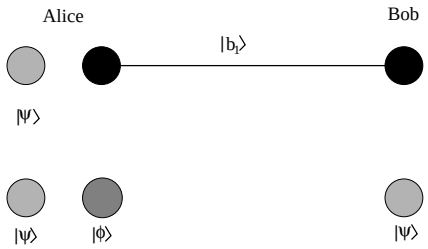

Abbildung 3.2: No-Cloning-Theorem

che sich in der Teleportation verbergen, führten zu einer mathematischen Beschreibung von Verschränktheit als Ressource.

Am Anfang dieses Abschnittes wurde darauf hingewiesen, daß die Teleportation auf elegante Art und Weise eine Alternative zum klassischen Transport von Quantenzuständen bietet. Dies setzt aber vorraus, daß die zwei Parteien schon im Besitz eines verschränkten Zustandes sind. Dieser verschränkte Zustand muß auf klassische Art und Weise ausgetauscht werden. Er kann natürlich ebenfalls verrauscht werden. Damit hätte man das Problem also nur verlagert. Dieses Problem läßt sich aber durch die Destillation beseitigen. Daher ist daß Verfahren der Destillation von enormer Wichtigkeit.

3.6 Destillation und Pseudodestillation von verschränkten Zuständen

Bevor das Phänomen der Pseudodestillierung erklärt werden kann, wird zuerst auf den Begriff der Destillation von verschränkten Zuständen eingegangen.

3.6.1 Destillation

Um Teleportation [30] oder Quantenkryptographie [23] zu betreiben, ist es manchmal zwingend notwendig, daß Alice und Bob im Besitz von maximal verschränkten Zuständen sind. Dies ist praktisch gesehen eine Idealvorstellung, welche in der Realität nicht zutreffend ist, weil sich das Quantensystem immer in Wechselwirkung mit seiner Umgebung befinden wird.

$$|\psi_{max}\rangle\langle\psi_{max}| \mapsto \sum_{\alpha,\beta} A_\alpha \otimes B_\beta |\psi_{max}\rangle\langle\psi_{max}| A_\alpha^\dagger \otimes B_\beta^\dagger =: \rho \qquad (3.17)$$

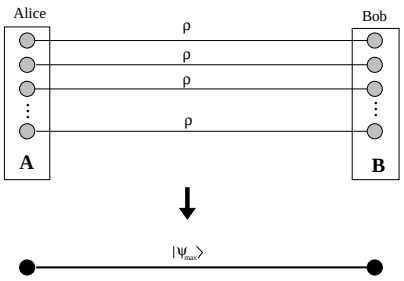

Abbildung 3.3: Destillation

Dieser Sachverhalt ist nicht nur für dieses Problem bekannt. Es ist ein Problem, mit dem sich auch die heutige moderne klassische Nachrichtentheorie konfrontiert sieht. In der Nachrichtentheorie wird das Problem durch Fehlerkorrekturcodes ([17], [18] und [19]) und Repeater [89] gelöst.

Dieses Konzept läßt sich auch in der Quanteninformationsverarbeitung verwenden, muß aber dementsprechend quantenmechanisch umgewandelt werden.

In unserem Fall wissen wir, welcher Zustand am Ende vorliegen soll. Bei den Fehlerkorrekturcodes aber kennt man den Zustand bei der Nachrichtenübertragung nicht. Würde man die Nachricht kennen, so bräuchte man sie ja auch nicht zu übertragen. Man ist also nur an der hohen Quantenkorrelation interessiert, den der maximal verschränkte Zustand mit sich bringt.

C. Benett und Mitarbeiter [32] entdeckten, daß man die Verschränkung erhöhen kann, wenn man mehrere Kopien des verschränkten Zustandes benutzt, um einen Zustand zu erhalten, welcher mehr Verschränktheit besitzt. Das Verfahren, welches dies bewerkstelligte, nennt man **Destillation**.

Darüber hinaus erhielt man mit der Destillation das Gefühl, daß Verschränktheit offensichtlich eine Ressource mit bestimmten Eigenschaften sein muß. Diese Eigenschaften werden später im Kapitel über Verschränktheitsmaße ausführlicher erläutert.

Wir fassen nun die Destillation mathematisch zusammen.

Definition 4 *Sei $|\psi\rangle$ ein maximal verschränkter Zustand. Existiert nun zu jedem $\varepsilon > 0$ eine natürliche Zahl $N(\varepsilon)$ und eine LQCC-Operation $D = A \otimes B : H_A^{\otimes N(\varepsilon)} \otimes H_B^{\otimes N(\varepsilon)} \mapsto H_A \otimes H_B$, so daß*

$$F \equiv 1 - \varepsilon = \frac{\langle\psi|D(\rho^{\otimes N(\varepsilon)})|\psi\rangle}{\mathrm{tr}(D(\rho^{\otimes N(\varepsilon)}))} \tag{3.18}$$

gilt, dann heißt ρ **destillierbar** *und das Verfahren, das dies bewerkstelligt* **Destillation**. *Desweiteren heißt D* **Destillierungsoperator**.

Nun stellt sich die Frage, welche Zustände destilliert werden können, bzw. was sind die notwendigen und hinreichenden Kriterien für eine Destillation? Die Horodecki Familie [31] konnte zeigen, daß in 2×2 und 2×3 Systemen jeder verschränkte Zustand zur Destillation ausgenutzt werden kann. Dieser Sachverhalt ermöglichte es, ein notwendiges und hinreichendes Kriterium zu formulieren.

Theorem 2 *Jeder verschränkte Zustand* ρ*, welcher einen Vektor* $|\psi\rangle$ *besitzt, so daß* $\langle\psi|\rho^{t_A\otimes N}|\psi\rangle < 0$ *erfüllt, wobei* $|\psi\rangle := \frac{1}{\sqrt{2}}(|\psi_1\rangle|\psi_2\rangle + |\phi_1\rangle|\phi_2\rangle)$ *für* $|\psi\rangle \in H_A \otimes H_B$*, ist destillierbar.*

Beweis: Als erstes zeigen wir, daß der Zustand ρ destillierbar sein muß, wenn die obige Bedingung gilt. Gegeben sei der Zustand $\rho^{\otimes N}$. Nun soll eine lokale Abbildung auf einen $C^2 \otimes C^2$-Unterraum $A \otimes B : (H_A \otimes H_B)^{\otimes N} \mapsto C^2 \otimes C^2$ existieren, so daß der Zustand $\tilde{\rho} \equiv A \otimes B \rho^{\otimes N} A^\dagger \otimes B^\dagger$ nach einer partiellen Transposition nicht mehr positiv definit ist. D.h. es existiert o.B.d.A. ein $\langle\phi| \equiv \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|) \in C^2 \otimes C^2$, so daß $\langle\phi|\tilde{\rho}^{t_A}|\phi\rangle < 0$. Die Nicht-Positivdefinitheit in $C^2 \otimes C^2$ ist aber für die Destillation eines maximal verschränkten Zustandes mit zwei Schmidt-Koeffizienten (Subsingulett) ausreichend. Sei p_s die Wahrscheinlichkeit für solch eine Destillation, dann ist die Wahrscheinlichkeit, D Subsinguletts zu erhalten, durch p^D gegeben. Aus diesen D Subsinguletts läßt sich wie folgt ein maximal verschränkter Zustand mit 2^D Schmidt-Koeffizienten konstruieren: $|\psi\rangle^{\otimes D}$ läßt sich auch schreiben als

$$\begin{aligned} |\psi\rangle^{\otimes D} &= \frac{1}{\sqrt{2^D}}(|00\ldots00\rangle_A|00\ldots00\rangle_B + |00\ldots01\rangle_A|00\ldots01\rangle_B \\ &+ |00\ldots10\rangle_A|00\ldots10\rangle_B + |00\ldots11\rangle_A|00\ldots11\rangle_B \\ &+ \ldots + |11\ldots11\rangle_A|11\ldots11\rangle_B). \end{aligned}$$

Nun können Alice und Bob folgende unitäre Operation durchführen

$$U := \sum_i^{2^D} |i\rangle\langle b_i|, \tag{3.19}$$

wobei b_i die binäre Darstellung von i ist. Für den Fall, daß N prim ist, wählt man D so, daß $N = 2^D - 1$ gilt und projeziert dann lokal auf die ersten N Basisvektoren. Auf diese Weise erhält man den gewünschten maximal verschränkten Zustand mit N Schmidtkoeffizienten.

Im Falle N nicht-prim ist die Gleichung $N = 2^D$ immer erfüllbar, so daß eine Projektion nicht notwendig ist. Bleibt noch die andere Richtung des Beweises zu zeigen!

Angenommen, wir destillieren einen maximal verschränkten Zustand mit N Schmidt-Koeffizienten, dann muß es aber auch zwangsläufig solch eine Projektion auf einen zweidimensionalen Unterraum geben, so daß der Zustand NPPT ist.$_{q.e.d.}$

Nun stellt sich aber die Frage, ob auch jeder höherdimensionale verschränkte Zustand destilliert werden kann? Diese Frage wurde wieder einmal von der Horodecki Familie negativ beantwortet. Die Horodeckis konnten nämlich zeigen, daß ein PPT verschränkter Zustand **nicht** durch eine zweidimensionale Projektion auf einen NPPT-Zustand projeziert werden kann, und er damit auch nicht destillierbar sein kann [90]. Verschränkte Zustände, welche nicht destillierbar sind, nennt man **gebunden verschränkt**!

Aber wie sieht es mit NPPT-Zuständen aus? Behält jeder NPPT-Zustand nach einer zweidimensionalen Projektion seine Eigenschaft NPPT zu sein? Man weiß, daß es NPPT-Zustände gibt, welche diese Eigenschaft mit nur einer Kopie **nicht** besitzen [91]. In der Arbeit von W. Dür, J.I. Cirac, M. Lewenstein und D. Bruss [91] wird diese Frage für eine endliche Anzahl von Kopien positiv beantwortet.

Wir sehen, daß man aufgrund des obigen Sachverhaltes Quantenzustände weiter unterteilen kann. Anfangs haben wir Zustände nach separablen und verschränkten Zuständen unterteilt. Diese Unterteilung war sinnvoll, weil sie eine gegebene physikalische Situation beschrieb. Separable Zustände konnte man nämlich allein durch lokale Operationen und klassische Kommunikation herstellen, was bei verschränkten Zuständen nicht machbar war. Jetzt haben wir eine weitere physikalische Situation.

Quantenzustände können unterteilt werden in **destillierbare** und **nicht destillierbare** Zustände. Die destillierbaren Zustände nennt man **frei verschränkt**, und die nicht destillierbaren Zustände sind entweder separabel oder gebunden verschränkt.

Aus dem Destillierungstheorem geht hervor wie man verschränkte Zustände am besten transportieren sollte, so daß man sie auch zur Destillation ausnutzen kann.

Angenommen, wir möchten einen verschränkten Zustand mit N Schmidtkoeffizienten zwischen Alice und Bob kreieren. Die erste Möglichkeit wäre, daß wir lokal einen verschränkten Zustand aus $N-$niveau atomaren Systemen erzeugen und diese dann durch den verrauschten Kanal (z.B. Atomwellenleiter) an Alice und Bob verschicken. Dann würde aber die Gefahr bestehen, daß durch das Rauschen

der Zustand begrenzt verschränkt wird. Dies hätte zur Folge, daß man den maximal verschränkten Zustand nicht mehr destillieren könnte.

Die zweite und durchaus bessere Methode ist es, statt ein atomares System durch den Kanal zu schicken, maximal verschränkte Photonenpaare zu erzeugen und diese dann durch den Kanal an Alice und Bob zu schicken. Photonen sind zweidimensionale Quantensysteme und sind deshalb aufgrund des Horodecki Theorems auch destillierbar, wenn sie verschränkt bei Alice und Bob ankommen. Man induziert dann die Verschränktheit schlicht und einfach nur auf die lokalen atomaren Systeme, wie schon im Beweis des Destiellierbarkeitstheorems geschildert wurde.

Mit anderen Worten: Es ist ökonomischer die Verschränktheit in viele kleine "Singulets" zu zerstückeln und später erst durch die Destillation zusammenzusetzen.

Zu guter letzt bleibt noch die Frage offen, wozu man die gebundene Verschränktheit überhaupt ausnutzen kann. Ist diese Verschränktheit irreversibel verloren? Diese Frage wird im nächsten Abschnitt ausführlicher behandelt.

3.6.2 Pseudodestillation

Im vorherigen Abschnitt wurde die Frage gestellt, wozu man begrenzt verschränkte Zustände ausnutzen kann? Die Horodeckis [34] waren in der Lage, zu zeigen, daß es möglich ist, ein Reservoir von gebunden verschränkten Zuständen so auszunutzen, daß man die Verschränktheit aus dem Reservoir in einen frei verschränkten Zustand überträgt. Auf diese Art und Weise gelang es ihnen, den frei verschränkten Zustand in einen maximal verschränkten Zustand umzuwandeln. Da man für diese Operation keine Verschränktheit von frei verschränkten Zuständen sondern gebunden verschränkte Verschränktheit benutzt, nannten sie dieses Verfahren **Pseudodestillation**. Die Pseudodestillierung läßt sich nun wie folgt definieren:

Definition 5 *Gegeben sei ein Reservoir aus gebunden verschränkten Zuständen* $\rho_b^{\otimes N}$*, und ein frei verschränkter Zustand* ρ_f*. Existiert nun eine LQCC-Operation D und eine Natürliche Zahl* N_0*, so daß der Ausdruck*

$$F(N) = \frac{\langle \psi_{\max} | D(\rho_f \otimes \rho_b^{\otimes N}) | \psi_{\max} \rangle}{\mathrm{tr}(D(\rho_f \otimes \rho_b^{\otimes N}))}, \tag{3.20}$$

für alle $N \geq N_0$ 1 *beliebig nahe gegen 1 konvergiert, nennt man D* **Pseudodestillierung**.

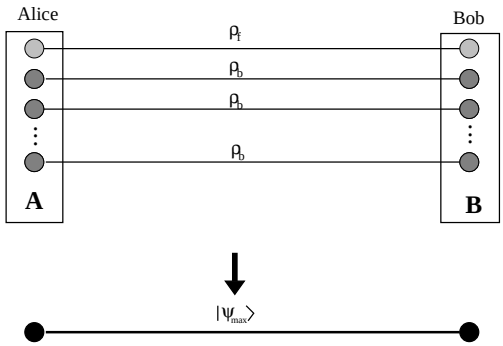

Abbildung 3.4: Pseudodestillation. Die gebundene Verschränktheit wird in den frei Verschränkten Zustand transformiert.

Die Frage, die sich stellt, ist nun, unter welchen Umständenob kann man pseudodestillieren. Hinreichende Kriterien sind für die Fragestellung bis heute noch unbekannt.

Ein weiteres interessantes Phänomen für die praktische Anwendung ist die Nutzung von verschränkten Zuständen als eine Art Katalysator. Dieses Phänomen tritt bei der Konvertierung von einem quantenmechanischen Zustand in einen anderen auf und ist aus der Sicht der Verschränktheitsmanipulation in der Quanteninformationsverarbeitung von enormer Bedeutung.

3.7 Der verschränkte Zustand als Katalysator

Seien ρ und σ Zustände in einem Hilbertraum $H = H_A \otimes H_B$. Man möchte nun allein durch lokale Operationen und klassische Kommunikation den Zustand σ nach ρ konvertieren. Für reine Zustände gibt es das Majorisierungskriterium [93], welches notwendig und hinreichend für die Konvertierung ist, und durch die folgende Ungleichung gegeben ist:

$$\sum_{i=1}^{k} \alpha_i \leq \sum_{i=1}^{k} \beta_i \quad \forall k = 1, \ldots, N-1, \tag{3.21}$$

wobei $N = \dim[H_A] = \dim[H_B]$ und $\{\alpha_i\}, \{\beta_i\}$ die Eigenwerte von $\mathrm{tr}_A[\sigma]$ und $\mathrm{tr}_A[\rho]$ sind.

Es konnte gezeigt werden, daß es für reine Zustände [35], welche das Majorisierungskriterium nicht erfüllen, einen weiteren verschränkten Zustand ω geben

kann, welcher sozusagen als Katalysator fungieren kann und somit die Konvertierung trotzdem ermöglicht:

$$\sigma \otimes \omega \rightarrow \rho \otimes \omega. \tag{3.22}$$

Bei solchen Katalyseprozessen bleibt der katalytische Zustand erhalten. Er ermöglicht also nur die Konvertierung und wird deshalb auch Katalysator genannt. Desweitern gibt es zur Zeit Untersuchungen, die sich mit der Katalyse von gemischten Zuständen und deren Zusammenhang mit der Purifikation/Destillation [36] auseinandersetzen. Dies ist wichtig, weil man deren physikalischen Zusammenhang verstehen möchte.

Im Verlauf dieser Arbeit haben wir bei Begriffen wie Teleportation, Destillation, Pseudo-Destillation, Katalyse und maximaler Verschränktheit den Eindruck gewonnen, daß es sich beim Begriff Verschränktheit um eine neue Art von physikalischer Ressource [94] handelt (wie bei Energie oder Entropie). Dies muß natürlich in einenem sauberen physikalisch/mathematischen Rahmen beschrieben werden [95]. Der nächste Abschnitt beschäftigt sich mit dem Begriff der Quantifizierung von Verschränktheit in Form des Verschränktheitsmaßes.

3.8 Verschränktheitsmaße

In den nächsten zwei Unterabschnitten dieses Kapitels wird auf die mathematische Formulierung der Verschränktheit und auf Beispiele von verschiedenen Verschränktheitsmaßen eingegangen. Diese Formulierungen stützen sich auf die verschiedenen physikalischen Eigenschaften, die in den letzten Abschnitten erläutert wurden.

3.8.1 Quantifizierung von Verschränktheitsmaßen

Es werden nun die physikalischen Eigenschaften eines Verschränktheitsmaßes aufgezählt und kommentiert [95]:

(I) $E(\rho) = 0$**, falls** ρ **ein separabler Zustand ist**

Die erste Bedingung besagt, daß jeder separable Zustand das Verschränktheitsmaß Null haben sollte, weil er nicht verschränkt ist. Bei einer Klassifizierung von Zuständen nach separabel und verschränkt ist dies auch plausibel.

(II) $E(\rho) = E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$

Die zweite Bedingung fordert, daß das Verschränktheitsmaß nicht abhängig davon sein sollte, was für Basen man lokal verwendet.

(III) Sei $\sum_\alpha A_\alpha A_\alpha^\dagger \otimes B_\alpha B_\alpha^\dagger = 1$. Dann folgt für das Verschränktheitsmaß

$$\sum_\alpha \mathrm{tr}(A_\alpha \otimes B_\alpha \rho A_\alpha^\dagger \otimes B_\alpha^\dagger) E\left(\frac{A_\alpha \otimes B_\alpha \rho A_\alpha^\dagger \otimes B_\alpha^\dagger}{\mathrm{tr}(A_\alpha \otimes B_\alpha \rho A_\alpha^\dagger \otimes B_\alpha^\dagger)}\right) \leq E(\rho) \tag{3.23}$$

Diese Bedingung garantiert daß im Mittelwert die verschränktheit nicht erhöht werden kann. Dadurch ist sichergestellt daß mann nicht mehr Verschränktheit erzeugen kann als schon vorher vorhanden ist. Diese Bedingung macht die Verschränktheit erst zu einer Ressoource.

(IV) $E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2)$

Die vierte Bedingung besagt, daß Verschränktheit eine additive Größe sein sollte. Diese Bedingung ist ziemlich umstritten, weil es Verschränktheitsmaße, wie z.b. **Robustheit** ([96]und[97]) aber auch daß relative Entropiemaß gibt, die diese Bedingung nicht erfüllen (R. I. Werner und K. G. H. Vollbrecht [98]). Trotzdem aber besitzen sie eine physikalische Interpretation.

Mehr oder weniger sieht man die ersten drei Bedingungen als vernünftige Eigenschaften von Verschränktheitsmaßen an.

3.8.2 Verschiedene Verschränktheitsmaße

In diesem Abschnitt zählen wir die bekanntesten und wichtigsten Verschränktheitsmaße auf.

1. Das Formationsmaß: $E(\rho) \equiv \min(\sum_\alpha p_\alpha S(\rho_A^\alpha))$. $S(\rho_A) = -\mathrm{tr}\rho_A \ln \rho_A$ ist die Von-Neumannsche-Entropie, und das Minimum ist über alle möglichen Realisierungen des Zustandes, $\rho = \sum_\alpha p_\alpha |\psi_\alpha\rangle\langle\psi_\alpha|$ mit $\rho_A^\alpha = \mathrm{tr}(|\psi_\alpha\rangle\langle\psi_\alpha|)$ zu nehmen. Die physikalische Bedeutung dieses Maßes ist die Anzahl der maximal verschränkten Zustände, die gebraucht werden, um den Zustand ρ mit lokalen Operationen zu kreieren. Deshalb auch der Name Formationsmaß [94].

2. Relatives Entropiemaß: $E(\rho) = \min_{\sigma \in S} D(\rho||\sigma)$. Hierbei wird das Minimum über alle separablen Zustände σ genommen, wobei $D(\rho||\sigma) := \mathrm{tr}(\rho \ln \rho - \rho \ln \sigma)$ die relative Enropie ist [95].

3. Destillationsmaß für einen reinen Zustand $|\psi\rangle$: Dieses Maß definiert wie viele maximal verschränkte Zustände man aus $|\psi\rangle^{\otimes N}$ für $N \to \infty$ destilieren kann. Dies ist durch $D(\psi) = \mathrm{tr}_B(|\psi\rangle\langle\psi|)$ gegeben. Das Destilationsmaß ist also nichts weiter als die Wahrscheinlichkeit für eine erfolgreiche Destillation am Zustand $|\psi\rangle$. Eine Verallgemeinerung für gemischte Zustände wurde in der Letzten Zeit von der Horodecki Familie [99] untersucht.

4. Das BSA Verschränktheitsmaß: $(1 - \Lambda_{BSA}(\rho))$. Dieses wird in einem separaten Kapitel ausführlicher behandelt.

Kapitel 4

Die beste separable Approximation (BSA)

4.1 Inhalt dieses Kapitels

Um eine vollständige Charakterisierung von verschränkten Zuständen zu ermöglichen, muß man so viel wie möglich über die geometrische und topologische Struktur der konvexen Menge aller separablen Zustände in Erfahrung bringen. In diesem Kapitel wird ein Theorem vorgestellt, welches uns einen tieferen Einblick in die Struktur von verschränkten Zuständen liefert, sowie einen konstruktiven Algorithmus, der unter dem Namen **„Die Beste separable Approximation“** oder auch **„BSA“** bekannt ist. Dieser ermöglicht es, einen gegebenen quantenmechanischen Zustand auf Separabilität zu prüfen. Das BSA-Theorem wurde ursprünglich von M. Lewenstein und A. Sanpera entwickelt [1] und ist für die vorliegende Arbeit von grundlegender Bedeutung. Aus diesem Grund wird das BSA-Theorem besonders ausführlich beschrieben. Kapitel 4.3 und 4.4 hingegen beinhalten neuere Untersuchungen zu dieser Thematik. Weitere wichtige Beiträge zum Thema BSA lieferten in letzterer Zeit B. G. Englert und N. Metwally ([100] und [101]).

4.2 Die Lewenstein-Sanpera beste separable Approximation (BSA)

Die zentrale Idee dieses Theorems basiert auf der Tatsache, daß die Menge der separablen Matrizen eine konvexe und kompakte Menge bildet. Aus diesem Grund

existiert zu jeder Dichtematrix ρ eine maximale separable Dichtematrix ρ_s^*, welche die Eigenschaft besitzt, daß $\rho - \rho_s^* \geq 0$ und $tr\rho_s^*$ maximal ist. Diese Idee läßt sich wie folgt als ein Theorem formulieren:

Theorem 3 : *Für jede Dichtematrix ρ und für jede Menge V von Produktvektoren, welche im Bild von ρ liegen, also $|e_\alpha, f_\alpha\rangle \in R(\rho)$, existiert eine separable (hier nicht normierte) Matrix*

$$\rho_s^*[V] = \sum_\alpha \Lambda_\alpha |e_\alpha, f_\alpha\rangle\langle e_\alpha, f_\alpha| \tag{4.1}$$

mit $\Lambda_\alpha \geq 0$, so daß $\delta\rho[V] = \rho - \rho_s^*[V] \geq 0$ und ρ_s^* die beste separable Approximation (BSA) in dem Sinne darstellt, daß $\mathrm{tr}(\rho_s^*[V])$ maximal ist.

Beweis: Wir betrachten nun alle separablen Dichtematrizen ρ_s der Form (4.1), welche nach einer Subtraktion von ρ eine nicht negative Differenz $\delta\rho[V]$ hinterlassen. Daraus folgt, daß $\rho_s[V]$ eine Spur besitzen muß, welche kleiner ist als Eins, da $0 \leq \mathrm{tr}(\delta\rho[V]) = 1 - \mathrm{tr}(\rho_s[V])$ ist. Die Menge solcher Dichtematrizen wird durch die Menge aller $\Lambda_\alpha \geq 0$ beschrieben, für welche $\delta\rho[V] \geq 0$ und $0 \leq \mathrm{tr}(\rho_s[V]) = \sum_\alpha \Lambda_\alpha \leq 1$ gilt. Die Menge solcher Λ's bildet eine kompakte Menge, und der Wertebereich der Spur ist beschränkt. Deshalb existiert auch ein Maximum. Dieses Maximum hängt natürlich von der Wahl der Menge V ab. Durch die Vergrößerung dieser Menge gelangt man auch zu einer größeren Spur. Dies kann man so lange fortsetzen, bis das universelle Maximum endgültig erreicht ist.$_{q.e.d.}$

Aus dem obigen Theorem folgt automatisch die folgende Bedingung für Separabilität:

Bedingung: Eine Dichtematrix ρ ist separabel, falls eine Menge V von Produktvektoren existieren, für welche die BSA $\rho_s^*[V]$ die Spur Eins besitzt.

Um den konstruktiven Algorithmus für die BSA vorzustellen, müssen noch einige neue Konzepte eingeführt werden.

Definition 6 : *Ein nicht negativer Parameter Λ heißt* **maximal** *in Bezug auf eine (im Allgemeinen nicht normierte) Dichtematrix ρ und einen Projektor $P = |\psi\rangle\langle\psi|$, falls $\rho - \Lambda P \geq 0$ und die Matrix $\rho - (\Lambda + \varepsilon)P$ für alle $\varepsilon \geq 0$ nicht positiv definit ist*
.

Dies bedeutet, daß Λ die maximale Kontribution von P darstellt, die man von ρ abzuziehen imstande ist. Das folgende Lemma charakterisiert dieses Λ.

Lemma 3 : *Λ ist in Bezug auf ρ und einen Projektor $P = |\psi\rangle\langle\psi|$ genau dann maximal, wenn gilt:*

1. *Falls $|\psi\rangle \notin R(\rho)$, dann ist $\Lambda = 0$.*
2. *Falls $|\psi\rangle \in R(\rho)$, dann ist*

$$0 \leq \Lambda = \frac{1}{\langle\psi|\rho^{-1}|\psi\rangle}. \tag{4.2}$$

Beweis: Der Beweis von (1) ist trivial. Da nun $|\psi\rangle \in R(\rho)$ liegt, bedeutet dies, daß ein $|\phi\rangle$ existiert, so daß $|\psi\rangle = \rho|\phi\rangle$ gilt. Nun haben wir für jedes $|\phi\rangle$ die Schwarzsche Ungleichung

$$\begin{aligned}\langle\phi|P|\phi\rangle &= |\langle\phi|\sqrt{\rho}\frac{1}{\sqrt{\rho}}|\psi\rangle|^2 \\ &\leq \langle\phi|\rho|\phi\rangle\langle\psi|\frac{1}{\rho}|\psi\rangle.\end{aligned}$$

Dies beweist, daß für alle $|\phi\rangle$,$\langle\phi|\rho - (\langle\psi|\frac{1}{\rho}|\psi\rangle)^{-1}P|\phi\rangle \geq 0$ ist. Für $|\phi\rangle = \frac{1}{\rho}|\psi\rangle$ erhält man, daß $(\rho - \Lambda P)|\phi\rangle = 0$ ist, wobei Λ durch (4.2) gegeben ist, und damit für alle $\varepsilon \geq 0$,$\langle\phi|(\rho - (\Lambda + \varepsilon)P)|\phi\rangle = -\varepsilon\Lambda^{-2} < 0$. Dies beweist die durch (4.2) gegebene Maximalität von Λ.$_{q.e.d.}$

Es folgt nun der Begriff der paarweisen Maximalität:

Definition 7 : *Ein Paar von nicht negativen Parametern (Λ_1, Λ_2) nennt man in Bezug auf ρ und ein Paar von Projektionsoperatoren $P_1 = |\psi_1\rangle\langle\psi_1|, P_2 = |\psi_2\rangle\langle\psi_2|$* **maximal**,

1. *falls $\rho - \Lambda_1 P_1 - \Lambda_2 P_2 \geq 0$,$\Lambda_1$ in Bezug auf $\rho - \Lambda_2 P_2$ und zum Projektor P_1 maximal ist,*
2. *falls Λ_2 in Bezug auf $\rho - \Lambda_1 P_1$ und zum Projektor P_2 maximal ist,*
3. *sowie die Summe $\Lambda_1 + \Lambda_2$ auch maximal ist.*

Gezeigt wird, daß es ausreicht, die Projektoren paarweise zu maximieren, um die BSA zu erhalten. Dafür wird folgendes Lemma benötigt.

Lemma 4 : *Ein Paar (Λ_1, Λ_2) ist genau dann in Bezug auf ρ und ein Paar von Projektoren (P_1, P_2) maximal, wenn:*

1. *Falls* $|\psi_1\rangle$,$|\psi_2\rangle \notin R(\rho)$, *dann ist* $\Lambda_1 = \Lambda_2 = 0$;

2. *Falls* $|\psi_1\rangle \notin R(\rho)$ *und* $|\psi_2\rangle \in R(\rho)$, *dann ist* $\Lambda_1 = 0$ *und* $\Lambda_2 = \frac{1}{\langle\psi_2|\rho^{-1}|\psi_2\rangle}$, *und falls* $|\psi_2\rangle \notin R(\rho)$ *und* $|\psi_1\rangle \in R(\rho)$, *dann ist* $\Lambda_2 = 0$ *und* $\Lambda_1 = \frac{1}{\langle\psi_1|\rho^{-1}|\psi_1\rangle}$;

3. *Falls* $|\psi_1\rangle, |\psi_2\rangle \in R(\rho)$ *und* $\langle\psi_1|\frac{1}{\rho}|\psi_2\rangle = 0$, *dann ist* $\Lambda_i = \langle\psi_i|\rho^{-1}|\psi_i\rangle$, $i = 1,2$;

4. *Falls* $|\psi_1\rangle$, $|\psi_2\rangle \in R(\rho)$ *und* $\langle\psi_1|\rho^{-1}|\psi_1\rangle, \langle\psi_2|\rho^{-1}|\psi_2\rangle \geq |\langle\psi_1|\rho^{-1}|\psi_2\rangle| \neq 0$, *dann ist*

$$\Lambda_1 = (\langle\psi_2|\rho^{-1}|\psi_2\rangle - |\langle\psi_1|\rho^{-1}|\psi_2\rangle|)/D \tag{4.3}$$
$$\Lambda_2 = (\langle\psi_1|\rho^{-1}|\psi_1\rangle - |\langle\psi_2|\rho^{-1}|\psi_1\rangle|)/D, \tag{4.4}$$

   wobei $D = \langle\psi_1|\rho^{-1}|\psi_1\rangle\langle\psi_2|\rho^{-1}|\psi_2\rangle - |\langle\psi_1|\rho^{-1}|\psi_2\rangle|^2$;

5. *Falls* $|\psi_1\rangle$,$|\psi_2\rangle \in R(\rho)$ *und* $\langle\psi_1|\rho^{-1}|\psi_1\rangle \geq |\langle\psi_1|\rho^{-1}|\psi_2\rangle|\langle\psi_2|\rho^{-1}|\psi_2\rangle$, *dann ist* $\Lambda_1 = \langle\psi_1|\rho^{-1}|\psi_1\rangle^{-1}$ *und* $\Lambda_2 = 0$.

Man beachte, daß die Schwarzsche Ungleichung $D \geq 0$ *impliziert.*

Beweis: Der Beweis von (1) und (2) ist identisch zu dem von Lemma 3. Für den Fall (3) gilt, daß $(\rho - \Lambda_1 P_1)^{-1}|\psi_2\rangle = \rho^{-1}|\psi_2\rangle$ und $(\rho - \Lambda_2 P_2)^{-1}|\psi_1\rangle = \rho^{-1}|\psi_1\rangle$, so daß aus der Maximalität von Λ_i automatisch $\Lambda_i = \langle\psi_i|\rho|\psi_i\rangle$,$i = 1,2$ folgt. Der letzte Fall ist der interessanteste von allen. Die Maximalität von Λ_1 und Λ_2 führt zur folgenden eindimensionalen Mannigfaltigkeit (Kapitel 2.2):

$$1 - \Lambda_1\langle\psi_1|\rho^{-1}|\psi_1\rangle - \Lambda_2\langle\psi_2|\rho^{-1}|\psi_2\rangle + \Lambda_1\Lambda_2 D = 0, \tag{4.5}$$

wobei $D = \langle\psi_1|\rho^{-1}|\psi_1\rangle\langle\psi_2|\rho^{-1}|\psi_2\rangle - |\langle\psi_1|\rho^{-1}|\psi_2\rangle|^2$ ist. Nun muß $\Lambda_1 + \Lambda_2$ auf dieser Mannigfaltigkeit maximiert werden. Dies liefern die im Lemma genannten Bedingungen.$_{q.e.d.}$

Es folgt nun das zentrale BSA-Theorem:

Theorem 4 : *Gegeben sei eine Menge V von Produktvektoren* $|e_\alpha, f_\alpha\rangle \in V \subset R(\rho)$. *Die Matrix* $\rho_s^*[V] = \sum_\alpha \Lambda_\alpha |e_\alpha, f_\alpha\rangle\langle e_\alpha, f_\alpha|$ *ist genau dann eine BSA,*

1. *Falls alle* Λ_α *in Bezug auf*
   $\rho_\alpha[V] = \rho - \sum_{\alpha' \neq \alpha} \Lambda_{\alpha'} |e_{\alpha'}, f_{\alpha'}\rangle\langle e_{\alpha'}, f_{\alpha'}|$ *maximal sind;*

2. *Falls alle Paare* $(\Lambda_\alpha, \Lambda_\beta)$ *in Bezug auf* $\rho_{\alpha\beta}[V] = \rho - \sum_{\alpha' \neq \alpha,\beta} \Lambda_{\alpha'} |e_{\alpha'}, f_{\alpha'}\rangle\langle e_{\alpha'}, f_{\alpha'}|$ *maximal sind.*

Beweis: Sei ρ_s^* eine BSA. Dann muß diese auch in allen Λ_α sowie auch in allen Paaren $(\Lambda_\alpha, \Lambda_\beta)$ maximal sein, weil man ansonsten den BSA-Parameter durch $\Lambda_\alpha + \Lambda_\beta$ erhöhen könnte.

Der Beweis in der umgekehrten Richtung ist schon etwas komplizierter. Als erstes nehme man an, daß die Anzahl der α's K sei. ρ_s^* sei die Matrix, die man durch Maximierung der Λ_α's und der paarweisen Maximierung der $(\Lambda_\alpha, \Lambda_\beta)$ erhalten hat. Nun betrachtet man eine Matrix $\rho = \sum_\alpha \lambda_\alpha P_\alpha$ in der Nähe von ρ_s^*, für welche alle λ_α's maximal sind. Dies bedeutet, daß sich ρ_s am Rand $F(\lambda_1, \ldots \lambda_K) = 0$ einer Menge Z befindet, wobei Z die Menge aller separablen Dichtematrizen ist, welche $\rho - \rho_s \geq 0$ erfüllen. Die λ_α's liegen also auf der $(K-1)$-dimensionalen Mannigfaltigkeit, welche durch die algebraische Gleichung (siehe (4.2)) $F(\lambda_1, \ldots \lambda_K) = 0$ gegeben ist. Die Maximalität von $(\Lambda_\alpha, \Lambda_\beta)$ impliziert, daß $(\lambda_\alpha + \lambda_\beta)$ ein Maximum bei $\lambda_{\alpha\beta} = \Lambda_{\alpha\beta}$ zur Zwangsbedingung $F = 0$ und für $\lambda_\gamma = \Lambda_\gamma, \gamma \neq \alpha\beta$ besitzt. Daraus folgt, daß $\frac{\partial F}{\partial \lambda_\alpha}|_{\lambda=\Lambda} = \frac{\partial F}{\partial \lambda_\beta}|_{\lambda=\Lambda}$ ist, was bedeutet, daß $\frac{\partial F}{\partial \lambda_\alpha}|_{\lambda=\Lambda} = \text{const}$ für alle α ist. Dies ist äquivalent zur Aussage, daß der Gradient von $\text{tr}(\rho_s)$ unter der Zwangsbedingung $F = 0$ verschwindet. Es muß sich um eine Extremalstelle handeln. Dabei kann es sich nicht um ein lokales Minimum oder einen Sattelpunkt handeln, da die Spur in Bezug auf alle λ_α's maximal und Z dabei noch konvex ist. Aus dem Grund der Konvexität muß dieses lokale Maximum auch ein Globales sein. Wäre dem nicht so, dann gäbe es ein anderes Maximum. Dies wäre die BSA ρ_s^*.

Nimmt man nun die Spur der konvexen Kombination von ρ_s und ρ_s^*, erhielte man $\varepsilon\text{tr}(\rho_s) + (1-\varepsilon)\text{tr}(\rho_s^*)$. Dann müßte aber für alle ε diese Spur größer sein als $\text{tr}(\rho_s)$, was wiederum bedeutet, daß dies kein lokales Maximum sein kann. *q.e.d.*

Die gesamte Information über die Verschränktheit des Zustandes ρ ist nun im BSA-Rest $\delta\rho$ enthalten. Der Bildbereich $R(\delta\rho)$ enthält wegen der BSA keine Produktvektoren, die man abziehen könnte. Ansonsten könnte man durch das Abziehen die BSA erhöhen. Dies ist aber laut Vorraussetzung nicht möglich, da die BSA schon vorliegt. Der Bildbereich der Matrix $\delta\rho$ muß deswegen kleiner oder gleich $(M-1)(N-1)$ sein. Das folgt aus der Tatsache, daß die Menge der Produktvektoren in einem $C^M \otimes C^N$-Raum eine $(M+N-1)$-dimensionale Mannigfaltigkeit aufspannen. Dieser besitzt immer einen Schnitt mit einem linearen Unterraum H, wenn dieser eine Dimension besitzt, welche größer oder gleich $(N-1)\times(M-1)$ ist. In Kapitel 7 wird dies ausführlicher bewiesen.

Interessant ist nun der 2-q-Bit Fall ($M = N = 2$). In diesem Fall ist nämlich der BSA-Rest $\delta\rho$ ein einziger Projektor auf einem verschränkten Zustand. Außerdem muß dieser Projektor eindeutig sein. Gäbe es eine weitere BSA-Zerlegung mit einem anderen Projektor als BSA-Rest, so könnte man die folgende konvexe

Kombination dieser beiden BSA-Zerlegungen nehmen:

$$\begin{aligned}\rho &= \lambda\frac{(\rho_s+\tilde{\rho}_s)}{2}+(1-\lambda)\frac{(P_e+\tilde{P}_e)}{2}\\ &= \lambda\bar{\rho}_s+(1-\lambda)\delta\rho\end{aligned}$$

Nun ist $\delta\rho$ aber ein BSA-Rest mit Rang zwei. Dies würde aber wiederum bedeuten, daß man einen Produktvektor findet [102], welchen man abziehen könnte, um damit die BSA zu erhöhen. Dies ist aber nicht möglich, da man schon eine BSA hat. Folglich gibt es nur einen Projektor als BSA-Rest. Diese einfache Struktur erlaubt es, die BSA-Zerlegungen etwas genauer für $2-$qbit-Systeme zu untersuchen [100]. Dies geschieht im Kapitel 5, in dem BSA-Zerlegungen von $2-$qbit-Systemen untersucht werden, welche maximalen Rang ($r(\rho)=4$) und einen maximal verschränkten Projektor als einen BSA-Rest besitzen. Solche Zustände sind deshalb besonders interessant, weil sie den Werner-Zuständen [69] ähneln.

In Kapitel 4.3 wird noch ausführlicher auf das Thema der Eindeutigkeit des BSA-Restes eingegangen. Doch bevor dies geschieht, wird auf die differentialgeometrische Struktur der separablen Matrizen ρ_s eingegangen, welche die Eigenschaft $\rho-\rho_s\geq 0$ besitzen.

4.3 Die BSA-Mannigfaltigkeit

In diesem Abschnitt wird die Struktur des Randes der konvexen Menge Z behandelt, d.h. der Menge aller separablen Zustände $\rho_s=\sum_\alpha \Lambda_\alpha P_\alpha$, welche bezüglich ρ die Eigenschaft besitzt, daß $\rho-\rho_s\geq 0$ ist.

Theorem 5 : *Die Oberfläche von Z wird durch die folgende Mannigfaltigkeit beschrieben:*

$$\begin{aligned}&1 \quad -\sum_i^n \Lambda_i D_i+\sum_{i<j}^n \Lambda_i\Lambda_j D_{ij}-\sum_{i<j<k}^n \Lambda_i\Lambda_j\Lambda_k D_{ijk}+\ldots\\ &+ \quad (-1)^m \sum_{i_1<i_2<\ldots<i_m} \Lambda_{i_1}\Lambda_{i_2}\ldots\Lambda_{i_m}D_{i_1 i_2\ldots i_m}+\ldots\\ \ldots \quad &+ \quad (-1)^n\Lambda_1\Lambda_2\ldots\Lambda_n D_{12\ldots n}=0,\end{aligned}$$

wobei die Menge $\{D_{i_1 i_2\ldots i_m}\}$ *durch die Subdeterminanten der Matrix*

$$D=\begin{pmatrix}\langle\psi_1|\rho^{-1}|\psi_1\rangle & \langle\psi_1|\rho^{-1}|\psi_2\rangle & \ldots & \langle\psi_1|\rho^{-1}|\psi_n\rangle\\ \langle\psi_2|\rho^{-1}|\psi_1\rangle & \langle\psi_2|\rho^{-1}|\psi_2\rangle & \ldots & \langle\psi_2|\rho^{-1}|\psi_n\rangle\\ \vdots & \vdots & \ddots & \vdots\\ \langle\psi_n|\rho^{-1}|\psi_1\rangle & \langle\psi_n|\rho^{-1}|\psi_2\rangle & \ldots & \langle\psi_n|\rho^{-1}|\psi_n\rangle\end{pmatrix}$$

beschrieben wird. Die Menge $\{|\psi_i\rangle\}$ ist die Menge der Produktvektoren, aus denen die P_i's zusammengesetzt sind.

Beweis: Der Beweis wird über die vollständige Induktion geführt. Es wird als erstes gezeigt, daß die Mannigfaltigkeit für $n = 2$ beschrieben wird durch:

$$1 - \Lambda_1 D_1 - \Lambda_2 D_2 + \Lambda_1 \Lambda_2 D_{12} = 0. \tag{4.6}$$

Es sei $(\rho - \Lambda_1 P_1)^{-1}|\psi_2\rangle = |\phi_2\rangle$, bzw. $|\psi_2\rangle = (\rho - \Lambda_1 P_1)|\phi_2\rangle$. Nun macht man den Ansatz $|\phi_2\rangle = \rho^{-1}(A|\psi_1\rangle + B|\psi_2\rangle)$ und erhält $|\psi_2\rangle = (\rho - \Lambda_1 P_1)(A\rho^{-1}|\psi_1\rangle + B\rho^{-1}|\psi_2\rangle)$. Dies determiniert die reellen Koeffizienten A und B zu $A = \frac{\Lambda_1\langle\psi_1|\rho^{-1}|\psi_2\rangle}{1-\Lambda_1\langle\psi_1|\rho^{-1}|\psi_1\rangle}$ und $B = 1$.

Nun gilt

$$\begin{aligned}
\langle\psi_2|(\rho - \Lambda_1 P_1)^{-1}|\psi_2\rangle &= \frac{\Lambda_1|\langle\psi_1|\rho^{-1}|\psi_2\rangle|^2}{1 - \langle\psi_1|\rho^{-1}|\psi_1\rangle} + \langle\psi_2|\rho^{-1}|\psi_2\rangle \\
\Lambda_2 &= \frac{\Lambda_1[|\langle\psi_1|\rho^{-1}|\psi_2\rangle|^2 - \langle\psi_1|\rho^{-1}|\psi_1\rangle\langle\psi_2|\rho^{-1}|\psi_2\rangle]}{1 - \langle\psi_1|\rho^{-1}|\psi_1\rangle}.
\end{aligned}$$

Daraus ergibt sich dann $1 - \Lambda_1 D_1 - \Lambda_2 D_2 + \Lambda_1 \Lambda_2 D_{12} = 0$.

Nun nehme man an, daß die Induktionsannahme auch für n gilt. Ersetzt man nun $\rho^{-1} \to (\rho - \Lambda_{n+1}|\psi_{n+1}\rangle\langle\psi_{n+1}|)^{-1}$ und definiert wieder den folgenden Ansatz

$$\begin{aligned}
(\rho - \Lambda_{n+1}|\psi_{n+1}\rangle\langle\psi_{n+1}|)^{-1}|\psi_i\rangle &= \rho^{-1}|\psi_i\rangle \\
&+ \frac{\Lambda_{n+1}\langle\psi_{n+1}|\rho^{-1}|\psi_i\rangle}{1 - \Lambda_{n+1}\langle\psi_{n+1}|\rho^{-1}|\psi_{n+1}\rangle}\rho^{-1}|\psi_{n+1}\rangle,
\end{aligned}$$

den man in den Ausdruck für die Mannigfaltigkeit mit n Koeffizienten einsetzt, so erhält man nach einigen algebraischen Umformungen den folgenden Ausdruck:

$$\begin{aligned}
1 \quad & - \sum_i^n \Lambda_i D_i + \sum_{i<j}^n \Lambda_i \Lambda_j D_{ij} - \sum_{i<j<k}^n \Lambda_i \Lambda_j \Lambda_k D_{ijk} + \ldots + \\
+ \quad & (-1)^m \sum_{i_1<i_2<\ldots<i_m} \Lambda_{i_1}\Lambda_{i_2}\ldots\Lambda_{i_m} D_{i_1 i_2 \ldots i_m} + \ldots \\
+ \quad & (-1)^n \sum_{i_1<i_2<\ldots<i_n} \Lambda_{i_1}\Lambda_{i_2}\ldots\Lambda_{i_n} D_{i_1 i_2 \ldots i_n} + \\
+ \quad & (-1)^{n+1} \Lambda_1 \Lambda_2 \ldots \Lambda_{n+1} D_{12\ldots n+1} = 0.
\end{aligned}$$

Dies beweist den Fall für $n + 1$ und somit wäre der Induktionsbeweis abgeschlossen.$_{q.e.d.}$

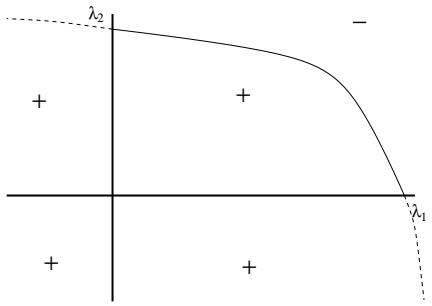

Abbildung 4.1: Die BSA-Mannigfaltigkeit für zwei Parameter

Man beachte, daß die BSA-Mannigfaltigkeit aus Polynomen zusammengesetzt ist, welche linear in Bezug auf jede einzelne Variable Λ_i ist. Dies bedeutet, daß man ohne weiteres nach jeder Variable explizit auflösen kann.

Desweiteren definiert die BSA-Mannigfaltigkeit ein konvexes Gebiet aller Λ's, welche nicht alle unbedingt positiv sein müssen und die die Eigenschaft besitzen, daß $\rho - \Lambda \sum_{\alpha=1}^{n} \Lambda_\alpha P_\alpha$ ein positiver Operator ist. Dies ist in Abb. 4.1 für zwei Parameter veranschaulicht. Befindet sich nun ein Teil einer Hyperebene auf der BSA-Mannigfaltigkeit, so muß auch die gesamte Hyperebene auf der BSA-Mannigfaltigkeit enthalten sein. Dies folgt aus der Tatsache, daß die BSA-Mannigfaltigkeit aus endlichen Polynomen zusammengesetzt ist. Dieser Sachverhalt ist im darauffolgenden Beweis der Eindeutigkeit einer BSA-Zerlegung von tragender Bedeutung.

4.4 Die Eindeutigkeit der BSA

Theorem 6 (Die Eindeutigkeit der BSA): *Jede Dichtematrix* ρ *hat eine eindeutige Zerlegung* $\rho = \Lambda\rho_s + (1-\Lambda)\delta\rho$*, wobei* ρ_s *separabel,* $\delta\rho$ *eine verschränkte Dichtematrix, welche keine Produktvektoren mehr in ihrem Bild enthält, und* Λ *maximal ist.*

Beweis: Als erstes wird angenommen, es gäbe keine eindeutige Zerlegung. Unter dieser Annahme existieren also zwei BSA-Zerlegungen: $\rho = \Lambda\rho_{s_1} + (1-\Lambda)\delta\rho_1$ und $\rho = \Lambda\rho_{s_2} + (1-\Lambda)\delta\rho_2$. Nun ist jede konvexe Kombination dieser zwei BSA-Zerlegungen wieder eine BSA-Zerlegung:

$$\rho \quad = \quad \varepsilon\Lambda\rho_{s_1} + (1-\varepsilon)\Lambda\rho_{s_2} + \varepsilon(1-\Lambda)\delta\rho_1 + (1-\varepsilon)(1-\Lambda)\delta\rho_2$$

$$
\begin{aligned}
&= \sum_i (\varepsilon\Lambda\Lambda_{1i} - (1-\varepsilon)\Lambda\Lambda_{2i})P_i + (1-\Lambda)(\varepsilon\delta\rho_1 + (1-\varepsilon)\delta\rho_2) \\
&= \rho_s(\varepsilon) + \delta\rho(\varepsilon),
\end{aligned}
$$

wobei $\varepsilon \in [0,1]$. Wie im letzten Abschnitt schon besprochen, bedeutet dies, daß die Hyperebene $\varepsilon\Lambda_{1i} + (1-\varepsilon)(1-\Lambda_{2i})$ für alle $\varepsilon \in [0,1]$ auf der BSA-Mannigfaltigkeit liegen muß. Aus der polynomialen Struktur der BSA-Mannigfaltigkeit geht aber wiederum hervor, daß die Hyperebene dann auch vollständig für alle ε auf der BSA-Mannigfaltigkeit liegen muß. Da für ein $\varepsilon \notin [0,1]$ und $\delta\rho_1 \neq \delta\rho_2$, $\delta\rho(\varepsilon)$ nicht mehr positiv definit wird, kann das aber nicht sein. Da für $\varepsilon \to \infty$, $\delta\rho(\varepsilon) \sim \delta\rho_1 - \delta\rho_2$ gilt, ist dies leicht einzusehen. Diese Matrix hat die Spur Null und ist offensichtlich ungleich Null, so daß diese nicht mehr positiv definit ist. Dadurch gewinnt man einen Widerspruch zur Annahme, daß die BSA nicht eindeutig sei. Somit wäre das Theorem bewiesen.*q.e.d.*

Im nächsten Kapitel wird auf die spezielle Struktur der BSA-Zerlegungen von $C^2 \otimes C^2$-Zuständen eingegangen. Wie bereits erwähnt, beinhalten die BSA-Zerlegungen nur einen verschränkten BSA-Projektor. Dies macht es möglich, eine genauere analytische Untersuchung vorzunehmen.

Kapitel 5

Die BSA von generischen $C^2 \otimes C^2$-Zuständen

5.1 Inhalt dieses Kapitels

In Kapitel 4 wurde erwähnt, daß der BSA-Rest eines $2-$qbit-Systems durch einen reinen verschränkten Projektor $P_e = |\psi_e\rangle\langle\psi_e|$ eindeutig bestimmt wird. Dieser Sachverhalt führt zur Frage, unter welchen Umständen ein gegebener separabler Zustand ρ_s und ein verschränkter Projektor P_e eine BSA bilden. Zu diesem Thema wurden zahlreiche Arbeiten geschrieben ([100] und [101]).

In diesem Kapitel wird darauf eingegangen, unter welchen Umständen man einen maximal verschränkten Zustand als BSA-Rest erhält, für den Fall, daß ein verschränkter Zustand ρ mit $r(\rho) = r(\rho^{t_A}) = 4$ vorliegt. Dies ist deshalb interessant, weil solche Zustände den Werner-Zuständen sehr ähneln [69], d.h. der Zustand ist durch eine konvexe Kombination von einem chaotisch separablen Zustand und einem maximal verschränkten Zustand ($\rho = \lambda\rho_s + (1-\lambda)|\psi_{max}\rangle\langle\psi_{max}|$) gegeben. Zusätzlich ergaben zahlreiche numerische Untersuchungen, daß der BSA-Rest sehr häufig einen maximal verschränkten Zustand enthält [1]. Dies war der ausschlaggebende Punkt für die Annahme, daß dies für Zustände mit $r(\rho) = r(\rho^{t_A}) = 4$ immer der Fall sei. B. G. Englert, M. O. Scully und N. Metwally ([100] und [101]) konnten aber Gegenbeispiele finden, dies nicht der Fall war. Sie nannten diese Zustände Werner-Zustände erster und zweiter Art. Dieser Sachverhalt führte zur Frage, unter welchen Bedingungen der BSA-Rest einen maximal verschränkten Zustand beinhaltet und warum dieser so häufig maximal verschränkt ist. Auf diese Frage wird in diesem Kapitel ausführlich eingegangen.

Desweiteren erwiesen sich die mathematischen Techniken, welche bei der Untersuchung dieser Bedingungen entwickelt wurden, für die weiteren Untersuchungen von $C^2 \otimes C^N$-, $C^M \otimes C^N$- und $C^2 \otimes C^2 \otimes C^N$-Systemen maßgebend.

Das Kapitel ist in zwei Unterkapitel aufgeteilt. Im ersten Unterkapitel wird auf die kanonische Struktur von separablen Dichtematrizen eingegangen, welche $r(\rho_s) = r(\rho_s^{t_A})$ erfüllt. Dies ist deshalb notwendig, weil diese im zweiten Unterkapitel bei der Untersuchung der BSA-Zerlegung auftritt.

5.2 Die kanonische Struktur

Es folgt nun das nächste wichtige Lemma, was von Woronowicz [80] schon einmal auf eine vollkommen andere Art und Weise bewiesen wurde. Der hier vorgestellte Beweis ist aber für die weiteren Untersuchungen des BSA-Restes und speziell für das $C^2 \otimes C^2 \otimes C^N$-System im letzten Kapitel viel praktischer.

Lemma 5 : *Sei* ρ *eine* 2*-qbit-Dichtematrix, und sei* $r(\rho) = 3$*, sowie* $r(\rho^{t_A}) = 3$*, dann existiert ein Produktvektor* $|e, f\rangle \in R(\rho)$*, so daß auch* $|e^*, f\rangle \in R(\rho^{t_A})$*.*

Beweis: Gegeben sei die Dichtematrix $\rho = \begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix}$. Nun muß A oder C invertierbar sein, da sonst Produktvektoren im Kern liegen würden. Sei C o.B.d.A invertierbar. Man wählt nun die Basis $\{\frac{1}{\sqrt{1+|\alpha|^2}}\binom{1}{\alpha}, \frac{1}{\sqrt{1+|\alpha|^2}}\binom{-\alpha^*}{1}\}$ in H_A. In dieser Basis erhält man $B(\alpha^*) = \frac{1}{1+|\alpha|^2}(1 \quad \alpha^*)\begin{pmatrix} A & B \\ B^\dagger & C \end{pmatrix}\binom{-\alpha^*}{1}$, was eine Funktion von α^* ist. Dies bedeutet, daß $\det B(\alpha^*)) = \det B^\dagger(\alpha) = 0$ immer für ein α (α^*) erfüllt werden kann. Wählt man solch ein α, so erhält man $r(B) = r(B^\dagger) = 1$.

Im nächsten Schritt wirkt man mit einer lokalen nichtunitären Transformation (später wird der Zusammenhang zu unitären Operationen erläutert) $\rho \to (I_A \otimes \frac{1}{\sqrt{C}})\rho(I_A \otimes \frac{1}{\sqrt{C}})$ und redefiniert $A \to \frac{1}{\sqrt{C}}A\frac{1}{\sqrt{C}}$,$B \to \frac{1}{\sqrt{C}}B\frac{1}{\sqrt{C}}$. Die neue Matrix hat dann die Form $\rho = \begin{pmatrix} A & B \\ B^\dagger & I \end{pmatrix}$.

Nun nutzt man die Annahme, daß $r(\rho) = 3$ sein soll. Daraus ergibt sich, daß $A = BB^\dagger + \lambda P$ sein muß, wobei P ein Projektor auf einen Zustand $|\psi\rangle$ ist. Ebenso muß aber auch $r(\rho^{t_A}) = 3$ gelten, so daß $A = B^\dagger B + \tilde{\lambda}\tilde{P}$ gilt, wobei $\tilde{P}$ ein Projektor auf einen Hilbertvektor $|\tilde{\psi}\rangle$ ist.

Dies führt zur Bedingung, daß $BB^\dagger + \lambda P = B^\dagger B + \tilde{\lambda}\tilde{P}$ erfüllt werden muß. Da nun $\mathrm{tr}(BB^\dagger - B^\dagger B) = 0$ ist, folgt daraus $\lambda = \tilde{\lambda}$. Die Bedingung, daß ein Produktvektor $\binom{|f\rangle}{z|f\rangle} \in R(\rho)$ und $\binom{|f\rangle}{z^*|f\rangle} \in R(\rho^{t_A})$ existiert, bedeutet nichts anderes, als daß die Gleichungen

$$\begin{pmatrix} BB^\dagger + \lambda P & B \\ B^\dagger & I \end{pmatrix} \begin{pmatrix} |h\rangle \\ |g\rangle \end{pmatrix} = \begin{pmatrix} |f\rangle \\ z|f\rangle \end{pmatrix}, \tag{5.1}$$

$$\begin{pmatrix} B^\dagger B + \lambda \tilde{P} & B^\dagger \\ B & I \end{pmatrix} \begin{pmatrix} |\tilde{h}\rangle \\ |\tilde{g}\rangle \end{pmatrix} = \begin{pmatrix} |f\rangle \\ z^*|f\rangle \end{pmatrix} \tag{5.2}$$

eine Lösung für $|h\rangle$, $|g\rangle$, $|\tilde{h}\rangle$ und $|\tilde{g}\rangle$ haben.

Aus diesen Gleichungen erhält man

$$\frac{1}{1-zB}|\psi\rangle = \eta \frac{1}{1-z^* B^\dagger}|\tilde{\psi}\rangle. \tag{5.3}$$

Um nun das Lemma zu beweisen, muß man zeigen, daß die Gleichung (5.3) eine Lösung für z und η besitzt. Im weiteren Verlauf des Beweises wird gezeigt, daß man die rechte Seite von (5.3) als komplex Konjugiertes der linken Seite darstellen kann. Dadurch wird dann sichergestellt, daß (5.3) eine Lösung besitzt.

Es wird nun gezeigt, daß sich die Gleichung (5.3) schreiben läßt als

$$\frac{1}{1-zB}|\psi\rangle = \sigma_x \eta \frac{1}{1-z^* B^*}|\psi *\rangle. \tag{5.4}$$

Als erstes wählt man eine Basis $|\psi_1\rangle, |\psi_2\rangle$, so daß $B^\dagger B - BB^\dagger = \begin{pmatrix} \Lambda & 0 \\ 0 & -\Lambda \end{pmatrix}$ gilt. Aus diesem Grund ist $\lambda(P-\tilde{P}) = \begin{pmatrix} \Lambda & 0 \\ 0 & -\Lambda \end{pmatrix}$. Da nun die globalen Phasen von $|\psi\rangle$ und $|\tilde{\psi}\rangle$ keine Rolle spielen, kann man solch eine Basis wählen, wo $|\psi\rangle = \binom{\sqrt{p}}{\sqrt{1-p}e^{i\phi}}$ und $|\tilde{\psi}\rangle = \binom{\sqrt{1-\tilde{p}}}{\sqrt{\tilde{p}}e^{i\tilde{\phi}}}$ gilt. Aus dieser Parametrisierung folgt $\tilde{p} = p, \tilde{\phi} = \phi$ und $\Lambda = \lambda(1-2p)$. Nun existiert immer ein unitärer Operator K, so daß $KBK^\dagger = B^T$ gilt. Daraus ergibt sich trivialerweise, daß $(K^\dagger)^T B^T K^T = B$ und deshalb auch $(K^\dagger)^T K B K^\dagger K^T = B$ ist. Definiert man nun $U = K^\dagger K^T$, so gilt dann $BU = UB$. Es wird gezeigt, daß $K = e^{i\varphi_0}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ist. Sei $M = BB^\dagger - B^\dagger B = \lambda(\tilde{P} - P)$. Nun gilt $KMK^\dagger = B^T B^* - B^* B^\dagger = B^*(B^\dagger)^* - (B^\dagger)^* B^* = -M^* = -M$. Deshalb ist nun $M = \lambda(K|\psi\rangle\langle\psi|K^\dagger - K|\tilde{\psi}\rangle\langle\tilde{\psi}|K^\dagger)$. Daraus ergibt sich

$$K|\psi\rangle = \begin{pmatrix} e^{i\varphi_1}\sqrt{1-p} \\ e^{i\varphi_1}\sqrt{p}e^{i\phi} \end{pmatrix}.$$

Dies bedeutet, daß $K = \begin{pmatrix} 0 & e^{i\theta_1} \\ e^{i\theta_2} & 0 \end{pmatrix}$, $\varphi_1 = \theta_1 + \phi$, $\varphi_1 + \phi = \theta_2$, $\varphi_2 = \theta_1 + \varphi$ und $\varphi_2 + \phi = \theta_2$ ist. Angenommen $\theta_1 \neq \theta_2$. Dann wäre $U = \begin{pmatrix} e^{i(\theta_1-\theta_2)} & 0 \\ 0 & e^{-i(\theta_1-\theta_2)} \end{pmatrix}$. U wird mit B kommutieren, falls B diagonal in dieser Basis ist. Dann wäre aber $BB^\dagger - B^\dagger B = 0$, was bedeuten würde, daß $|\psi\rangle \sim |\tilde{\psi}\rangle$ ist, und dann wäre $\binom{\psi}{0}$ im Bild von ρ. Daraus ergibt sich, daß $\theta_1 = \theta_2$ und $K = e^{i\varphi_0}\sigma_x$ ist. Da nun die globale Phase nicht von Bedeutung ist, setzt man $K = \sigma_x$.

Nun definiert man $\frac{1}{1-zB}|\psi\rangle = \binom{v_1}{v_2}$. Damit die letztere Gleichung (5.4) erfüllt ist, muß $v_1 = \eta e^{i\phi} v_2^*$ und $v_2 = \eta e^{i\phi} v_1^*$ gelten. Diese Gleichungen haben eine Lösung, falls $v_1 = ve^{i\theta}$ und $v_2 = ve^{i\theta+\delta}$ ist, wobei $|v_1| = |v_2| = v$ gilt. Nun wählt man ein beliebiges δ und fordert, daß $\binom{1}{e^{i\delta}} \sim \frac{1}{1-zB}|\psi\rangle$ sei, was bedeutet, daß

$$\left(\; e^{i\delta}, \quad -1 \; \right) \frac{1}{1-zB}|\psi\rangle = 0 \tag{5.5}$$

ist. Diese Gleichung hat nicht nur eine sondern unendlich viele Lösungen.

Um das Lemma abzuschließen, muß nur noch gezeigt werden, daß die nichtunitäre Transformation, die am Anfang des Beweises durchgeführt wurde, nichts am Resultat verändert. Deshalb wird der Zustand ρ jetzt wieder zurücktransformiert. ρ besitzt also die Form

$$\rho = \begin{pmatrix} \sqrt{C}BB^\dagger\sqrt{C} + \lambda\sqrt{C}P\sqrt{C} & \sqrt{C}B\sqrt{C} \\ \sqrt{C}B^\dagger\sqrt{C} & C \end{pmatrix}.$$

Fordert man, daß $\binom{|f>}{z|f>} \in R(\rho)$ und $\binom{|f>}{z^*|f>} \in R(\rho^{t_A})$ gilt, so erhält man

$$\frac{1}{1-\sqrt{C}B\frac{1}{\sqrt{C}}z}\sqrt{C}|\psi> \;\; = \;\; \eta\frac{1}{1-\sqrt{C}B^\dagger\frac{1}{\sqrt{C}}z^*}\sqrt{C}|\tilde{\psi}>.$$

Dies ist äquivalent zu

$$\sqrt{C}(1-f(z)B)|\psi> \;\; = \;\; \sqrt{C}\eta(1-f^*(z)B^\dagger)|\tilde{\psi}>,$$

was wiederum

$$(1-f(z)B)|\psi> \;\; = \;\; \eta(1-f^*(z)B^\dagger)\sigma_x|\psi>$$

nach sich zieht. Damit wäre der Beweis abgeschlossen.$_{q.e.d.}$

Nun wird untersucht, unter welchen Bedingungen die BSA-Zerlegung eines Zustandes ρ mit $r(\rho) = r(\rho^{t_A}) = 4$ einen maximal verschränkten BSA-Rest aufweisen kann.

5.3 Die BSA-Zerlegung mit maximal verschränktem BSA-Rest

Nehmen wir an, daß ρ die BSA-Zerlegung $\rho = \Lambda\rho_s + (1-\Lambda)P_{\psi_e}$ besitzt und generisch ist, d.h. $r(\rho) = r(\rho^{t_A}) = 4$. Ist Λ ungleich 1, so ist ρ^{t_A} nicht positiv definit. $r(\rho_s^{t_A}) = 4$ darf nicht sein. Wäre dies der Fall, so könnte man $1-\Lambda$ so durch $1-\Lambda-\varepsilon$ ersetzen, daß $\Lambda\rho_s^{t_A} + \varepsilon P_{\psi_e}^{t_A}$ positiv definit ist, d.h. $\rho_s' = \rho_s + \varepsilon P_{\psi_e}$ wäre separabel. Da nun der Rang von $\rho_s^{t_A}$ nicht voll sein kann, bedeutet dies, daß ein Hilbertvektor $|v\rangle$ existieren muß, so daß $\rho_s^{t_A}|v\rangle = 0$ gilt. $P_{\psi_e}^{t_A}$ hat jetzt 3 positive und einen negativen Eigenwert. Den Eigenvektor zum negativen Eigenwert kann man in einer geeigneten Basis schreiben als

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

Es muß gelten, daß $\langle v|\psi_-\rangle \neq 0$. Wäre dies nicht der Fall, so könnte man $1-\Lambda$ wieder durch $(1-\lambda-\varepsilon)$ ersetzen, so daß $\Lambda\rho_s^{t_A} + \varepsilon P_{\psi_-}^{t_A}$ positiv bleibt. Dies alles bedeutet, daß für die BSA-Zerlegung entweder $r(\rho_s) = 4$ und $r(\rho_s^{t_A}) = 3$ oder $r(\rho_s) = r(\rho_s^{t_A}) = 3$ gilt. Der Fall, in dem $r(\rho_s) < 3$ ist kann nicht auftreten, da ansonsten $r(\rho_s) = 3$ oder $r(\rho_s) = 4$ nicht erfüllt werden kann [102]. Nehmen wir also an, daß $r(\rho_s) = 4$ zutrifft.

Nun kann man immer $|\psi_e\rangle$ für alle Basen $|e_1\rangle$,$|e_2\rangle$ schreiben als

$$|\psi_e\rangle = N_1|e_1, f_1\rangle + N_2|e_2, f_2\rangle, \tag{5.6}$$

wobei $\langle e_1|e_1\rangle = \langle e_2|e_2\rangle = 1$, aber $\langle e_1|e_2\rangle$ nicht Null sein muß. Sei nun $|\hat{e}_1\rangle$,$|\hat{e}_2\rangle$ die biorthogonale Basis zu $|e_1\rangle$ und $|e_2\rangle$.

Man erhält

$$\langle\hat{e}_1|\psi_e\rangle = N_2\langle\hat{e}_1|e_2\rangle|f_2\rangle \tag{5.7}$$
$$\langle\hat{e}_2|\psi_e\rangle = N_1\langle\hat{e}_2|e_1\rangle|f_1\rangle. \tag{5.8}$$

Fordert man nun, daß $\langle f_1|f_1\rangle = \langle f_2|f_2\rangle = 1$ gilt, so kann man aus den letzten beiden Gleichungen eindeutig $N_1, N_2, |f_1\rangle$ und $|f_2\rangle$ bestimmen. O.B.d.A. wird nun angenommen, daß $N_1 \geq N_2$ gilt.

Man definiert

$$|\psi_e(\alpha)\rangle = \frac{1}{N(\alpha)}(\alpha N_1|e_1, f_1\rangle + \frac{N_2}{\alpha}|e_2, f_2\rangle), \tag{5.9}$$

wobei $N(\alpha)$ definiert ist als

$$N(\alpha)^2 = \alpha^2 N_1^2 + \frac{1}{\alpha^2} N_2^2 + 2N_1 N_2 \mathrm{Re}(\langle e_1|e_2\rangle\langle f_1|f_2\rangle). \tag{5.10}$$

Der BSA-Projektor kann geschrieben werden als

$$P_{\psi_e} = N(\alpha)^2 P_{\psi_e(\alpha)} + (1-\alpha^2) P_{e_1 f_1} + (1 - \frac{1}{\alpha^2}) P_{e_2 f_2}. \tag{5.11}$$

Der Projektor P_{ψ_e} wird durch den Ausdruck (5.11) ersetzt, um dadurch die BSA zu verbessern. Dafür muß vorausgesetzt werden, daß $N(\alpha)^2 < 1$ ist, woraus sich die Bedingung

$$\alpha^2 N_1^2 + \frac{1}{\alpha^2} N_2^2 < N_1^2 + N_2^2 \tag{5.12}$$

ergibt.

Definiert man $x = \frac{N_2^2}{N_1^2}$, so sieht man, daß $N(\alpha)^2 < 1$ genau dann erfüllt ist, wenn $x < \alpha^2 < 1$ gilt. Dies ist nur möglich, wenn $N_1 \neq N_2$ erfüllt ist. Nun wählt man $\alpha^2 < 1$ sehr nah an 1. Wenn man $-\frac{1-\alpha^2}{\alpha^2} P_{e_2^* f_2}$ von $\Lambda\rho_s^{t_A}$ abziehen kann, verbessert man dadurch die BSA. Dies funtioniert nur, falls $|e_2^* f_2\rangle$ im Bild von $\rho_s^{t_A}$ liegt. Das bedeutet, daß falls $|v\rangle = |\hat{e}_1^*, h_1\rangle + |e_2^*, h_2\rangle$ ist, man dann die Gleichung $\langle h_1|f_2\rangle = 0$ erfüllen muß, bzw.

$$\langle v|e_2^*\rangle\langle\hat{e}_1|\psi_e\rangle = 0. \tag{5.13}$$

Es ist der obigen Gleichung leicht anzusehen, daß sie sehr viele Lösungen besitzt. Nimmt man z.B. $|e_2\rangle = |\hat{e}_1\rangle$ und wählt $|\hat{e}_1\rangle$ proportional zu $|0\rangle + \alpha|1\rangle$, dann folgt aus der Gleichung, daß $[\langle v|0\rangle + \alpha^*\langle v|1\rangle][\langle 0|\psi_e\rangle + \alpha^*\langle 1|\psi_e\rangle] = 0$ erfüllt werden muß. Dies ist eine quadratische Gleichung in α^*, welche immer eine Lösung besitzt. Daraus ergibt sich, daß entweder $r(\rho_s) = 3$ ist oder $N_1 = N_2$. Tritt der letztere Fall ein, so ist $|\psi_e\rangle$ maximal verschränkt. Dies ist leicht zu sehen, wenn man die allgemeine Form $|e_1\rangle = \binom{\sqrt{p}}{\sqrt{1-p}e^{i\phi}}$ und $|\hat{e}_2\rangle = \binom{\sqrt{1-p'}}{\sqrt{p'}e^{i\phi'}}$ in dieser Basis wählt. In der so gewählten Basis ist $|\psi_e\rangle = a|00\rangle + \sqrt{1-a^2}|11\rangle$, so daß dann

$$\begin{aligned} \langle\hat{e}_1|\psi_e\rangle &= a\sqrt{p}|0\rangle + \sqrt{1-a^2}\sqrt{1-p}|1\rangle e^{-i\phi} \\ &\text{und} \\ \langle\hat{e}_2|\psi_e\rangle &= a\sqrt{p'}|0\rangle + \sqrt{1-a^2}\sqrt{1-p'}|1\rangle e^{-i\phi'} \end{aligned} \tag{5.14}$$

ist.

Daraus ergibt sich dann

$$\begin{aligned} N_2^2 |\langle\hat{e}_1|e_2\rangle|^2 &= a^2 p + (1-a^2)(1-p), \\ N_1^2 |\langle\hat{e}_2|e_1\rangle|^2 &= a^2 p' + (1-a^2)(1-p'). \end{aligned}$$

Man beachte, daß $|\langle\hat{e}_1|e_2\rangle|^2 = |\langle\hat{e}_2|e_1\rangle|^2$ gilt, so daß sich $a^2 = \frac{1}{2}$ für $N_1^2 = N_2^2$, ergibt. Dies bedeutet also, daß $|\psi_e\rangle$ maximal verschränkt ist.

Deshalb wird nun der Fall $r(\rho_s) = r(\rho_s^{t_A}) = 3$ betrachtet. Interessant für diesen Fall ist, daß wenn man in der Lage ist $P_{e_2^*,f_2}$ von $\Lambda\rho_s^{t_A}$ abzuziehen, man gleichzeitig $P_{e_1^*,f_1}$ zum Bild von $\rho_s^{t_A}$ und P_{e_1,f_1} zum Bild von ρ_s addiert. Dies führt wegen $r(\rho) = 4$ zu einer Vergrößerung des Ranges von ρ_s auf $r(\rho_s) = 4$. Es können also nur die folgenden zwei Fälle auftreten:

- Ist man in der Lage $P_{e_2^*,f_2}$ von $\rho_s^{t_A}$ abzuziehen, wobei $r(\rho_s) = r(\rho_s^{t_A}) = 3$ gilt, so besitzt die BSA-Zerlegung einen maximal verschränkten BSA-Rest und es gilt wieder $r(\rho_s) = 4$.
- Ist man nicht mehr in der Lage $P_{e_2^*,f_2}$ von $\rho_s^{t_A}$ abzuziehen, wobei $r(\rho_s) = r(\rho_s^{t_A}) = 3$ gilt, so besitzt die BSA-Zerlegung entweder in diesem Grenzfall einen maximal verschränkten BSA-Rest oder keinen.

Es wird also nun untersucht unter welchen Umständen man $P_{e_2^*,f_2}$ von $\rho_s^{t_A}$ abziehen kann. Aus den Resultaten des letzteren Abschnits wissen wir das eine eindimensionale Familie von Produktvektoren $|e_2(\delta), f_2(\delta)\rangle$ existiert, wobei δ reell ist, so daß $|e_2(\delta), f_2(\delta)\rangle \in R(\rho)$ und $|e_2(\delta)^*, f_2(\delta)\rangle \in R(\rho^{T_A})$ gilt.
Nun sind wir in der Lage explizit nachzuprüffen wann $|\psi_e\rangle$ unter den gegebenen Voraussetzungen maximal verschränkt ist. Ist $|\psi_e\rangle$ gegeben und sei $|e_2, f_2\rangle = |e_2(\delta), f_2(\delta)\rangle$, für ein gegebenes ρ_s, dann läßt sich $|f_1\rangle$ und $|e_1\rangle$ wie folgt bestimmen:

$$
\begin{aligned}
|f_1\rangle &= \frac{\langle\hat{e}_2(\delta)|\psi_e\rangle}{|\langle\hat{e}_2(\delta)|\psi_e\rangle|}, \\
|e_1\rangle &= \frac{\langle\hat{f}_2(\delta)|\psi_e\rangle}{|\langle\hat{f}_2(\delta)|\psi_e\rangle|}.
\end{aligned}
$$

Aus der Normierung $\langle f_1|f_1\rangle = 1$, erhält man $N_1 = \frac{|\langle\hat{e}_2|\psi_e\rangle|}{|\langle\hat{e}_2|e_1\rangle|}$. Da wir nun $|e_1\rangle$ und $|f_1\rangle$ kennen, können wir auch $N_2 = \frac{|\langle\hat{e}_1|\psi_e\rangle|}{|\langle\hat{e}_1|e_2\rangle|}$ berechnen.

Dies bedeutet daß man N_1 und N_2 explizit berechnen kann aus ρ_s und $|\psi_e\rangle$. Daraus ergibt sich folgendes Theorem:

Theorem 7 : *Sei ρ ein $C^2 \otimes C^2$-Zustand mit $r(\rho) = r(\rho^{T_A}) = 4$ und der explizit gegebenen BSA-Zerlegung $\rho = \Lambda\rho_s + (1-\Lambda)P_{\psi_e}$. Dann ist entweder $|\psi_e\rangle$ maximal verschränkt, oder $r(\rho_s) = r(\rho_s^{T_A}) = 3$ und für jede expansion von $|\psi_e\rangle = N_1|e_1, f_1\rangle + N_2|e_2, f_2\rangle$, so daß $|e_2, f_2\rangle \in R(\rho_s)$ und $|e_2^*, f_2\rangle \in R(\rho_s^{T_A})$ erfüllt ist, gilt daß $N_1 < N_2$.*

Beweis: Würde ein $|e_2(\delta), f_2(\delta)\rangle$ existieren so daß $N_1 > N_2$ gilt, so könnte man die Optiemirungsprozedur anwenden und dadurch ein Wiederspruch zur Optimalität der BSA erhalten.$_{q.e.d.}$

Das Theorem liefert damit eine Erklärung, warum in den numerischen Untersuchungen [1] so häufig ein maximal verschränkter BSA-Projektor auftritt. Desweiteren liefert dieses Theorem ein Konstruktiosschema für BSA-Zerlegungen mit maximal verschränkten BSA-Resten.

Kapitel 6

Die PPT-BSA

6.1 Inhalt dieses Kapitels

In diesem Kapitel werden BSA-Zerlegungen von PPT-Zuständen untersucht. Wie schon in Kapitel 4 erwähnt, wird als Vorbild für die erweiterte Formulierung der BSA die Arbeit von M. Lewenstein und A. Sanpera [1] sowie die Arbeit von A. Sanpera, R. Tarrach und G. Vidal [102] genutzt. Der konstruktive Algorithmus, der hier vorgestellt wird, ermöglicht es, PPT Dichtematritzen nach deren Separabilität zu untersuchen. Desweiteren basieren die Arbeiten über $C^2 \otimes C^N$ ([51] und [52]) und $C^M \otimes C^N$ [103] und die im letzten Kapitel beschriebene Arbeit über $C^2 \otimes C^2 \otimes C^N$ auf dem nun folgenden PPT-BSA-Theorem. Am Ende dieses Kapitels wird auf die Konstruktion von Witness-Operatoren ([104], [105], [107] und [108]) eingegangen. Die Witness-Operatoren ermöglichen es, PPT-verschränkte Zustände zu detektieren ([107] und [108]) und sie können Bell-Ungleichungen beschreiben.

6.2 Die PPT-BSA von $C^M \otimes C^N$ zusammengesetzten Systemen

Für eine Dichtematrix ρ bezeichnet $V[\rho] = \{|e,f\rangle \mid |e,f\rangle \in R(\rho) \text{ und } |e^*,f\rangle \in R(\rho^{t_A})\}$, d.h. die Menge aller Produktvektoren $|e,f\rangle$, welche sich nicht nur im Bildbereich von ρ befinden, sondern es gilt auch zusätzlich, daß $|e^*,f\rangle$ sich im Bildbereich von ρ^{t_A} befinden soll. Gegeben sein nun eine Dichtematrix ρ in $C^M \otimes C^N$, welche ein PPT-Zustand ist. Es gilt folgendes Theorem:

Theorem 8 : *Für jede PPT-Dichtematrix* ρ *existiert eine separable Matrix*

$$\rho_s^* = \sum_\alpha \Lambda_\alpha |\, e_\alpha, f_\alpha\rangle\langle e_\alpha, f_\alpha\,| \tag{6.1}$$

mit $\Lambda_\alpha \geq 0$ *und einer abzählbaren Menge von Produktvektoren* $\{|\, e_\alpha, f_\alpha\rangle \in V[\rho]\}$, *so daß* $\delta\rho = \rho - \rho_s^* \geq 0$ *und* $\delta\rho^{t_A} = (\rho - \rho_s^*)^{t_A} \geq 0$ *ist, und*

$$\Lambda_{PPT} \equiv \mathrm{tr}(\rho_s^*) \tag{6.2}$$

maximal ist.

Beweis: Der Beweis funktioniert wie im Theorem (3) analog zum Beweis der Existenz einer BSA. Aufgrund des kompakten Gebietes aller separablen Dichtematritzen existiert ein Maximum bezüglich der Menge V. Durch Vergrößerung der Menge V maximiert man die PPT-BSA bis das Maximum erreicht ist.$_{q.e.d.}$

Zu beachten ist, daß die gesamte Information über die Verschränktheit des PPT-Zustandes von ρ durch den PPT-BSA-Parameter Λ_{PPT} und durch $\delta\rho$ gegeben ist.

Analog zur Definition der BSA-Maximalität, wird nun der Begriff der PPT-Maximalität definiert.

Definition 8 : *Sei* $|\, e, f\rangle \in V[\rho]$. *Ein nicht negativer Parameter* Λ *heißt in Bezug auf eine Dichtematrix* ρ *und einen Projektor* $P = |\, e, f\rangle\langle e, f\,|$, *PPT-maximal, falls* $\rho - \Lambda P \geq 0$ *ist, und für alle* $\varepsilon \geq 0$ *die Matrix* $\rho - (\Lambda + \varepsilon)P$ *kein PPT-Zustand mehr ist.*

Man sieht, daß in Bezug auf die BSA aus dem letzten Kapitel hier nun noch die zusätzliche Einschränkung von PPT auf allen Systemen gewährleistet werden muß. Das folgende Lemma liefert die Bedingung für eine PPT-Maximalität.

Lemma 6 : *In Bezug auf einen PPT-Zustand* ρ *und einen Projektor* $P = |\, e, f\rangle\langle e, f\,|$ *ist* Λ *genau dann PPT-maximal, wenn gilt:*

- *Falls* $|\, e, f\rangle \notin V[\rho]$, *dann ist* $\Lambda = 0$.
- *Ist* $\Lambda^{(0)} = \frac{1}{\langle e,f\,|\rho^{-1}|\,e,f\rangle}$ *und* $\Lambda^{(1)} = \frac{1}{\langle e^*,f\,|(\rho^{t_A})^{-1}|\,e^*,f\rangle}$, *dann ist* Λ *gegeben durch*

$$\Lambda = \min(\Lambda^{(0)}, \Lambda^{(1)}). \tag{6.3}$$

Beweis: Der erste Teil ist trivial. Aus dem BSA-Lemma (1) folgt, daß jedes $\Lambda^{(0)}$ bzw. $\Lambda^{(1)}$ in Bezug auf $|e, f\rangle$, bzw. $|e^*, f\rangle$ maximal ist. Nimmt man nun das Minimum aus dieser Menge, so erhält man den maximalen Anteil, den man abziehen kann, ohne die PPT zu verlieren.$_{q.e.d.}$

Nun wird die paarweise Maximalität so definiert, wie es auch bei der BSA der Fall war.

Definition 9 : *Ein Paar von nicht negativen* (Λ_1, Λ_2) *ist in Bezug auf einen PPT-Zustand* ρ *und ein Paar von Projektoren* $P_1 = |e_1, f_1\rangle\langle e_1, f_1|$ *und* $P_2 = |e_2, f_2\rangle\langle e_2, f_2|$ *paarweise PPT-maximal, wobei* $|e_1, f_1\rangle, |e_2, f_2\rangle \in V[\rho]$ *ist, falls:*

1. $\rho - \Lambda_1 P_1 - \Lambda_2 P_2$ *ein PPT-Zustand ist,*
2. Λ_1 *in Bezug auf* $\rho - \Lambda_2 P_2$ *und den Projektor* P_1 *PPt-maximal ist,*
3. Λ_2 *in Bezug auf* $\rho - \Lambda_1 P_1$ *und den Projektor* P_2 *PPT-maximal ist,*
4. *und* $\Lambda_1 + \Lambda_2$ *maximal ist.*

Analog zur BSA (Kapitel 4.3) wird bezüglich einer abzählbaren Menge V von Produktvektoren die PPT-BSA-Mannigfaltigkeit wie folgt definiert:

Definition 10 : *Sei* $F(\lambda_1, \ldots, \lambda_K) = 0$ *die BSA-Mannigfaltigkeit bezüglich des Zustandes* ρ *und* $\tilde{F}(\lambda_1, \ldots, \lambda_K) = 0$ *die des Zustandes* ρ^{t_A}*. Dann läßt sich die PPT-BSA-Mannigfaltigkeit schreiben als:*

$$\lambda_1 = \bar{f}(\lambda_2, \ldots, \lambda_K) \equiv \begin{cases} \lambda_1 = f(\lambda_2, \ldots, \lambda_K) & \textit{falls } f < \tilde{f} \\ \lambda_1 = \tilde{f}(\lambda_2, \ldots, \lambda_K) & \textit{sonst,} \end{cases} \tag{6.4}$$

wobei f *und* $\tilde{f}$ *die expliziten Auflösungen der BSA-Mannigfaltigkeiten* $F = 0$ *und* $\tilde{F} = 0$ *nach* λ_1 *sind. Dementsprechend wird die PPT-BSA-Mannigfaltigkeit in ihrer impliziten Form als* $\bar{F}(\lambda_1, \ldots \lambda_K) = 0$ *bezeichnet.*

Zu beachten ist, daß die PPT-BSA-Mannigfaltigkeit $\bar{F}(\lambda_1, \ldots \lambda_K) = 0$ eine stetige aber nicht überall differenzierbare Mannigfaltigkeit ist. Dies wird im weiteren Verlauf bei der Untersuchung des Algorithmus zur paarweisen Maximalität in Anhang B näher erläutert.

Zu zeigen ist nun, daß die paarweise Maximierung auch zur PPT-BSA führt.

Theorem 9 : *Gegeben sei ein PPT-Zustand* ρ*. Die Matrix* $\rho_s^* = \sum_\alpha \Lambda_\alpha P_\alpha$ *ist die PPT-BSA genau dann, wenn gilt:*

1. *Alle* Λ_α *sind in Bezug auf* $\rho - \sum_{\alpha' \neq \alpha} \Lambda_{\alpha'} P_{\alpha'}$ *und den Projektor* $P_{\alpha'}$ *PPT-maximal.*

2. *Alle Paare* $(\Lambda_\alpha, \Lambda_\beta)$ *sind in Bezug auf* $\rho - \sum_{\alpha' \neq \alpha.\beta} \Lambda_\alpha P_\alpha$ *und die Projektoren* (P_α, P_β) *paarweise PPT-maximal.*

Beweis: Für den Fall, daß ρ_s^* eine PPT-BSA ist, muß diese für alle Λ_α und Paare $(\Lambda_\alpha, \Lambda_\beta)$ auch PPT-maximal sein. Ansonsten könnte man den PPT-BSA-Parameter erhöhen, was ein Widerspruch zur Annahme der PPT-BSA von ρ_s^* wäre.

ρ_s sei definiert als $\rho_s = \sum_\alpha \lambda_\alpha P_\alpha$, wo alle λ_α individuell PPT-maximal sind. Dies bedeutet, daß ρ_s auf dem Rand der konvexen Menge Z aller separablen Matrizen liegt, welche $\rho - \rho_s \geq 0$ und $(\rho - \rho_s)^{t_A} \geq 0$ erfüllen. Dieser Rand wird durch die PPT-Mannigfaltigkeit $F(\lambda_1, \ldots, \lambda_K) = 0$ beschrieben. Diese BSA-Mannigfaltigkeit ist eine stetige aber nicht überall differenzierbare Mannigfaltigkeit.

Sei $\rho_m = \sum_\alpha^K \Lambda_\alpha P_\alpha$ die separable Matrix, welche paarweise PPT-maximal ist. Die paarweise Maximalität in $(\Lambda_\alpha, \Lambda_\beta)$ bedeutet, daß $(\lambda_\alpha + \lambda_\beta)$ für $\lambda_{\alpha.\beta} = \Lambda_{\alpha.\beta}$ und für alle $\gamma \neq \alpha, \beta$ $\lambda_\gamma = \Lambda_\gamma$ maximal sein muß. Die Punkte Λ lassen sich mindestens einer Mannigfaltigkeit eindeutig zuordnen, so daß man $\lambda_\beta = f_\beta(\lambda_1, \ldots, \lambda_{\beta-1}, \lambda_{\beta+1}, \ldots, \lambda_K)$ schreiben kann. Dies bedeutet, daß $\lambda_\alpha + \lambda_\beta = \lambda_\alpha + f_\beta$ für alle α und β geschrieben werden kann. Es gilt nun

$$\frac{\partial}{\partial \lambda_i} (\lambda_i + f_j) \mid_{\lambda=\Lambda} = \frac{\partial}{\partial \lambda_i} \left(\sum_{i' \neq j} \lambda_{i'} + f_j \right) \mid_{\lambda=\Lambda} \leq 0, \tag{6.5}$$

wobei $\Lambda = (\Lambda_1, \ldots, \Lambda_K)$ ist. Es können nun folgende Fälle auftreten:

1. O.B.d.A. seien die Ableitungen für $(\lambda_1, \ldots, \lambda_n)$ kleiner als Null und für die restlichen λ's im Punkte $\lambda = \Lambda$ gleich Null, wobei $n < K$ ist. Dies ist der Fall, wenn die paarweise PPT-Maximalität auf der Schnittfläche der verschiedenen Mannigfaltigkeiten liegt. Dann folgt, daß der Punkt $\lambda = \Lambda$ in Bezug auf die Koordinaten $(\lambda_{n+1}, \ldots, \lambda_K)$ entweder ein lokales Maximum oder ein Sattelpunkt sein muß. Da nun Z eine konvexe Menge ist, muß für jedes $\rho_s, \rho_s' \in Z$ auch $\varepsilon\rho_s + (1-\varepsilon)\rho_s' \in Z$ gelten. Hätte man nun einen Sattelpunkt, so würden zwei separable Matrizen existieren, welche nicht mehr in Z liegen. Dies ist natürlich nicht möglich, also muß es ein lokales Maximum sein. Dieses lokale Maximum muß aber mit dem Wert der PPT-BSA übereinstimmen, da ansonsten $\varepsilon \mathrm{tr}(\rho_s^*) + (1-\varepsilon)\mathrm{tr}(\rho_s) > \mathrm{tr}(\rho_s)$ gilt. Also muß $\mathrm{tr}(\rho_s^*) = \mathrm{tr}(\rho_s)$ gelten.

2. Alle Ableitungen sind gleich Null. Dies bedeutet, daß die paarweise PPT-Maximalität sich auf keiner Schnittfläche befindet. In diesem Fall wird die Beweisführung entsprechend dem BSA-Fall geführt.

Somit wäre der Beweis abgeschlossen.$_{q.e.d.}$

Am Ende dieses Unterkapitels ist noch zu bemerken, daß sämtliche Überlegungen und Beweise auf mehrfach zusammengesetzte Systeme übertragbar sind.

6.3 Konstruktion von Verschränktheitszeugen (Witnesses)

Witness-Operatoren ([104], [105] und [106]) sind Operatoren, mit denen man quantenmechanische Zustände auf Verschränktheit untersuchen kann. Sie sind deshalb in der Untersuchung von quantenmechanischen Zuständen von entscheidener Bedeutung. Aus diesem Grund wird in diesem Unterkapitel auf die Konstruktion von Witness-Operatoren mit Hilfe des PPT-Restes $\delta\rho$ eingegangen [107]. Der Begriff des Witness-Operators wird im Verlauf der Konstruktion durch den PPT-Rest wie in der Arbeit von M. Lewenstein, B. Kraus, J.I. Cirac und P. Horodecki [107] erklärt.

Definition 11 : *Ein Operator W, welcher auf einen N-fach zusammengesetzten Hilbertraum $H = C^{M_1} \otimes \ldots \otimes C^{M_N}$ wirkt, wird Verschränktheitszeuge oder Witness-Operator genannt, wenn für alle separablen Zustände ρ_s, $\mathrm{tr}(W\rho_s) \geq 0$ gilt, und ein verschränkter Zustand ρ existiert, so daß $\mathrm{tr}(W\rho) < 0$ erfüllt ist.*

Die Existenz solch eines Witnesses zu einem gegebenen verschränkten Zustand ρ ist leicht einzusehen, wenn man bedenkt, daß die Menge aller separablen Zustände eine konvexe und kompakte Menge bilden. Der verschränkte Zustand ρ kann demnach als ein Punkt außerhalb dieser Menge angesehen werden. Laut dem Hahn-Banach-Theorem existiert aber immer eine Hyperebene, welche eine konvexe Menge Z und einen Punkt außerhalb dieser Menge $(\rho \notin Z)$ trennt, d.h. $\mathrm{tr}(W\rho) < 0$.

Wie konstruiert man nun einen Witness über die PPT-BSA-Zerlegung? Die entscheidende Charakteristik der PPT-BSA-Zerlegung $\rho = \Lambda_{PPT}\rho_s^* + (1 - \Lambda_{PPT})\delta\rho$ ist, daß der PPT-BSA-Rest $\delta\rho$ keine Produktvektoren mehr enthält, die man abziehen könnte, ohne die PPT von $\delta\rho$ zu verletzen.

Definiert wird nun $K \equiv \{|k_i\rangle\} \in K(\delta\rho)$ und $K_A \equiv \{|k_{A_i}\rangle\} \in K(\delta\rho^{t_A})$ als die Menge aller orthonormalen Basen, die den Kern von $\delta\rho$ und $\delta\rho^{t_A}$ aufspannen.

Nun wird der Operator

$$V \equiv \sum_{i=1}^{k(\delta\rho)} |k_i\rangle\langle k_i| + \sum_{i=1}^{k(\delta\rho^{t_A})} (|k_{A_i}\rangle\langle k_{A_i}|)^{t_A} \tag{6.6}$$

definiert, wobei $k(\delta\rho)$ und $k(\delta\rho^{t_A})$ die Dimension der jeweiligen Kerne von $\delta\rho$ und $\delta\rho^{t_A}$ sind. Jetzt bildet man den Erwartungswert von V bezüglich der Produktvektoren $|ef\rangle$ und erhält:

$$\begin{aligned}\langle e,f|V|e,f\rangle &= \sum_{i=1}^{k(\delta\rho)} \langle e,f|k_i\rangle\langle k_i|e,f\rangle + \sum_{i=1}^{k(\delta\rho^{t_A})} \langle e,f|(|k_{A_i}\rangle\langle k_{A_i}|)^{t_A}|e,f\rangle \\ &= \sum_{i=1}^{k(\delta\rho)} \langle e,f|k_i\rangle\langle k_i|e,f\rangle + \sum_{i=1}^{k(\delta\rho^{t_A})} \langle e^*,f|k_{A_i}\rangle\langle k_{A_i}|e^*,f\rangle\end{aligned}$$

Dies bedeutet, daß $\langle e,f|V|e,f\rangle \geq \varepsilon$ ist, wobei $\varepsilon > 0$ gilt. Wäre nämlich $\langle e,f|V|e,f\rangle = 0$, dann gäbe es einen Produktvektor, der gleichzeitig im Bild von $\delta\rho$ und $\delta\rho^{t_A}$ liegen würde. Dies wäre aber wiederum ein Widerspruch zur Annahme, daß $\delta\rho$ ein PPT-BSA-Rest ist.

Kennt man nun die Schwelle ε, dann kann man folgenden Operator definieren:

$$W \equiv V - \varepsilon I. \tag{6.7}$$

Der Operator W erfüllt die Bedingung, daß für alle Produktvektoren $\langle e,f|W|e,f\rangle \geq 0$ gilt. Dies bedeutet, daß wenn ein Zustand ρ die Eigenschaft $\mathrm{tr}(W\rho) \leq 0$ besitzt, dieser dann auch nicht separabel sein kann. Bildet man z.B. die Spur $\mathrm{tr}(\delta\rho W)$, so erhält man per Konstruktion $\mathrm{tr}(\delta\rho W) < 0$. Dies beweist die Existenz eines verschränkten Zustandes, welchen man mit der PPT-BSA-Konstruktion eines Witness-Operators bezeugen kann.

Man beachte, daß der Witness-Operator eine Art Bell-Ungleichung $\mathrm{tr}(W\rho) \leq 0$ liefern kann, wenn sich der Witness-Operator W als Summe von Produktprojektoren $W = \sum_i^{\alpha} c_\alpha |e_\alpha, f_\alpha\rangle\langle e_\alpha, f_\alpha|$ schreiben läßt, wobei die c_α's nicht unbedingt positiv sein müssen. Dadurch läßt sich $\mathrm{tr}(W\rho) \leq 0$ auch schreiben als

$$\mathrm{tr}(W\rho) = \sum_{\alpha} c_\alpha \langle e_\alpha, f_\alpha|\rho|e_\alpha, f_\alpha\rangle \leq 0. \tag{6.8}$$

Wie man sieht, ist dies eine Bell-Ungleichung. Genauer gesagt, impliziert diese Ungleichung, daß es keine Theorie geben kann, welche den Zustand ρ durch lokal verborgene Parameter mit beschränkten Werten beschreibt [109].

Man sieht, daß sich die PPT-BSA-Zerlegungsmethode exzellent zur Untersuchung von PPT-verschränkten Zuständen eignet.

Kapitel 7

Das BSA-Verschränktheitsmaß

7.1 Inhalt dieses Kapitels

Die Formulierung der BSA ermöglicht auf natürliche Art und Weise, ein Verschränktheitsmaß zu definieren. Da es in der Regel sehr schwer ist, Verschränktheitsmaße mit den notwendigen Eigenschaften zu formulieren, ist dieses Thema für die BSA-Theorie von besonderem Interesse.

7.2 Das BSA-Verschränktheitsmaß

Es wird nun gezeigt, daß der BSA-Parameter $E(\rho) := (1 - \Lambda_{BSA}(\rho))$ die folgenden Eigenschaften eines Verschränktheitsmaßes erfüllt:

- Für alle separablen Zustände ρ_s gilt $E(\rho_s) = 0$;
- Lokale unitäre Transformationen ändern das Verschränkheitsmaß nicht;
- Sei $\sum_\alpha A_\alpha A_\alpha^\dagger \otimes B_\alpha B_\alpha^\dagger = 1$. Dann folgt für das Verschränktheitsmaß

$$\sum_\alpha \mathrm{tr}(A_\alpha \otimes B_\alpha \rho A_\alpha^\dagger \otimes B_\alpha^\dagger) \left(E\left(\frac{A_\alpha \otimes B_\alpha \rho A_\alpha^\dagger \otimes B_\alpha^\dagger}{\mathrm{tr}(A_\alpha \otimes B_\alpha \rho A_\alpha^\dagger \otimes B_\alpha^\dagger)}\right) \right) \leq E(\rho). \qquad (7.1)$$

Um dies zu zeigen, muß als erstes untersucht werden, wie ein POVM die BSA beeinflußt. Zu diesem Zweck definiert man $V_i := A_i \otimes B_i$, so daß $\sum_i V_i V_i^\dagger = 1$ gilt.

Die V's sind demnach lokale POVM's. Die BSA-Zerlegung ist durch $\rho = \Lambda_{BSA}\rho_s^* + (1-\Lambda_{BSA})\delta\rho$ gegeben. Nach der Wirkung des obigen POVM's

$$\begin{aligned}
\rho_i &:= \frac{V_i\rho V_i}{\mathrm{tr}(V_i\rho V_i)} \\
&= \frac{\Lambda_{BSA}\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}{\mathrm{tr}(V_i\rho V_i^\dagger)}\sum_\alpha\left(\frac{\Lambda_\alpha\mathrm{tr}(V_iP_\alpha V_i^\dagger)}{\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}\right)\left(\frac{V_iP_\alpha V_i^\dagger}{\mathrm{tr}(V_iP_\alpha V_i^\dagger)}\right) \\
&+ (1-\Lambda_{BSA})\frac{\mathrm{tr}(V_i\delta\rho V_i^\dagger)}{\mathrm{tr}(V_i\rho V_i^\dagger)}\left(\frac{V_i\delta\rho V_i^\dagger}{\mathrm{tr}(V_i\delta\rho V_i^\dagger)}\right. \\
&= \frac{\Lambda_{BSA}\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}{\mathrm{tr}(V_i\rho V_i^\dagger)}\sum_\alpha\left(\frac{\Lambda_\alpha\mathrm{tr}(V_iP_\alpha V_i^\dagger)}{\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}\right)\left(\frac{V_iP_\alpha V_i^\dagger}{\mathrm{tr}(V_iP_\alpha V_i^\dagger)}\right) \\
&+ (1-\Lambda_{BSA}\frac{\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}{\mathrm{tr}(V_i\rho V_i^\dagger)})\left(\frac{V_i\delta\rho V_i^\dagger}{\mathrm{tr}(V_i\delta\rho V_i^\dagger)}\right)
\end{aligned}$$

definiert man:

$$\Lambda_{i\alpha} \equiv \frac{\Lambda_\alpha\mathrm{tr}(V_iP_\alpha V_i^\dagger)}{\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}, \tag{7.2}$$

$$\Lambda_i \equiv \frac{\Lambda_{BSA}\mathrm{tr}(V_i\rho_s^* V_i^\dagger)}{\mathrm{tr}(V_i\rho V_i^\dagger)}, \tag{7.3}$$

$$P_{i\alpha} \equiv \frac{V_iP_\alpha V_i^\dagger}{\mathrm{tr}(V_iP_\alpha V_i^\dagger)}, \tag{7.4}$$

$$\delta\rho_i \equiv \frac{V_i\delta\rho V_i^\dagger}{\mathrm{tr}(V_i\delta\rho V_i^\dagger)}. \tag{7.5}$$

Nun gilt folgender Zusammenhang:

$$\Lambda_{BSA}\mathrm{tr}(V_i\rho_s^* V_i^\dagger) = \mathrm{tr}(V_i\rho V_i^\dagger)\Lambda_i,$$

bzw. man erhält nach der Ausführung der Summe über i:

$$\Lambda_{BSA} = \sum_i \Lambda_i\mathrm{tr}(V_i\rho V_i^\dagger). \tag{7.6}$$

Dies wird später eine sehr nützliche Relation sein.

Lemma 7 : *Gegeben sei eine BSA-Zerlegung* $\rho = \Lambda_{BSA}\rho_s^* + (1-\Lambda_{BSA})\delta\rho$. *Dann erfüllt* $E(\rho) = (1-\Lambda_{BSA}(\rho))$ *die letzteren drei Eigenschaften eines Verschränktheitsmaßes.*

Beweis:

1. Für den Fall, daß ρ separabel ist, gilt $\Lambda_{BSA} = 1$ und damit $E(\rho) = 0$.

2. Lokale unitäre Transformationen ändern die BSA trivialerweise nicht.

3. Dies ist der schwierigste Teil. Es gilt, daß $\Lambda_{BSA} = \sum_i \Lambda_i \mathrm{tr}(V_i \rho V_i^\dagger)$(7.6) ist. Nun ist nach der POVM der Zustand durch $\rho_i = \Lambda_i \rho_{s_i} + (1 - \Lambda_i)\delta\rho_i$ gegeben. Allgemein muß Λ_i kein BSA-Parameter sein. Angenommen wird also, daß dies nicht der Fall ist. Daraus ergibt sich $\Lambda_{BSA} \leq \sum_i \Lambda_{BSA_i} \mathrm{tr}(V_i \rho V_i^\dagger)$ und damit aber auch $(1 - \Lambda_{BSA}) \geq \sum_i (1 - \Lambda_{BSA_i}) \mathrm{tr}(V_i \rho V_i^\dagger)$ $_{.q.e.d.}$

Somit wäre das Lemma bewiesen.$_{q.e.d.}$

Kapitel 8

Separabilität in $C^2 \times C^N$-Quantensystemen

8.1 Inhalt dieses Kapitels

Das folgende Kapitel beschäftigt sich mit $C^2 \otimes C^N$-Räumen ([51] und [52]). Die vorliegenden Resultate werden im letzten Kapitel für die Untersuchung von $C^2 \otimes C^2 \otimes C^N$-Zuständen benötigt.

8.2 Der Begriff der Unterstützung

Betrachtet man als Beispiel einen positiv definiten Operator ρ, welcher auf einen $C^2 \otimes C^2$-Raum wirkt, so kann man den Operator ρ trivialerweise immer in einen $C^2 \otimes C^4$-Raum einbetten. Dieser Operator wird dann nach der Einbettung in $C^2 \times C^4$ einen Kern besitzen, in dem sich Produktvektoren befinden. Anhand dieses Beispiels wird sofort klar, daß es für die Untersuchungen von $C^2 \times C^N$-Räumen von Nutzen ist, diese Produktvektoren loszuwerden und somit die Dimensionalität des zweiten Raumes zu verringern. Aus diesem Grund wird folgende Definition eingeführt:

Definition 12 : *Man sagt, daß der Dichteoperator ρ, welcher auf $C^2 \otimes C^N$ wirkt, auf $C^2 \otimes C^M$* **unterstützt** *wird, falls ein minimaler Unterraum $H \subseteq C^N$ existiert, so daß $R(\rho) \subseteq C^2 \otimes H$ ist, und H die Dimension M besitzt.*

Falls nun ein positiv definiter Operator ρ auf die obige Art und Weise unterstützt wird, folgt die Existenz von genau $N-M$ linear unabhängigen Vektoren $\{|f_i\rangle, i=1,2,\ldots,N-M\} \in C^N$, so daß $|ef,_i\rangle \in K(\rho)$ für alle $|e\rangle \in C^2$ ist.

Für die Untersuchung der Separabilität wird nun die im letzten Kapitel vorgestellte Methode verwendet, welche Produktvektoren aus dem Bild von ρ abzieht, so daß sowohl ρ als auch ρ^{t_A} positiv definit bleiben. Es werden sowohl an ρ als auch an ρ^{t_A} Bedingungen gegeben, bei welchen nach einer endlichen Anzahl von Subtraktionen kein Rest mehr verbleibt. Damit wäre dann die Separabilität bewiesen. Um diese Bedingungen zu liefern, müssen sowohl der Bildbereich als auch der Kern von ρ genauer untersucht werden.

8.3 Subtraktion von Produktvektoren

Aus dem Kapitel über die PPT-BSA wissen wir, daß die maximale Kontribution λ, die man anwenden muß, um einen Projektor $|e,f\rangle\langle e,f|$ von ρ abziehen zu können, durch $\lambda = \min(\lambda_0, \tilde{\lambda}_0)$ gegeben ist, wobei $\lambda_0 = \frac{1}{\langle e,f|\rho^{-1}|e,f\rangle}$ und $\tilde{\lambda}_0 = \frac{1}{\langle e^*,f|(\rho^{t_A})^{-1}|e^*,f\rangle}$ ist. Die Differenz ist dann gegeben durch

$$\tilde{\rho} = \rho - \lambda|e,f\rangle\langle e,f|. \tag{8.1}$$

Wenn es um die Untersuchung von $C^2 \otimes C^N$-Systemen geht, ist nun folgendes Lemma für den weiteren Verlauf von zentraler Bedeutung.

Lemma 8 : *Sei* $|ef\rangle \in R(\rho)$ *und* $|e^*,f\rangle \in R(\rho^{t_A})$. *Dann gilt:*

1. *Falls* $\lambda = \lambda_0 < \tilde{\lambda}_0$, *dann ist* $r(\tilde{\rho}) = r(\rho) - 1$ *und* $r(\tilde{\rho}^{t_A}) = r(\rho^{t_A})$.
2. *Falls* $\lambda = \tilde{\lambda}_0 < \lambda_0$, *dann ist* $r(\tilde{\rho}) = r(\rho)$ *und* $r(\tilde{\rho}^{t_A}) = r(\rho^{t_A}) - 1$.
3. *Falls* $\lambda = \lambda_0 = \tilde{\lambda}_0$, *dann ist* $r(\tilde{\rho}) = r(\rho) - 1$ *und* $r(\tilde{\rho}^{t_A}) = r(\rho^{t_A}) - 1$.

Beweis: Es reicht, den ersten Teil des Lemmas zu beweisen. Für die anderen kann man die gleiche Argumentation anwenden. Als erstes bemerkt man, daß afgrund der Differenz um einen Projektor $r(\tilde{\rho}) \geq r(\rho) - 1$ sein muß. Andererseits muß $K(\rho) \subseteq K(\tilde{\rho})$ gelten, da für ein $|\Psi\rangle \in K(\rho)$ gilt, daß $\tilde{\rho}|\Psi\rangle = -\lambda_0\langle e,f|\Psi\rangle = 0$, weil $|e,f\rangle \in R(\rho)$. Desweiteren ist aber $\rho^{-1}|e,f\rangle$ nicht in $K(\rho)$ aber dafür in $K(\tilde{\rho})$ enthalten, wie man durch Substitution leicht nachprüfen kann. $_{q.e.d.}$

Der Vorteil dieses Lemmas ist, daß man durch maximales PPT-Abziehen die Dimension der Bilder verringern kann. Im nächsten Abschnitt wird bewiesen, daß

man durch diesen Sachverhalt das Problem der Separierbarkeit sukzessiv vereinfachen kann. Das ganze Problem reduziert sich der Differenz immer um eine Dimension, ohne die Eigenschaft der Separabilität zu ändern. Man verlagert somit das Problem auf kleinere Dimensionen, bis die Separabilität gezeigt werden kann.

8.4 Der Kern von ρ

Dieser Abschnitt behandelt, unter welchen Umständen man durch geschicktes Abziehen von Produktvektoren das Problem von $C^2 \otimes C^N$ auf $C^2 \otimes C^{N-1}$ verlagern kann. Dabei sind folgende zwei Lemmas hilfreich:

Lemma 9 : *Sei ρ ein PPT-Zustand. Dann gilt $|e^*, f\rangle \in K(\rho^{t_A})$, falls $|e, f\rangle \in K(\rho)$.*

Beweis: Es sei $\rho|e, f\rangle = 0$. Dann folgt, daß $\langle e, f|\rho|e, f\rangle = \langle e^*, f|\rho^{t_A}|e^*, f\rangle = 0$ ist. Da nun $\rho^{t_A} \geq 0$, folgt, daß $\rho^{t_A}|e^*, f\rangle = 0$ ist. Für die andere Richtung gilt dies dementsprechend genauso.$_{q.e.d.}$

Lemma 10 : *Gegeben sei ein PPT-Zustand ρ. Falls $|e, f\rangle \in K(\rho)$, dann ist entweder:*

1. *$|\hat{e}, f\rangle \in K(\rho)$ oder*
2. *es existiert ein Vektor $|g\rangle \in C^N$, so daß $\rho|\hat{e}, f\rangle = |\hat{e}, g\rangle$ und $\rho^{t_A}|\hat{e}^*, f\rangle = |e^*, g\rangle$ gilt.*

Beweis: Laut des letzten Lemmas folgt, daß $|e^*, f\rangle \in K(\rho^{t_A})$ ist. Daher gilt

$$0 = \langle \hat{e}^*, h|\rho^{t_A}|e^*, f\rangle = \langle e, h|\rho|\hat{e}, f\rangle \tag{8.2}$$

für alle $|h\rangle \in C^N$. Nun muß entweder $\rho|\hat{e}, f\rangle = 0$ sein oder $\rho|\hat{e}, f\rangle = |\hat{e}, g_1\rangle$ für ein $|g_1\rangle \in C^N$. Analog gilt dies auch für $|e, f\rangle \in K(\rho)$, wobei entweder $\rho^{t_A}|\hat{e}, f\rangle = 0$ oder $\rho^{t_A}|\hat{e}^*, f\rangle = |\hat{e}^*, g_2\rangle$ für ein $|g_2\rangle \in C^N$ gilt. Bleibt nur noch zu zeigen, daß $|g_1\rangle = |g_2\rangle$ gilt.

Nutzt man die Orthonormalität von $|e\rangle$ und $|\hat{e}\rangle$, so erhält man

$$|g_1\rangle = \langle \hat{e}|\rho|\hat{e}, f\rangle = \langle \hat{e}^*|\rho^{t_A}|\hat{e}^*, f\rangle = |g_2\rangle_{\cdot q.e.d.} \tag{8.3}$$

Für den Fall, daß der erste Teil des letzteren Lemmas eintritt, weiß man, daß ρ auf einen kleineren Raum $C^2 \otimes C^M$ mit $M < N$ unterstützt wird, weil $|e, f\rangle \in K(\rho)$

für alle $|e\rangle \in C^2$ gilt. Dies ist ein trivialer Fall, welchen wir nicht zu besprechen brauchen, und deshalb setzen wir von nun an voraus, daß ρ auf dem gesamten Raum $C^2 \otimes C^N$ unterstützt wird. In diesem Fall folgt aus den letzteren beiden Lemmas die Existenz eines Produktvektors, welchen man von ρ abziehen kann, ohne die Positivität der Differenz von ρ und ρ^{t_A} zu ändern.

Lemma 11 : *Falls ρ auf $C^2 \otimes C^N$ unterstützt wird und ein Produktvektor in $K(\rho)$ existiert, dann ist $\rho = \tilde{\rho} + \rho_s$, wobei ρ_s ein Projektor auf einen Produktvektor ist, und es gilt:*

1. *$r(\tilde{\rho}) = r(\rho) - 1$ und $r(\tilde{\rho}^{t_A}) = r(\rho^{t_A}) - 1$.*
2. *$\tilde{\rho}$ wird auf $C^2 \otimes C^{N-1}i$ unterstützt.*
3. *$\tilde{\rho}$ ist separabel, falls ρ separabel ist.*

Beweis: Aus der Existenz von $|e, f\rangle \in K(\rho)$ folgt aus Lemma (10), daß

$$\begin{aligned} \rho|\hat{e}, f\rangle &= |\hat{e}, g\rangle \\ \rho^{t_A}|\hat{e}^*, f\rangle &= |\hat{e}^*, g\rangle. \end{aligned}$$

Daraus folgert man, daß man den Produktvektor $|\hat{e}, g\rangle$ so von ρ abziehen kann, daß $\tilde{\rho} = \rho - \rho_s \geq 0$ gilt, wobei $\rho_s = \lambda|\hat{e}, g\rangle\langle\hat{e}, g|$ und

$$\begin{aligned} \lambda &= \lambda_0 = \frac{1}{\langle\hat{e}, g|\rho^{-1}|\hat{e}, g\rangle} = \frac{1}{|||\hat{e}\rangle||^2\langle g|f\rangle} \\ &= \frac{1}{\langle\hat{e}^*, g|(\rho^{t_A})^{-1}|\hat{e}^*, g\rangle} = \tilde{\lambda}_0. \end{aligned}$$

Aus Lemma (10) folgt dann, daß der Rang von ρ und ρ^{t_A} gleichzeitig um eine Dimension verringert wurde, was dann Punkt (1) beweist. Da nun $|\hat{e}, f\rangle, |e, f\rangle \in K(\tilde{\rho})$ gilt, folgt wiederum, daß $\tilde{\rho}$ auf einem kleineren Raum $C^2 \otimes C^M$ unterstützt wird, wobei $M < N$ gilt.

Nun wird gezeigt, daß $M = N - 1$ gilt. Man nehme an, daß M noch kleiner wäre. Dann würde ein $|h\rangle$ existieren, welches orthogonal auf $|f\rangle$ wäre, so daß $|e, h\rangle, |\hat{e}, h\rangle \in K(\tilde{\rho})$ gälte. In diesem Fall würde das bedeuten, daß $\rho|e, h\rangle = 0$ und $\rho|\hat{e}, h\rangle = c|\hat{e}, g\rangle$, wobei c eine Konstante wäre. Definiert man nun $|f'\rangle = c|f\rangle - |h\rangle \neq 0$, würde man erhalten, daß $|e, f'\rangle, |\hat{e}, f'\rangle \in K(\rho)$ liegen würde, was ein Widerspruch zur Annahme wäre, daß ρ auf $C^2 \otimes C^N$ unterstützt wäre, was wiederum Punkt (2) beweist.

Bleibt noch Punkt (3). Falls $\tilde{\rho}$ separabel ist, ist auch ρ separabel. Umgekehrt folgt, falls ρ separabel ist, kann man ρ schreiben als:

$$\rho = \sum_i |e_i, f_i\rangle\langle e_i, f_i| + |\hat{e}\rangle\langle\hat{e}| \otimes \eta,$$

wobei $\langle f|f_i\rangle = 0$ für alle i und η ein positiver Operator ist, welcher auf C^N wirkt. Verlangt man nun, daß $|\hat{e}, g\rangle = \rho|\hat{e}, f\rangle$ gilt, so erhält man $|g\rangle = |||\hat{e}\rangle||^2\eta|f\rangle$ und deshalb $|g\rangle \in R(\eta)$. Man schreibt

$$\tilde{\rho} = \sum_i |e_i, f_i\rangle\langle e_i, f_i| + |\hat{e}\rangle\langle\hat{e}| \otimes (\eta - \lambda_0|g\rangle\langle g|). \tag{8.4}$$

Nun ist aber

$$\eta - \frac{1}{\langle g|f\rangle}|g\rangle\langle g| = \eta - \frac{1}{\langle g|\eta^{-1}|g\rangle}|g\rangle\langle g|. \tag{8.5}$$

Da also dieser Operator positiv ist, folgt, daß ρ separabel sein muß.$_{q.e.d.}$

Das letztere Lemma ist von besonderer Wichtigkeit. Es besagt, daß wenn ein Produktvektor im Kern von ρ liegt, man das Problem der Separabilität auf $\tilde{\rho}$ reduzieren kann, ohne dabei die separable Eigenschaft zu ändern. Wir können von nun an annehmen, daß sich kein Produktvektor mehr im Kern von ρ befindet.

8.5 Das Bild von ρ

In diesem Abschnitt wird das Bild von ρ und ρ^{t_A} nach Produktvektoren untersucht. Dabei kann angenommen werden, daß sich keine Produktvektoren mehr im Kern befinden. Für den weiteren Verlauf der Untersuchungen definiert man nun $\{|\psi_i^1\rangle, i = 1, \ldots, k(\rho)\}$ und $\{|\psi_i^2\rangle, i = 1, \ldots, k(\rho^{t_A})\}$ als die Basis von $K(\rho)$ und $K(\rho^{t_A})$. Es folgt:

Lemma 12 : *Falls kein Produktvektor von ρ im Kern existiert, sind $\{\langle e|\psi_i^1\rangle\}$ und $\{\langle e^*|\psi_i^2\rangle\}$ für alle $|e\rangle \in C^2$ linear unabhängige Vektoren in C^N.*

Beweis: Zuerst wird gezeigt, daß $\langle e|\rho|e\rangle$ invertierbar sein muß. Angenommen, $\langle e|\rho|e\rangle$ sei nicht invertierbar. Dann existiert ein $|h\rangle$, so daß $0 = \langle h|\langle e|\rho|e\rangle|h\rangle$ gilt. Dies bedeutet aber, daß wegen $\rho \geq 0$ ein Produktvektor im Kern liegen würde, was ein Widerspruch zur Annahme wäre. Also ist $\langle e|\rho|e\rangle$ invertierbar. Nun definiert man eine Basis $\{|e\rangle, |\hat{e}\rangle\}$ in C^2 und schreibt die Kernvektoren von ρ als:

$$|\psi_i^1\rangle = |e, \psi_i^e\rangle + |\hat{e}, \psi_i^{\hat{e}}\rangle. \tag{8.6}$$

Nutzt man aus, daß dies Vektoren im Kern von ρ sind, so erhält man

$$|\psi_i^{\hat{e}}\rangle = -\frac{1}{\langle\hat{e}|\rho|\hat{e}\rangle}\langle\hat{e}|\rho|e\rangle|\psi_i^e\rangle. \tag{8.7}$$

Setzt man dies in die Definition von $|\psi_i^1\rangle$ ein, so erhält man

$$|\psi_i^1\rangle = \left(I + |\hat{e}\rangle\frac{1}{\langle\hat{e}|\rho|\hat{e}\rangle}\langle\hat{e}|\rho\right)|e,\psi_i^e\rangle. \tag{8.8}$$

Daraus folgt dann deren lineare Unabhängigkeit. Die gleiche Argumentation gilt auch für die Kernvektoren von ρ^{t_A}.*q.e.d.*

Im weiteren Verlauf sind $\{|0\rangle,|1\rangle\}$ und $\{|0\rangle,\ldots,|N\rangle\}$ orthonormale Basen in C^2 und C^N.

Lemma 13 : *Jeder Unterraum $H \subseteq C^2 \otimes C^N$ mit $dim(H) = M > N$ enthält unendlich viele Produktvektoren und für $M = N$ mindestens einen Produktvektor.*

Beweis: $\{|\Psi_i\rangle, i = 1,\ldots,2N-M\}$ sei eine Basis des orthogonalen Komplementes von H. Nun läßt sich $|\Psi_i\rangle$ schreiben als:

$$|\Psi_i\rangle = \sum_{k=1}^{N}[A_{i,k}|0k\rangle + B_{i,k}|1k\rangle], \tag{8.9}$$

wobei $A_{i,k}$ und $B_{i,k}$ $(2N-M)\times N$ Matrizen sind. Der Produktvektor $|e,f\rangle$ wird geschrieben als:

$$|e,f\rangle = (\alpha|0\rangle_A + |1\rangle_A)\otimes\sum_k f_k|k\rangle_B. \tag{8.10}$$

Fordert man nun für alle i, daß $|e,f\rangle$ orthogonal auf $|\Psi_i\rangle$ ist, so erhält man $(\alpha A^* + B^*)\vec{f} = 0$ als Gleichung für $\vec{f}$. Ist nun $M > N$, so gibt es unendlich viele nichttriviale Lösungen. Für $M = N$ existiert eine nichttriviale Lösung, falls $\det(\alpha A^* + B^*) = 0$ gilt. Dies ist eine polynomiale Gleichung für α, welche immer eine Lösung besitzt.*q.e.d.*

Korollar 1 : *Jeder Unterraum $H \subseteq C^2 \otimes C^N$ mit* $\dim(H) = M > N$ *besitzt unendlich viele Produktvektoren von der Form $|e_r,f\rangle$, wobei $|e_r\rangle = |e_r^*\rangle$ gilt.*

Nun ist es wichtig, zu wissen, wann es einen Produktvektor $|e,f\rangle \in R(\rho)$ gibt, so daß auch $|e^*,f\rangle \in R(\rho^{t_A})$ liegt. Zu diesem Zweck werden im nächsten Lemma Bedingungen dafür formuliert.

Lemma 14 : *Gegeben seien die Unterräume $H_1, H_2 \in C^2 \otimes C^N$ mit der Dimension $dim(H_{1,2}) = M_{1,2}$, wobei $\{|\Psi^{1,2}_{i_{1,2}}\rangle, i_{1,2} = 1,\ldots,2N - M_{1,2}\}$ gleichzeitig eine Basis der orthogonalen Komplemente von $H_{1,2}$ ist. Dann gilt:*

1. *Falls $M_1 + M_2 > 3N$ ist, existieren unendlich viele Produktvektoren $|e, f\rangle \in H_1$, so daß $|e^*, f\rangle \in H_2$;*

2. *Falls $M_1 + M_2 \leq 3N$ ist, existiert ein Produktvektor $|e, f\rangle \in H_1$, so daß $|e^*, f\rangle \in H_2$* **vorausgesetzt**, *daß man ein α finden kann, so daß maximal $N-1$ linear unabhängige Vektoren $\{\alpha\langle\Psi^1_i|0\rangle + \langle\Psi^1_i|1\rangle, \alpha^*\langle\Psi^2_{i_1}|0\rangle + \langle\Psi^2_{i_2}|1\rangle\}$ existieren.*

Beweis: Gegeben sei die Basis

$$|\Psi^{1,2}_i\rangle = \sum_k [A^{1,2}_{i,k}|0k\rangle + B^{1,2}_{ik}|1k\rangle], \tag{8.11}$$

wobei $A^{1,2}_{i,k}$ und $B^{1,2}_{ik}$ $(2N - M_{1,2})$ Matrizen sind. Verlangt man nun für alle Indizes die Orthogonalität $\langle e, f|\Psi^1_i\rangle = 0$ und $\langle e^*, f|\Psi^2_i\rangle = 0$, so gelangt man zu folgendem Gleichungssystem:

$$[\alpha(A^1)^* + (B^1)^*]\vec{f} = 0 \tag{8.12}$$

$$[\alpha^*(A^2)^* + (B^2)^*]\vec{f} = 0, \tag{8.13}$$

welches für $\vec{f}$ als $4N - M_1 - M_2$ Gleichungen angesehen werden kann. Für $M_1 + M_2 > 3N$ hat man weniger Gleichungen als Unbekannte, und deshalb existieren für alle α Lösungen. Ist nun $M_1 + M_2 \leq 3N$, dann existieren nur dann nichttriviale Lösungen, wenn der Rang der Matrix $M(\alpha, \alpha^*)$, welche aus den $\alpha(A^1)^* + (B^1)^*$ und $\alpha^*(A^2)^* + (B^2)^*$ zusammengesetzt ist, kleiner ist als N. Dies ist äquivalent zur Aussage im Lemma.$_{q.e.d.}$

8.6 Resultate

Lemma 15 : *Falls ρ auf $C^2 \otimes C^N$ unterstützt wird, ist $r(\rho) \geq N$.*

Beweis: Man nehme an, daß $r(\rho) < N$ ist. Dann folgt, daß $K(\rho)$ eine Dimension besitzt, welche größer ist als N, und es enthält deshalb einen Produktvektor. Aus diesem Grund erhält man einen Operator $\tilde{\rho}_1$, welcher auf $C^2 \otimes C^{N-1}$ unterstützt wird. Nun hat aber $K(\tilde{\rho}_1)$ eine Dimension, welche größer ist als $N-1$. Deshalb existiert wiederum ein Operator $\tilde{\rho}_2$, welcher auf $C^2 \otimes C^{N-2}$ unterstützt wird. Man

führt diese Prozedur sukzessiv weiter fort, bis man an einem Zustand $\tilde{\rho}_{N-1}$ angelangt ist, welcher auf $C^2 \otimes C^1$ unterstützt wird und $r(\tilde{\rho}_{N-1}) < 1$ besitzt, was natürlich unmöglich ist.$_{q.e.d.}$

8.6.1 Der PPT-Zustand mit $r(\rho) = N$

Dieses Unterkapitel ist besonders wichtig, da wir über $C^2 \otimes C^2 \otimes C^N$-Zustände diskutieren werden.

Theorem 10 : *Wird ρ auf $C^2 \otimes C^N$ unterstützt, und ist $r(\rho) = N$, dann ist ρ separabel.*

Beweis: Den Beweis erhält man über vollständige Induktion. Für $N = 1$ ist die Aussage wahr. Angenommen wird nun, daß die Aussage für $N-1$ wahr sei. Nun sei ρ auf $C^2 \otimes C^N$ unterstützt. Dann hat $K(\rho)$ die Dimension N und deshalb einen Produktvektor $|e, f\rangle$. Es folgt, daß ρ separabel ist, falls $\tilde{\rho}$ separabel ist. $\tilde{\rho}$ ist aber auf $C^2 \otimes C^{N-1}$ unterstützt und hat den Rang $N-1$. Laut Induktionsannahme ist dieser aber separabel und somit auch ρ.$_{q.e.d.}$

Korollar 2 : *Ist ρ auf $C^2 \otimes C^N$ unterstützt, und $r(\rho) = N$, dann ist $r(\rho^{t_A}) = N$.*

Korollar 3 : *Wird ρ auf $C^2 \otimes C^N$ unterstützt und ist es nicht separabel, dann ist $r(\rho) > N$.*

8.6.2 Der PPT-Zustand mit $r(\rho) + r(\rho^{t_A}) \leq 3N$

Es wird angenommen, daß $r(\rho), r(\rho^{t_A}) > N$ sind. Nun sei $H_1 = R(\rho)$ und $H_2 = R(\rho^{t_A})$. Jetzt kann man herausfinden, wie viele Produktvektoren gleichzeitig im Rang von ρ und ρ^{t_A} liegen. Das Problem reduziert sich auf Nullstellensuche von Polynomen in α und α^*. Im Anhang wird beschrieben, wie man feststellen kann, wie viele maximale Lösungen es für den Fall, daß das Polynom generisch ist, geben kann. Ist die Anzahl der Produktvektoren kleiner als das Minimum von $r(\rho)^2$ und $r(\rho^{t_A})^2$, dann hat man ein hinreichendes Kriterium für die Separabilität.

Es wird nun gezeigt, daß man für den Fall, daß $N \leq 10$ gilt, für ein generisches ρ immer Produktvektoren finden kann, so daß deren Anzahl kleiner ist als das Minimum von $r(\rho)$ und $r(\rho^{t_A})$. O.B.d.A. kann man annehmen, daß $k(\rho) = X \geq k(\rho^{t_A}) = Y$. Ebenso wird natürlich auch angenommen, daß kein Produktvektor im Kern von ρ liegt, weil ansonsten das Problem auf $C^2 \otimes C^N$ reduziert werden kann.

Es ist also $N > X \geq Y > 0$ und $X+Y \geq N$. Nun werden zwei Fälle separat betrachtet (s. Anhang A):

1. $X+Y=N$**:** Dann muß $0 < X \leq [N/2]$ sein, wobei $[N]$ den ganzzahligen Anteil von N bedeutet. Aus dem Anhang folgt, daß es nicht mehr polynomiale Lösungen geben kann als $2^{X-1}[N^2+(N-X)^2-X(N-X)]$. Dies sollte nicht größer sein als $(N+X)^2$. Für $N \leq 10$ ist dies immer erfüllt.

2. $X+Y \geq N$**:** In diesem Fall hat man $[(N+1)/2] \leq Y \leq N]$. Man erhält also zwei polynomiale Gleichungen vom Grade $N-Y$ in α und Y in α^*. Die Anzahl der Lösungen kann also nicht größer werden als $(2N-Y)^2$. Die zwei Polynome können zu einem Polynom vom Grade $2^{N-Y}Y$ gebracht werden. Die Anzahl der Lösungen sollte also nicht größer werden als $(2N-Y)^2$, was immer der Fall für $N \leq 10$ ist.

8.6.3 Der PPT-Zustand $r(\rho)+r(\rho^{t_A}) \geq 3N$

In diesem Fall existiert immer ein Produktvektor, welchen man von ρ abziehen kann. Durch sukzessives Abziehen wird man dann zum Fall $r(\rho)+r(\rho^{t_A}) \leq N$ geführt. Dort einmal angekommen, kann man die gleiche Prozedur durchführen, um die Separabilität festzustellen.

Wir sahen, daß sich sämtliche Bedingungen ausschließlich auf die Dimensionalität der Bildbereiche von ρ und ρ^{t_A} stützen. Natürlich gibt es einen Zusammenhang zwischen diesen beiden Größen, welcher durch die partielle Transposition gegeben ist. Dieser ist aber explizit von der Struktur der Dichtematrizen abhängig und deshalb außerordentlich komplex. Aus diesem Grund sind mathematische Untersuchungen solcher Zusammenhänge von enormem Interesse, weil sie weitere Bedingungen an die Multipolynomialgleichungen stellen und dadurch weitere Informationen über die Separabilität liefern. Nichtsdestotrotz gibt es einen Zusammenhang, der sich sehr leicht formulieren läßt. Dies ist der Fall, wenn der Zustand unter einer partiellen Transposition bezüglich Alices Basis invariant ist. Im nächsten Abschnitt wird darauf eingegangen.

8.7 Invarianz unter partieller Transposition

Das folgende Theorem beweist, daß wenn ein $C^2 \otimes C^N$-Zustand unter einer partiellen Transposition bezüglich Alices Basis invariant ist, er dann auch separabel ist. Dadurch wird besonders deutlich, wie wichtig es ist, die Zusammenhänge zwischen den jeweiligen Bildbereichen von ρ und ρ^{t_A} zu kennen.

Theorem 11 : *Falls* $\rho = \rho^{t_A}$ *ist, ist* ρ *separabel.*

Beweis: Den Beweis erhält man über vollständige Induktion. Ist ρ auf $C^2 \otimes C^1$ unterstützt, so ist dies offensichtlich wahr. Nun wird angenommen, daß dies auch für ein auf $C^2 \otimes C^{N-1}$ unterstützbares ρ wahr ist. Falls nun $r(\rho) = N$ ist, so ist ρ bereits separabel. Nun soll $r(\rho) > N$. Dann existiert ein Produktvektor $|e_r, g\rangle$ mit $|e_r, g\rangle = |e_r^*, g\rangle$. Nun kann man diesen abziehen, und man erhält einen Operator, welcher auf $C^2 \otimes C^{N-1}$ wirkt und zusätzlich unter partieller Transposition invariant ist. Dieser ist aber nach Induktiosannahme schon separabel, also gilt das Theorem.$_{q.e.d.}$

Man beachte an dieser Stelle, daß man auch eine andere Basis für die partielle Transposition hätte wählen können. Da die Separabilität nicht von lokalen invertierbaren Transformationen auf C^2 abhängig ist, erhält man:

Korollar 4 : *Ist* $[(A \otimes I)\rho(A \otimes I)^\dagger]^{t_A} = (A \otimes I)\rho(A \otimes I)^\dagger$ *für einen nicht singulären Operator A, dann ist* ρ *separabel.*

Aus dem letzten Theorem gewinnt man nun den Eindruck, daß wenn ρ nicht zu sehr von ρ^{t_A} unterschiedlich ist, es dann separabel sein sollte. Dies wird sich in Kürze als wahr erweisen und somit eine sehr starke Bedingung für die Separabilität liefern. Bevor dies aber gezeigt wird, müssen noch einige Größen definiert werden.

Ein $C^2 \otimes C^N$-Zustand ρ kann immer geschrieben werden als:

$$\rho = \frac{\rho + \rho^{t_A}}{2} + \frac{\rho - \rho^{t_A}}{2} \equiv \rho_s + \sigma_y^A \otimes B. \tag{8.14}$$

Dabei ist $\rho_s = \frac{\rho + \rho^{t_A}}{2}$, $\sigma_y^A = i(|0\rangle\langle 1| - |1\rangle\langle 0|)_A$ und $4B = 4B^\dagger = \mathrm{tr}_A[\sigma_y^A(\rho - \rho^{t_A})]$. Der Operator B besitzt die spektrale Zerlegung

$$B = \sum_i^K \lambda_i |v_i\rangle\langle v_i|. \tag{8.15}$$

Nun kann man mit Hilfe der Spektralzerlegung $\{\lambda_i, |v_i\rangle\}_{i=1}^K$ und einer Menge von reellen Zahlen $\{a_i\}_{i=1}^K$ den folgenden Operator definieren:

$$C(a, \lambda, v) = \sum_{i=1}^K |\lambda_i|(a_i^2 |0\rangle\langle 0| + a_i^{-2} |1\rangle\langle 1|) \otimes |v_i\rangle\langle v_i|, \tag{8.16}$$

welcher positiv definit ist. Nun folgt

Theorem 12 :*Gegeben sei eine Spektraldarstellung* $\{\lambda_i, |v_i\rangle\}_{i=1}^K$ *von B und eine Menge von reellen Zahlen* $\{a_i\}_{i=1}^K$. *Ist nun* $||C^{1/2}(a,\lambda,v)\rho_s^{-1/2}||^2 \leq 1$, *dann ist* ρ *separabel.*

Beweis: Definiert wird der separable Zustand $\tilde{\rho}_s = \rho_s - C(a,\lambda,v) = \tilde{\rho}_s^{t_A} \geq 0$. Sei nun $|w_i\rangle = a_i|0\rangle - ia_i^{-1}\text{sign}(\lambda_i)|1\rangle$. Jetzt ist es leicht, nachzuprüfen, daß

$$\rho = \tilde{\rho}_s + \sum_{i=1}^{K} |\lambda_i|\, w_i, v_i\rangle\langle w_i, v_i\,|. \tag{8.17}$$

Dies beweist die Separabilität von ρ.$_{q.e.d.}$

Es ergibt sich nun folgendes Korrollar.

Korollar 5 : *Ist* $\rho + \rho^{t_A}$ *von vollem Rang,* $||(\rho+\rho^{t_A})^{-1}|| \leq 1$ *und* $||(\rho-\rho^{t_A})^{-1}|| \leq 1$, *dann ist* ρ *separabel.*

Daraus ergibt sich, daß wenn ρ von vollem Rang und nahe an ρ^{t_A} ist, es dann auch separabel ist. Dies ist eine wichtige Erkenntnis über die geometrische Struktur von separablen Zuständen.

8.8 Beispiel: $C^2 \otimes C^4$

In diesem Unterkapitel werden die aus den letzten Abschnitten entwickelten Methoden für den $C^2 \otimes C^4$-Fall vorgestellt. Desweiteren werden die Resultate aus diesem Abschnitt später für die Untersuchungen von $C^2 \otimes C^2 \otimes C^2$ verwendet.

Angenommen wird natürlich, daß $C^2 \otimes C^4$ keine Produktvektoren im Kern enthält. Hätte man Produktvektoren, so könnte man das ganze Problem auf $C^2 \otimes C^3$ reduzieren, und dort wäre der Zustand ja schon separabel. Ebenso ist $r(\rho), r(\rho^{t_A}) > 4$, da man andernfalls auch auf die Separabilität schließen könnte. Betrachtet werden in diesem Unterkapitel:

- $r(\rho) = r(\rho^{t_A}) = 5$
- $r(\rho) + r(\rho^{t_A}) \leq 12$
- $r(\rho) = r(\rho^{t_A}) = 6$

Wie üblich sind $\{|\Psi_i^1\rangle, i=1\ldots,k(\rho)\}$ und $\{|\Psi_i^2\rangle, i=1\ldots,k(\rho^{t_A})\}$ Basen von $K(\rho)$ und $K(\rho^{t_A})$. Es existiert nach Lemma ein Produktvektor $|e,f\rangle$ in $R(\rho)$, so daß $|e^*,f\rangle$ in $K(\rho^{t_A})$ liegt. Falls ein α existiert, erhält man maximal zwei linear unabhängige Vektoren von der Form $\{\alpha\langle\Psi_{i_1}^1|0\rangle+\langle\Psi_{i_1}^1|1\rangle\}$ und $\{\alpha^*\langle\Psi_{i_2}^2|0\rangle+\langle\Psi_{i_2}^2|1\rangle\}$ (generischer Zustand).

8.8.1 Der Fall $r(\rho)=r(\rho^{t_A})=5$

Jeder der beiden Kerne besitzt Dimension 3. Zu lösen ist also die Gleichung $M(\alpha,\alpha^*)\,\vec{f}=0$, wobei

$$M(\alpha,\alpha^*)=\begin{pmatrix}\alpha\langle\Psi_1^1|0\rangle+\langle\Psi_1^1|1\rangle\\ \alpha\langle\Psi_2^1|0\rangle+\langle\Psi_2^1|1\rangle\\ \alpha\langle\Psi_3^1|0\rangle+\langle\Psi_3^1|1\rangle\\ \alpha^*\langle\Psi_1^2|0\rangle+\langle\Psi_1^2|1\rangle\\ \alpha^*\langle\Psi_2^2|0\rangle+\langle\Psi_2^2|1\rangle\\ \alpha^*\langle\Psi_3^2|0\rangle+\langle\Psi_3^2|1\rangle\end{pmatrix}$$

eine 6×4-Matrix ist. Nun muß M mindestens drei linear unabhängige Vektoren enthalten, damit ein Produktvektor im Rang existiert, so daß man ihn abziehen kann. Dies ist äquivalent zur Forderung, daß die folgenden drei Minoren aus M verschwinden:

$$\begin{aligned}\det_1(\alpha,\alpha^*) &= \det[M_1(\alpha,\alpha^*)]=0\\ \det_2(\alpha,\alpha^*) &= \det[M_2(\alpha,\alpha^*)]=0\\ \det_3(\alpha,\alpha^*) &= \det[M_3(\alpha,\alpha^*)]=0\end{aligned}$$

$M_{1,2,3}$ sind $4\times 4-$Matrizen, welche aus den letzten drei Zeilen von M und der ersten, zweiten und dritten Zeile geformt sind. Wie man leicht sieht, sind die Determinanten Polynome, welche linear in α und kubisch in α^* sind. Deshalb schreibt man nun

$$\begin{aligned}\det_1 &= \alpha P_3^1(\alpha^*)+P_3^0(\alpha^*)\\ \det_2 &= \alpha\tilde{P}_3^1(\alpha^*)+\tilde{P}_3^0(\alpha^*)\\ \det_3 &= \alpha\hat{P}_3^1(\alpha^*)+\hat{P}_3^0(\alpha^*),\end{aligned}$$

wobei der untere Index den Grad des Polynoms in α^* kennzeichnet. Nun betrachtet man α und α^* als unabhängige Variablen. Multipliziert man die erste Gleichung mit $\tilde{P}_3^1(\alpha^*)$ und die zweite Gleichung mit $P_3^1(\alpha^*)$ und subtrahiert diese voneinander, so erhält man eine polynomiale Gleichung in α^* vom Grade 6. Wiederholt man diese

Prozedur jetzt noch einmal mit der ersten und dritten Gleichung, so erhält man ein zweites Polynom vom Grade 6 in α^*. Durch geeignete Subtraktion dieser beiden Gleichungen erhält man ein Polynom vom Grade 5 in α^*. Dies bedeutet, daß es maximal 5 Produktvektoren geben kann.

8.8.2 Der Fall $r(\rho)+r(\rho^{t_A}) \leq 12$, wobei $r(\rho) \neq r(\rho^{t_A})$

In diesem Abschnitt werden die folgenden Fälle betrachtet:

- $r(\rho)=6$ und $r(\rho^{t_A})=5$ oder $r(\rho)=5$ und $r(\rho^{t_A})=6$
- $r(\rho)=7$ und $r(\rho^{t_A})=5$ oder $r(\rho)=5$ und $r(\rho^{t_A})=7$

Für den Fall, daß $r(\rho)=6$ und $r(\rho^{t_A})=5$, gilt $k(\rho)=3$ und $k(\rho^{t_A})=2$. Dieser Fall hat nur zwei Minoren. Durch die gleiche Prozedur wie im letzten Abschnitt erhält man ein Polynom vom Grade 6. Man hat also maximal 6 Produktvektoren.

Für den zweiten Fall gilt $k(\rho)=1$ und $k(\rho^{t_A})=3$. Daraus folgt nur ein Minor von der Form

$$0=\alpha P_3^1(\alpha^*)+P_3^0(\alpha^*).$$

Laut Anhang A folgt daraus ein Polynom vom Grade 10.

8.8.3 Der Fall $r(\rho)=r(\rho^{t_A})=6$

In diesem Fall hat man zwei Vektoren im Kern von ρ und ρ^{t_A}. Es muß also folgende Gleichung gelten:

$$\begin{aligned} 0 &= \det(M(\alpha,\alpha^*))=\alpha^2 P_2^2(\alpha^*)+\alpha P_2^1(\alpha^*)+P_2^0(\alpha^*) && (8.18)\\ &= (\alpha^*)^2 Q_2^2(\alpha)+\alpha^* Q_2^1(\alpha)+Q_2^0(\alpha). && (8.19)\end{aligned}$$

Komplex konjugiert man nun die erste Gleichung, erhält man:

$$\begin{aligned} (\alpha^*)^2 Q_2^2(\alpha)+\alpha^* Q_2^1(\alpha)+Q_2^0(\alpha) &= 0\\ (\alpha^*)^2 \tilde{Q}_2^2(\alpha)+\alpha^* \tilde{Q}_2^1(\alpha)+\tilde{Q}_2^0(\alpha) &= 0\end{aligned}$$

Die erste Gleichung wird nun mit $\tilde{Q}_2^2$ und die zweite mit Q_2^2 multipliziert und danach subtrahiert. Dann wird die erste Gleichung mit $\tilde{Q}_2^0$ und die zweite mit Q_2^0 multipliziert und danach subtrahiert. Danach dividiert man durch α^* und erhält:

$$\begin{aligned} \alpha^*[Q_2^1\tilde{Q}_2^2-Q_2^2\tilde{Q}_2^1]+Q_2^0\tilde{Q}_2^2-\tilde{Q}_2^0Q_2^2 &= 0 && (8.20)\\ \alpha^*[Q_2^2\tilde{Q}_2^0-\tilde{Q}_2^2Q_2^0]+Q_2^1\tilde{Q}_2^0-Q_0^2\tilde{Q}_2^1 &= 0. && (8.21)\end{aligned}$$

Multipiziert man die erste Gleichung mit $Q_2^2\tilde{Q}_2^0 - \tilde{Q}_2^2 Q_2^0$ und die zweite mit $Q_2^1\tilde{Q}_2^2 - Q_2^2\tilde{Q}_2^1$ und subtrahiert diese voneinander, so erhält man am Ende ein Polynom vom Grade 8. Dies kann bedeuten, daß sich die Zustände notwendigerweise nicht nur durch 6 Produktvektoren schreiben lassen.

8.8.4 Zusammenfassung

Die letzteren Beispiele weisen eine Möglichkeit auf, wie sich die Separabilität von PPT-Zuständen mit niedrigem Rang explizit nachprüfen läßt. Diese Methode wurde auch für $C^M \otimes C^N$-Zustände [103] verallgemeinert und wird im letzten Kapitel über $C^2 \otimes C^2 \otimes C^N$ noch einmal für weitere Untersuchungen benutzt. Dort werden ähnliche Bedingungen an die Ränge der Dichtematrizen gestellt und für den $C^2 \otimes C^2 \otimes C^2$-Fall genauer untersucht.

Kapitel 9

Dreifach zusammengesetzte Systeme

9.1 Inhalt dieses Kapitels

Für die Quanteninformationstheorie sind $C^2 \otimes C^2 \otimes C^N$-Systeme von besonderer Bedeutung, weil sie eine Kopplung zwischen zwei q-Bits und einem N-Niveau-System beschreiben (z.B. zwei q-Bits in einer Ionenfalle ([9], [10])). Mit solchen Systemen lassen sich komplexere Quantengatter (z.B. XOR [110]) beschreiben, die für Quantenrechner benutzt werden könnten.

Aus diesem Grund ist es wichtig, ausgiebig über die physikalische Struktur und die Eigenschaften von $C^2 \otimes C^2 \otimes C^N$ informiert zu sein. In diesem Kapitel untersuchen wir solche Systeme nach deren Separabilität.

9.2 $C^2 \otimes C^2 \otimes C^N$-Quantensysteme

In diesem Abschnitt wird eine kanonische Struktur für separable Zustände in $C^2 \otimes C^2 \otimes C^N$ mit $r(\rho) = N$ abgeleitet. Dadurch wird es möglich sein, die explizite Zerlegung nach Produktprojektoren zu erhalten. In weiterem Verlauf werden wie vereinbart die drei Teilräume nach Alice, Bob und Charlie benannt.

Lemma 16 : *Jede $C^2 \otimes C^2 \otimes C^N$-PPT-Dichtematrix ρ mit $r(\rho) = N$ und solch einer Basis, wo o.B.d.A. $r(\langle 1_A, 1_B | \rho | 1_A, 1_B \rangle = N$ gilt , kann durch eine reversible lokale*

Operation auf die folgende kanonische Form gebracht werden:

$$\rho = \sqrt{D}\begin{pmatrix} B^\dagger C^\dagger CB & B^\dagger C^\dagger C & B^\dagger C^\dagger B & B^\dagger C^\dagger \\ C^\dagger CB & C^\dagger C & C^\dagger B & C^\dagger \\ B^\dagger CB & B^\dagger C & B^\dagger B & B^\dagger \\ CB & C & B & 1 \end{pmatrix}\sqrt{D} \tag{9.1}$$

$$= \sqrt{D}\begin{pmatrix} B^\dagger C^\dagger \\ C^\dagger \\ B^\dagger \\ 1 \end{pmatrix}\begin{pmatrix} CB & C & B & 1 \end{pmatrix}\sqrt{D}, \tag{9.2}$$

wobei $[B,B^\dagger] = [C,C^\dagger] = [C,B] = [C,B^\dagger] = 0$ *und* $D = D^\dagger$ *gilt. Die B,C und D sind Operatoren in Charlies System.*

Beweis: Die Dichtematrix ρ wird geschrieben als:

$$\rho = \begin{pmatrix} E_1 & E_5 & E_6 & E_7 \\ E_5^\dagger & E_2 & E_8 & E_9 \\ E_6^\dagger & E_8^\dagger & E_3 & E_{10} \\ E_7^\dagger & E_9^\dagger & E_{10}^\dagger & E_4 \end{pmatrix},$$

wobei die E's $N \times N$-Matrizen sind. Nach einer Projektion $\tilde{\rho} = \langle 1_A |\rho| 1_A \rangle$ erhält man den Zustand

$$\tilde{\rho} = \begin{pmatrix} E_3 & E_{10} \\ E_{10}^\dagger & E_4 \end{pmatrix}.$$

Durch die reversible Filteroperation $\frac{1}{\sqrt{E_4}}$ auf Charlies Seite kann die Matrix $\tilde{\rho}$ geschrieben werden als:

$$\tilde{\rho} = \begin{pmatrix} A & B^\dagger \\ B & 1 \end{pmatrix}.$$

Diese läßt sich dann schreiben als $\tilde{\rho} = \Sigma + \mathrm{diag}[\Delta, 0]$, wobei $\Delta = A - B^\dagger B$ und

$$\Sigma = \begin{pmatrix} B^\dagger B & B^\dagger \\ B & 1 \end{pmatrix}.$$

$\tilde{\rho}$ muß nun Rang N besitzen. Dies ist für Σ durch die N Kernvektoren $|\phi_f\rangle = |1\rangle|f\rangle - |2\rangle B|f\rangle$ gewährleistet. Gezeigt wird, daß $\Delta = 0$ ist.

Die Dimension des Bildes von Σ ist $r(\Sigma) = N$. Wegen der Positivität von $\tilde{\rho}$ folgt, daß $\Delta \geq 0$ sein muß. Da aber $r(\tilde{\rho}) = r(\Sigma)$, gilt für die Bildbereiche, daß $R(\tilde{\rho}) = R(\Sigma) \supseteq R(\mathrm{diag}[\Delta, 0])$, also $K(\mathrm{diag}[\Delta, 0]) \supseteq K(\Sigma)$. Nun wird $K(\Sigma)$ von den Kernvektoren $|\phi_f\rangle = |1\rangle|f\rangle - |2\rangle B|f\rangle$ aufgespannt, für welche dann $\langle \phi_f |\mathrm{diag}[\Delta, 0]| \phi_f \rangle = 0$

gelten muß. Dies aber bedeutet, daß $\Delta|\,f\rangle = 0$ für alle $|\,f\rangle$ sein muß und deshalb ist $\Delta = 0$.

Die Normalität von B erhält man durch die Forderung, daß $\tilde{\rho}^{t_A}$ ein positiv definiter Operator ist. Diese Bedingung liefert, daß $BB^\dagger - B^\dagger B \geq 0$ gilt. Dieser positiv definite Operator besitzt aber die Spur Null und muß deshalb auch verschwinden, d.h. $[B, B^\dagger] = 0$.

Ebenso muss sich durch die Projektion $\langle 1_B|\rho|\,1_B\rangle$ aus gleichen Gründen die Matrix

$$\bar{\rho} = \begin{pmatrix} C^\dagger C^\dagger & C^\dagger \\ C & 1 \end{pmatrix}$$

mit $[C, C^\dagger] = 0$ ergeben. Man erhält nach der lokalen Filteroperation $\frac{1}{\sqrt{E_4}}$ folgende Form:

$$\bar{\rho} = \begin{pmatrix} E_1 & E_5 & E_6 & E_7 \\ E_5^\dagger & C^\dagger C & E_8 & C^\dagger \\ E_6^\dagger & E_8^\dagger & B^\dagger B & B \\ E_7^\dagger & C^\dagger & B & 1 \end{pmatrix}.$$

Es wird wieder $\rho \equiv \bar{\rho}$ gesetzt.

Nun soll ρ die Kernvektoren $|\,10\rangle|\,f\rangle - |\,11\rangle B|\,f\rangle$ und $|\,01\rangle|\,g\rangle - |\,11\rangle C|\,g\rangle$ für alle $|\,f\rangle, |\,g\rangle$ enthalten. Daraus egibt sich, daß $E_8 = C^\dagger B$, $E_6 = E_7 B$ und $E_5 = E_7 C$ sein muß. ρ hat nun die Form:

$$\rho = \begin{pmatrix} E_1 & E_7 C & E_7 B & E_7 \\ C^\dagger E_7^\dagger & C^\dagger C & C^\dagger C & C^\dagger \\ B^\dagger E_7^\dagger & B^\dagger C & B^\dagger B & B^\dagger \\ E_7^\dagger & C & B & 1 \end{pmatrix}.$$

Jetzt betrachten wir die partiell Transponierte bezüglich Alice, welche gegeben ist durch:

$$\rho^{t_A} = \begin{pmatrix} E_1 & E_7 C & B^\dagger E_7^\dagger & B^\dagger C \\ C^\dagger E_7^\dagger & C^\dagger C & E_7^\dagger & C^\dagger \\ E_7 B & E_7 & B^\dagger B & B^\dagger \\ C^\dagger B & C^\dagger & B & 1 \end{pmatrix}.$$

Da sich bezüglich $\langle 1_A|\rho|\,1_A\rangle$ nichts geändert hat, müssen die Kernvektoren $|\,10\rangle|\,f\rangle - |\,11\rangle B|\,f\rangle$ aufgrund der Positivität von ρ^{t_A} wieder enthalten sein. Dies liefert dann die Beziehung, daß $E_7 = B^\dagger C^\dagger$ ist. Nun hat ρ folgende Form:

$$\rho = \begin{pmatrix} E_1 & B^\dagger C^\dagger C & B^\dagger C^\dagger B & B^\dagger C^\dagger \\ C^\dagger C B & C^\dagger C & C^\dagger B & C^\dagger \\ B^\dagger C B & B^\dagger C & B^\dagger B & B^\dagger \\ C B & C & B & 1 \end{pmatrix}.$$

Diese kann aber auch geschrieben werden als:

$$\rho = \begin{pmatrix} B^\dagger C^\dagger CB & B^\dagger C^\dagger C & B^\dagger C^\dagger B & B^\dagger C^\dagger \\ C^\dagger CB & C^\dagger C & C^\dagger B & C^\dagger \\ B^\dagger CB & B^\dagger C & B^\dagger B & B^\dagger \\ CB & C & B & 1 \end{pmatrix} + \mathrm{diag}[\tilde{\Delta}, 0, 0, 0],$$

wobei $\Delta = E_1 - B^\dagger C^\dagger CB$ ist. Dies läßt sich schreiben als:

$$\rho = \begin{pmatrix} B^\dagger C^\dagger \\ C^\dagger \\ B^\dagger \\ 1 \end{pmatrix} \begin{pmatrix} CB & C & B & 1 \end{pmatrix} + \mathrm{diag}[\tilde{\Delta}, 0, 0, 0].$$

Der erste Teil von ρ ist PPT und besitzt die folgenden $3N$-Kernvektoren für alle $|f\rangle, |g\rangle$ und $|h\rangle$:

$$\begin{aligned} |\psi\rangle &= |00\rangle|f\rangle + |11\rangle CB|f\rangle \\ |\phi\rangle &= |01\rangle|g\rangle + |11\rangle C|g\rangle \\ |\chi\rangle &= |10\rangle|h\rangle + |11\rangle B|h\rangle. \end{aligned}$$

Nun folgt aus der vorherigen Überlegung zu Δ, daß $\tilde{\Delta}$ verschwinden muß, so daß letzten Endes ρ die Gestalt:

$$\rho = \begin{pmatrix} B^\dagger C^\dagger CB & B^\dagger C^\dagger C & B^\dagger C^\dagger B & B^\dagger C^\dagger \\ C^\dagger CB & C^\dagger C & C^\dagger B & C^\dagger \\ B^\dagger CB & B^\dagger C & B^\dagger B & B^\dagger \\ CB & C & B & 1 \end{pmatrix} \tag{9.3}$$

$$= \begin{pmatrix} B^\dagger C^\dagger \\ C^\dagger \\ B^\dagger \\ 1 \end{pmatrix} \begin{pmatrix} CB & C & B & 1 \end{pmatrix} \tag{9.4}$$

annimmt. Es bleibt noch, die Kommutatorrelationen $[B, C] = [B, C^\dagger] = 0$ zu zeigen. Dies geschieht bei der Ausnutzung der PPT auf allen Teilsystemen von ρ.

ρ^{t_A} läßt sich schreiben als:

$$\rho^{t_A} = \begin{pmatrix} B^\dagger C \\ C \\ B^\dagger \\ 1 \end{pmatrix} \begin{pmatrix} C^\dagger B & C^\dagger & B & 1 \end{pmatrix}, \tag{9.5}$$

was offensichtlich positiv definit ist.

Nun läßt sich ρ^{t_B} schreiben als:

$$\rho^{t_B} = \begin{pmatrix} B^\dagger C^\dagger CB & C^\dagger CB & B^\dagger C^\dagger B & C^\dagger B \\ B^\dagger C^\dagger C & C^\dagger C & B^\dagger C^\dagger & C^\dagger \\ B^\dagger CB & CB & B^\dagger B & B \\ B^\dagger C & C & B^\dagger & 1 \end{pmatrix}. \tag{9.6}$$

ρ^{t_A} muß wegen der PPT-Bedingung auch den Kernvektor $|01\rangle|g\rangle - |11\rangle C|g\rangle$ enthalten, so daß sich daraus die Kommutatorrelation $[C,B] = 0$ ergibt. ρ^{t_B} läßt sich somit schreiben als:

$$\rho^{t_B} = \begin{pmatrix} C^\dagger B \\ C^\dagger \\ B \\ 1 \end{pmatrix} \begin{pmatrix} B^\dagger C & C & B^\dagger & 1 \end{pmatrix}, \tag{9.7}$$

wodurch die Positivität gewährleistet wird. Bleibt noch $\rho^{t_{AB}}$.

Dieses läßt sich schreiben als:

$$\rho^{t_{AB}} = \begin{pmatrix} B^\dagger C^\dagger CB & C^\dagger CB & B^\dagger CB & CB \\ B^\dagger C^\dagger C & C^\dagger C & B^\dagger C & C \\ B^\dagger C^\dagger B & C^\dagger B & B^\dagger B & B \\ B^\dagger C^\dagger & C^\dagger & B^\dagger & 1 \end{pmatrix}. \tag{9.8}$$

Nun muß wiederum aus der Positivität von $\rho^{t_{AB}}$ folgen, daß $|10\rangle - |11\rangle B^\dagger |f\rangle$ ein Kernvektor ist, so daß sich die Kommutatorrellation $[B^\dagger, C] = 0$ ergibt. Damit läßt sich $\rho^{t_{AB}}$ schreiben als:

$$\rho^{t_{AB}} = \begin{pmatrix} CB \\ C \\ B \\ 1 \end{pmatrix} \begin{pmatrix} B^\dagger C^\dagger & C^\dagger & B^\dagger & 1 \end{pmatrix}. \tag{9.9}$$

Dieser Zustand ist wiederum positiv definit, so daß damit das Lemma bewiesen wäre.$_{q.e.d.}$

Nun läßt sich folgendes Lemma beweisen:

Lemma 17 : *Jeder PPT-Zustand* ρ *in* $C^2 \otimes C^2 \otimes C^N$, *welcher* $r(\rho) = N$ *und o.B.d.A. eine Produktbasis* $|e_A, f_B\rangle$ *besitzt, so daß* $r(\langle e_A, f_B|\rho|e_A, f_B\rangle) = N$ *beträgt, ist separabel.*

Beweis: Der Zustand ρ kann mit Zuhilfenahme des Lemmas (16) geschrieben werden als

$$\rho = \begin{pmatrix} B^\dagger C^\dagger \\ C^\dagger \\ B^\dagger \\ 1 \end{pmatrix} \begin{pmatrix} CB & C & B & 1 \end{pmatrix}. \tag{9.10}$$

Da nun alle Operatoren kommutieren, folgt daraus, daß es gemeinsame Eigenvektoren $|f_n\rangle$ gibt.

Daraus ergibt sich dann:

$$\langle f_n|\rho|f_n\rangle = \begin{pmatrix} b_n^* c_n^* \\ c_n^* \\ b_n^* \\ 1 \end{pmatrix} \begin{pmatrix} c_n b_n & c_n & b_n & 1 \end{pmatrix}. \tag{9.11}$$

Dies ist aber ein Produktzustand in Alices und Bobs Hilbertraum, so daß ρ als $\rho = \sum_{n=1}^{N} |\psi_n\rangle\langle\psi_n| \otimes |\phi_n\rangle\langle\phi_n| \otimes |f_n\rangle\langle f_n|$ geschrieben werden kann. Da nun die lokale Transformation, die man am Anfang angewendet hat, reversibel war, muß der Anfangszustand separabel gewesen sein. Somit wäre das Lemma bewiesen.$_{q.e.d.}$

Um nun zu beweisen, daß alle PPT-Zustände ρ mit $r(\rho) = N$, welche auf $C^2 \otimes C^2 \otimes C^N$ unterstützt werden, separabel sind, muß bewiesen werden, daß man eine Produktbasis finden kann, so daß o.B.d.A. $r(\langle e_A, f_B|\rho|e_A, f_B\rangle) = N$ gilt. Dies wird im weiteren Verlauf aber nicht geschehen. Stattdessen wird die Separabilität direkt bewiesen, woraus dann die angestrebte kanonische Form automatisch bewiesen ist. Zu diesem Zweck benutzt man die Resultate aus den vorherigen Kapiteln und das folgende Theorem [103].

Theorem 13 : *Alle Rang-N-PPT-Zustände* ρ *welche auf* $M \times N$ $(M \leq N)$ *unterstützt werden, besitzen eine Produktbasis, so daß o.B.d.A.* $r(\langle 1_A|\rho|1_A\rangle) = N$ *gilt und* ρ *separabel von der Form*

$$\rho = \sum_{i=1}^{N} |e_i, b_i\rangle\langle e_i, b_i| \tag{9.12}$$

ist, wobei alle $|b_i\rangle$ *linear unabhängig sind. Diese Zerlegung ist zusätzlich noch eindeutig.*

Das letztere Theorem kann nun für das folgende Lemma benutzt werden:

Lemma 18 : *Jede PPT-Dichtematrix* ρ*, welche auf* $C^2 \otimes C^2 \otimes C^N$ *unterstützt wird und* $r(\rho) = N \geq 4$ *erfüllt, ist separabel.*

Beweis: Ein $C^2 \otimes C^2 \otimes C^N$-System kann als ein $C^4 \otimes C^N$-System aufgefaßt werden. Benutzt man nun Theorem 13, so erhält man o.B.d.A. folgende Struktur:

$$\rho = |\psi_{AB_1}\rangle\langle\psi_{AB_1}| \otimes |C_1\rangle\langle C_1| + \sum_{i=2}^{N} |\psi_{AB_i}, C_i\rangle\langle\psi_{AB_i}, C_i|. \tag{9.13}$$

Nun läßt sich ein Vektor $|C\rangle$ in Charlies Raum finden, so daß $\langle C|\rho|C\rangle \sim |\psi_{AB_1}\rangle\langle\psi_{AB_1}|$ ist. Da aber der Zustand ρ bezüglich aller Systeme PPT ist, muß dieser ein Produktzustand sein. Da sich dies auf alle Projektoren in der konvexen Summe übertragen läßt, muß der Zustand ρ separabel sein.$_{q.e.d.}$

Nun müssen die Fälle $N = 2,3$ gesondert untersucht werden. Das darauf folgende Korollar und Lemma beschäftigen sich mit dem $N = 2$ Fall:

Korollar 6 : *Gegeben sei eine PPT-Dichtematrix* ρ*, welche auf* $C^2 \otimes C^2 \otimes C^2$ *unterstützt wird und* $r(\rho) = 2$ *erfüllt. Dann besitzt dieser Zustand einen Kernproduktvektor* $|e, f, g\rangle$.

Beweis: Ist $|e, f, g\rangle$ ein Kernvektor, so muß dieser auf den zwei Hilbertvektoren $\{|\psi_1\rangle, |\psi_2\rangle\}$ senkrecht sein, welche das Bild von ρ aufspannen. Wählt man $|e\rangle$ beliebig und setzt $|f\rangle = |0\rangle + \alpha|1\rangle$, so erhält man folgende zwei Gleichungen:

$$(\langle\psi_i|e,0\rangle + \alpha\langle\psi_i|e,1\rangle)|g\rangle = 0 \tag{9.14}$$

Dieses Gleichungssystem ist erfüllt, wenn die Determinante Null ergibt. Dies liefert eine quadratische Gleichung in α, welche immer eine Lösung besitzt.$_{q.e.d.}$

Lemma 19 : *Jede PPT-Dichtematrix* ρ*, welche auf* $C^2 \otimes C^2 \otimes C^2$ *unterstützt wird und* $r(\rho) = 2$ *erfüllt, ist separabel.*

Beweis: Für den Kernvektor $|e, f, g\rangle$ folgt nun, daß $\rho^{t_A}|e^*, f, g\rangle = 0$ gelten muß. Daraus ergibt sich, daß $\langle\hat{e}^*|\rho^{t_A}|e^*, f, g\rangle = 0$ gilt. Diese Gleichung ist aber äquivalent zu $\langle e|\rho|\hat{e}, f, g\rangle = 0$. Dies bedeutet wiederum, daß $\rho|\hat{e}, f, g\rangle = |\hat{e}\psi_{BC}\rangle$ gelten muß, wobei $|\psi_{BC}\rangle$ ein beliebiger Hilbertvektor in Bobs und Charlies System ist. Nun läßt sich laut Lemma 11 aus Kapitel 8, das von $C^2 \otimes C^N$-Systemen handelt, der Projektor $|\hat{e}, \psi_{BC}\rangle\langle\hat{e}, \psi_{BC}|$ von ρ abziehen, so daß $\tilde{\rho} = \rho - \frac{1}{\langle\hat{e},\psi_{BC}|\rho^{-1}|\hat{e},\psi_{BC}\rangle}|\hat{e}, \psi_{BC}\rangle\langle\hat{e}, \psi_{BC}|$ ein Projektor ist und zugleich PPT bezüglich

Alices System. Allgemein kann man ansetzen, daß $\rho = \tilde{\Lambda}|\tilde{e}\rangle\langle\tilde{e}| \otimes |\tilde{\psi}_{BC}\rangle\langle\tilde{\psi}_{BC}| + \Lambda|\hat{e},\psi_{BC}\rangle\langle\hat{e},\psi_{BC}|$ ist. Nun erhält man o.B.d.A. $\langle e|\rho|e\rangle \sim |\tilde{\psi}_{BC}\rangle\langle\tilde{\psi}_{BC}|$. Da ρ aber bezüglich aller Systeme PPT sein soll, muß dieser Projektor ein Produktzustand sein. Das gleiche läßt sich nun auch für $|\psi_{BC}\rangle\langle\psi_{BC}|$ zeigen. Die Projektion auf $|\tilde{\tilde{e}}\rangle\langle\tilde{\tilde{e}}|$ liefert nämlich $\langle\tilde{\tilde{e}}|\rho|\tilde{\tilde{e}}\rangle \sim |\psi_{BC}\rangle\langle\psi_{BC}|$. Also muß $|\psi_{BC}\rangle\langle\psi_{BC}|$ auch ein Produktzustand sein. Damit wäre das Lemma bewiesen.$_{q.e.d.}$

Zu guter Letzt bleibt noch der Fall $N = 3$. Um diesen Fall zu beweisen, wird daß folgende Korollar und Lemma benötigt:

Korollar 7 : *Jede PPT-Dichtematrix* ρ*, welche auf* $C^2 \otimes C^2 \otimes C^2$ *unterstützt wird und* $r(\rho) = 3$ *erfüllt, besitzt einen Kernvektor* $|e,f,g\rangle$.

Beweis: Sei ρ ein PPT-Zustand in $C^2 \otimes C^2 \otimes C^2$. Dieser kann als ein $C^2_A \otimes C^4_{BC}$-Zustand aufgefaßt werden. Dieser Zustand wird laut Theorem 10 auf $C^2_A \otimes C^3_{BC}$ unterstützt. Daraus ergibt sich folgende Form:

$$\rho = \sum_{i=1}^{3} |e_{A_i}\rangle\langle e_{A_i}| \otimes |\psi_{BC_i}\rangle\langle\psi_{BC_i}|. \tag{9.15}$$

Nun wählt man o.B.d.A. $|e\rangle$ orthogonal auf $|e_{A_3}\rangle$. Dies bedeutet, daß $|f,g\rangle$ orthogonal auf $|\psi_{BC_1}\rangle$ und $|\psi_{BC_2}\rangle$ sein muß. Setzt man den Ansatz $|f_B\rangle = |0\rangle_B + \alpha|1\rangle_B$ voraus, so erhält man folgendes Gleichungssystem für $|g\rangle$:

$$(\langle\psi_{BC_i}|0_B\rangle + \alpha\langle\psi_{BC_i}|1_B\rangle)|g\rangle = 0 \tag{9.16}$$

für $i = 1,2$. Diese Gleichung besitzt eine Lösung für den Fall, daß die Determinante Null ergibt. Dies liefert aber eine quadratische Gleichung für α, welche immer eine Lösung besitzt, und damit wäre das Korollar bewiesen.$_{q.e.d.}$

Die Existenz solch eines Produktvektors wird nun im folgenden Lemma benötigt.

Lemma 20 : *Jede PPT-Dichtematrix* ρ*, welche auf* $C^2 \otimes C^2 \otimes C^2$ *unterstützt wird und* $r(\rho) = 3$ *erfüllt, ist separabel.*

Beweis: Aus der Bedingung $\rho|e,f,g\rangle = 0$ für den Produktkernvektor, folgen die Bedingungen:

$$\begin{aligned}
\langle e|\rho|\hat{e},f,g\rangle &= 0 \\
\langle f|\rho|e,\hat{f},g\rangle &= 0 \\
\langle g|\rho|e,f,\hat{g}\rangle &= 0.
\end{aligned}$$

Dies bedeutet, daß

$$\begin{aligned}\rho|\hat{e},f,g\rangle &= |\hat{e}_A\rangle|\psi_{BC}\rangle\\ \rho|e,\hat{f},g\rangle &= |\hat{f}_B\rangle|\psi_{AC}\rangle\\ \rho|e,f,\hat{g}\rangle &= |\hat{g}_C\rangle|\psi_{AB}\rangle\end{aligned}$$

gilt. Nun definiert man:

$$\tilde{\rho} = \rho - \lambda|\hat{e}_A\rangle\langle\hat{e}_A| \otimes |\psi_{BC}\rangle\langle\psi_{BC}|, \tag{9.17}$$

wobei $\lambda = \frac{1}{\langle\hat{e}_A,\psi_{BC}|\rho^{-1}|\hat{e}_A,\psi_{BC}\rangle}$ ist (s. Lemma (11)). $\tilde{\rho}$ ist nun ein PPT-Zustand bzgl. $\tilde{\rho}^{t_A}$ und besitzt $r(\tilde{\rho}) = 2$. Nun läßt sich $\tilde{\rho}$ schreiben als:

$$\tilde{\rho} = \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_{AC}\rangle\langle\psi_{AC}| + \lambda_2|\hat{g}_C\rangle\langle\hat{g}_C| \otimes |\psi_{AB}\rangle\langle\psi_{AB}|. \tag{9.18}$$

Durch die Redefinition $|e_A\rangle = |0\rangle$ und $|\hat{e}_A\rangle = |1\rangle$ der Basis in Alices System, lassen sich die Vektoren $|\psi_{AC}\rangle$ und $|\psi_{AB}\rangle$ schreiben als:

$$|\psi_{AC}\rangle = |0\rangle|\psi_C^1\rangle + |1\rangle|\psi_C^2\rangle \tag{9.19}$$

$$|\psi_{AB}\rangle = |0\rangle|\phi_B^1\rangle + |1\rangle|\phi_B^2\rangle. \tag{9.20}$$

In Matrixform sieht $\tilde{\rho}$ wie folgt aus:

$$\tilde{\rho} = \begin{pmatrix} \begin{pmatrix} \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_C^1\rangle\langle\psi_C^1| \\ +\lambda_2|\phi_B^1\rangle\langle\phi_B^1| \otimes |\hat{g}_C\rangle\langle\hat{g}_C| \end{pmatrix} & \begin{pmatrix} \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_C^1\rangle\langle\psi_C^2| \\ +\lambda_2|\phi_B^1\rangle\langle\phi_B^2| \otimes |\hat{g}_C\rangle\langle\hat{g}_C| \end{pmatrix} \\ \begin{pmatrix} \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_C^2\rangle\langle\psi_C^1| \\ +\lambda_2|\phi_B^2\rangle\langle\phi_B^1| \otimes |\hat{g}_C\rangle\langle\hat{g}_C| \end{pmatrix} & \begin{pmatrix} \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_C^2\rangle\langle\psi_C^2| \\ +\lambda_2|\phi_B^2\rangle\langle\phi_B^2| \otimes |\hat{g}_C\rangle\langle\hat{g}_C| \end{pmatrix} \end{pmatrix}.$$

Aus der Positivität des Operators $\tilde{\rho}$ und $\tilde{\rho}^{t_A}$ folgt, daß wenn der diagonale Block $\begin{pmatrix} \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_C^2\rangle\langle\psi_C^2| \\ +\lambda_2|\phi_B^2\rangle\langle\phi_B^2| \otimes |\hat{g}_C\rangle\langle\hat{g}_C| \end{pmatrix}$ durch die Multiplikation mit $|\hat{\phi}_B^2\hat{\psi}_C^2\rangle$ verschwindet, dann auch die Nebendiagonalblöcke verschwinden müssen. Ebenso gilt das gleiche für den diagonalen Block $\begin{pmatrix} \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B| \otimes |\psi_C^1\rangle\langle\psi_C^1| \\ +\lambda_2|\phi_B^1\rangle\langle\phi_B^1| \otimes |\hat{g}_C\rangle\langle\hat{g}_C| \end{pmatrix}$ mit $|\hat{\phi}_B^1\hat{\psi}_C^1\rangle$. Dies liefert folgendes System von Gleichungen:

$$\langle\hat{f}_B|\hat{\phi}_B^1\rangle\langle\psi_C^2|\hat{\psi}_C^1\rangle = 0 \tag{9.21}$$

$$\langle\phi_B^2|\hat{\phi}_B^1\rangle\langle\hat{g_C}|\hat{\psi}_C^1\rangle = 0 \tag{9.22}$$

$$\langle\hat{f}_B|\hat{\phi}_B^2\rangle\langle\psi_C^1|\hat{\psi}_C^2\rangle = 0 \tag{9.23}$$

$$\langle\phi_B^1|\hat{\phi}_B^2\rangle\langle\hat{g_C}|\hat{\psi}_C^2\rangle = 0. \tag{9.24}$$

Dieses triviale Gleichungssystem besagt, daß mindestens einer der Projektoren $|\psi_{AB}\rangle\langle\psi_{AB}|$ und $|\psi_{AC}\rangle\langle\psi_{AC}|$ ein Produktzustand sein muß. Sei dies o.B.d.A der Projektor $|\psi_{AB}\rangle\langle\psi_{AB}|$. Dann läßt sich ρ schreiben als

$$\begin{aligned}\rho &= \lambda_1|\hat{f}_B\rangle\langle\hat{f}_B|\otimes|\psi_{AC}\rangle\langle\psi_{AC}|+\lambda_2|\tilde{e}_A\rangle\langle\tilde{e}_A|\otimes|\hat{f}_B\rangle\langle\hat{f}_B|\otimes|\hat{g}_C\rangle\langle\hat{g}_C| \\ &+ \lambda|\hat{e}\rangle\langle\hat{e}|\otimes|\psi_{BC}\rangle\langle\psi_{BC}| \\ &= |\hat{f}_B\rangle\langle\hat{f}_B|\otimes\underbrace{(\lambda_1|\psi_{AC}\rangle\langle\psi_{AC}|+\lambda_2|\tilde{e}_A\rangle\langle\tilde{e}_A|\otimes|\hat{g}_C\rangle\langle\hat{g}_C|)}_{\sigma} \\ &+ \lambda|\hat{e}\rangle\langle\hat{e}|\otimes|\psi_{BC}\rangle\langle\psi_{BC}| \qquad (9.25)\end{aligned}$$

σ ist nun ein Rang 2 $C^2\otimes C^2$-PPT-Zustand. Für diese Zustände gelten folgende Fälle:

- Im Hilbertraum von σ existiert nur ein Produktvektor. σ wäre damit NPPT. Dies ist ein Widerspruch zur Annahme, daß σ PPT sei.
- Im Hilbertraum von σ existieren zwei Produktvektoren P_1 und P_2. Die erste Möglichkeit wäre dann, daß o.B.d.A $P_1 = |\psi_{AC}\rangle$ und $P_2 = |\tilde{e}_A\rangle\otimes|\hat{g}_C\rangle$ ist. Damit wäre $|\psi_{AC}\rangle$ ein Produktvektor. Die zweite Möglichkeit wäre o.B.d.A folgende Gestalt:

  $$\sigma = \lambda_1(|\alpha P_1+\beta P_2\rangle\langle\alpha P_1+\beta P_2|+\lambda_2|P_1\rangle\langle P_1|. \qquad (9.26)$$

  Zu diesem Zustand existiert aber eine lokale reversible nichtunitäre Filteroperation $A\otimes B$, so daß $\sigma = f|\psi_{max}\rangle\langle\psi_{max}|+(1-f)|00\rangle\langle 00|$ wäre. Diese ist aber nur ein PPT-Zustand für $f=0$.
- Im Hilbertraum von σ existieren unendlich viele Produktvektoren. Dies bedeutet aber, daß o.B.d.A. $\sigma = |\tilde{e}_A\rangle\langle\tilde{e}_A|\otimes(\lambda_1|\tilde{g}_C\rangle\langle\tilde{g}_C|+\lambda_2|\hat{g}_C\rangle\langle\hat{g}_C|)$ ist, also wäre in diesem Falle $|\psi_{AC}\rangle$ ein Produktvektor.

Dies bedeutet, daß sich o.B.d.A ρ schreiben läßt als:

$$\begin{aligned}\rho &= \lambda_1|\bar{e}_A\rangle\langle\bar{e}_A|\otimes|\hat{f}_B\rangle\langle\hat{f}_B|\otimes|\tilde{g}_C\rangle\langle\tilde{g}_C|+\lambda_2|\tilde{e}_A\rangle\langle\tilde{e}_A|\otimes|\hat{f}_B\rangle\langle\hat{f}_B|\otimes|\hat{g}_C\rangle\langle\hat{g}_C| \\ &+ \lambda|\hat{e}\rangle\langle\hat{e}|\otimes|\psi_{BC}\rangle\langle\psi_{BC}|.\end{aligned}$$

Für die Beweisführung ist Alice natürlich in keiner Art und Weise ausgezeichnet. Dies bedeutet, daß

$$\begin{aligned}\bar{\rho} &= \rho-\bar{\lambda}|\tilde{e}_A\rangle\langle\tilde{e}_A|\otimes|\hat{f}_B\rangle\langle\hat{f}_B|\otimes|\hat{g}_C\rangle\langle\hat{g}_C| \\ &= \lambda_1|\bar{e}_A\rangle\langle\bar{e}_A|\otimes|\hat{f}_B\rangle\langle\hat{f}_B|\otimes|\tilde{g}_C\rangle\langle\tilde{g}_C|+\lambda|\hat{e}\rangle\langle\hat{e}|\otimes|\psi_{BC}\rangle\langle\psi_{BC}|,\end{aligned}$$

wobei $\bar{\lambda} \equiv \lambda_2 = \frac{1}{\langle \tilde{e}_A \hat{f}_B \hat{g}_C | \rho^{-1} | \tilde{e}_A \hat{f}_B \hat{g}_C \rangle}$ gilt, ein PPT Zustand bzgl. Charlie sein muß. Die Projektion von $\bar{\rho}$ auf $|\hat{\tilde{e}}\rangle$ liefert $\langle \hat{\tilde{e}} | \bar{\rho} | \hat{\tilde{e}} \rangle \sim |\psi_{BC}\rangle\langle\psi_{BC}|$. Dies bedeutet aber, daß $|\psi_{BC}\rangle$ ein Produktvektor sein muß und somit wäre der Beweis abgeschlossen.$_{q.e.d.}$

Da aber ρ ein PPT-Zustand bezüglich aller Systeme sein soll, muß $|\psi_{BC}\rangle$ ein Produktzustand sein. Durch weiteres äquivalentes Vorgehen erhält man auch, daß $|\psi_{AC}\rangle$ ein Produktzustand sein soll. Damit wäre das Korollar bewiesen.$_{q.e.d.}$

Nun läßt sich der $N = 3$ Fall beweisen, wie das folgende Lemma gleich zeigen wird.

Lemma 21 : *Jede PPT-Dichtematrix ρ, welche auf $C^2 \otimes C^2 \otimes C^3$ unterstützt wird und $r(\rho) = 3$ erfüllt, ist separabel.*

Beweis: Man faßt das $C^2 \otimes C^2 \otimes C^3$-System als ein $C^4_{AB} \otimes C^3_C$-System auf. Laut Theorem (13) können nun drei Fälle der Unterstützung auftreten:

- Das System wird auf $C^3_{AB} \otimes C^3_C$ unterstützt. Dann hat die Dichtematrix folgende Form:

$$\begin{aligned} \rho &= \Lambda_1 |e_{AB_1}\rangle\langle e_{AB_1}| \otimes |f_{C_1}\rangle\langle f_{C_1}| + \Lambda_2 |e_{AB_2}\rangle\langle e_{AB_2}| \otimes |f_{C_2}\rangle\langle f_{C_2}| \\ &+ \Lambda_3 |e_{AB_3}\rangle\langle e_{AB_3}| \otimes |f_{C_3}\rangle\langle f_{C_3}|. \end{aligned}$$

  Da die $|f_{C_i}\rangle$ linear unabhängig sind, läßt sich solch ein Vektor $|C\rangle$ in Charlies System finden, so daß o.B.d.A. $\langle C|\rho|C\rangle \sim |e_{AB_1}\rangle\langle e_{AB_1}|$ gilt. Da der Zustand aber bezüglich allen Systemen PPT ist, muß er also auch separabel sein.

- Das System wird auf $C^2_{AB} \otimes C^3_C$ unterstützt. Auch hier läßt sich das obige Verfahren durch geschickte Projektion ausnutzen, um die Separabilität zu zeigen.

- Das System wird auf $C^3_{AB} \otimes C^2_C$ unterstützt. Dies ist aber nichts weiter als ein $C^2 \otimes C^2 \otimes C^2$-System mit Rang 3. Deren Separabilität wurde aber im letzten Korollar schon bewiesen.

Somit wäre das Lemma bewiesen.$_{q.e.d.}$

Nun lassen sich die einzelnen Korollars zu einem Theorem zusammenfassen:

Theorem 14 : *Jeder PPT-Zustand, welcher auf $C^2 \otimes C^2 \otimes C^N$ unterstüzt wird und $r(\rho) = N$ besitzt, ist separabel und besitzt die kanonische Form*

$$\rho = \sqrt{D} \begin{pmatrix} B^\dagger C^\dagger CB & B^\dagger C^\dagger C & B^\dagger C^\dagger B & B^\dagger C^\dagger \\ C^\dagger CB & C^\dagger C & C^\dagger B & C^\dagger \\ B^\dagger CB & B^\dagger C & B^\dagger B & B^\dagger \\ CB & C & B & 1 \end{pmatrix} \sqrt{D} \qquad (9.27)$$

$$= \sqrt{D}\begin{pmatrix} B^\dagger C^\dagger \\ C^\dagger \\ B^\dagger \\ 1 \end{pmatrix}\begin{pmatrix} CB & C & B & 1 \end{pmatrix}\sqrt{D} \tag{9.28}$$

aus Lemma (16), wobei $[B,B^\dagger]=[C,C^\dagger]=[C,B]=[C,B^\dagger]=0$ *und* $D=D^\dagger$ *gilt. Die B,C und D sind Operatoren in Charlies System.*

Im nächsten Abschnitt werden ähnlich wie bei den $C^2\otimes C^N$-Zuständen die Bildbereiche nach Produktvektoren untersucht.

9.3 Separabilitätskriteria und Separabilitätsüberprüfungen von generischen $C^2\otimes C^2\otimes C^N$-Zuständen

In diesem Abschnitt werden PPT-Dichtematrizen untersucht, welche eine endliche Anzahl von Produktzuständen $\{|e_i,f_i,g_i\rangle\}\in C^2\otimes C^2\otimes C^N$ besitzen, so daß $|e_i,f_i,g_i\rangle\in R(\rho)$,$|e_i^*,f_i,g_i\rangle\in R(\rho^{t_A})$,$|e_i,f_i^*,g_i\rangle\in R(\rho^{t_B})$ und $|e_i^*,f_i^*,g_i\rangle\in R(\rho^{t_{AB}})$ erfüllt sind. Gezeigt wird, daß Zustände, die der Ungleichung $r(\rho)+r(\rho^{t_A})+r(\rho^{t_B})+r(\rho^{t_{AB}})\leq 15N-1$ genügen, genau die letztere Eigenschaft besitzen können. Die gesamte Frage nach den Produktvektoren $\{|e_i,f_i,g_i\rangle\}\in C^2\otimes C^2\otimes C^N$ reduziert sich auf das Lösen von multipolynomialen Gleichungen. Existiert eine endliche Menge solcher Lösungen, so wird der Zustand **generisch** genannt.

9.3.1 Generische Zustände

Seien die $|K_i\rangle$,$|K_{A_i}\rangle$,$|K_{B_i}\rangle$ und $|K_{AB_i}\rangle$ linear unabhängige Kernvektoren von ρ, ρ^{t_A}, ρ^{t_B} und $\rho^{t_{AB}}$, d.h. es gilt:

$$\begin{aligned} K(\rho) &= \text{span}\{|K_i\rangle, i=1,\ldots,k(\rho)\},\\ K(\rho^{t_A}) &= \text{span}\{|K_{A_i}\rangle, i=1,\ldots,k(\rho^{t_A})\},\\ K(\rho^{t_B}) &= \text{span}\{|K_{B_i}\rangle, i=1,\ldots,k(\rho^{t_B})\},\\ K(\rho^{t_{AB}}) &= \text{span}\{|K_{AB_i}\rangle, i=1,\ldots,k(\rho^{t_{AB}})\}. \end{aligned}$$

Nun lassen sich die Kernvektoren bezüglich einer Basis in Alices und Bobs Raum schreiben als:

$$\begin{aligned} |K_i\rangle &= |00\rangle|k_i^{00}\rangle+|01\rangle|k_i^{01}\rangle+|10\rangle|k_i^{10}\rangle+|11\rangle|k_i^{11}\rangle\\ |K_{A_i}\rangle &= |00\rangle|k_{A_i}^{00}\rangle+|01\rangle|k_{A_i}^{01}\rangle+|10\rangle|k_{A_i}^{10}\rangle+|11\rangle|k_{A_i}^{11}\rangle \end{aligned}$$

$$
\begin{aligned}
|K_{B_i}\rangle &= |00\rangle|k_{B_i}^{00}\rangle + |01\rangle|k_{B_i}^{01}\rangle + |10\rangle|k_{B_i}^{10}\rangle + |11\rangle|k_{B_i}^{11}\rangle \\
|K_{AB_i}\rangle &= |00\rangle|k_{AB_i}^{00}\rangle + |01\rangle|k_{AB_i}^{01}\rangle + |10\rangle|k_{AB_i}^{10}\rangle + |11\rangle|k_{AB_i}^{11}\rangle.
\end{aligned}
$$

Ein Produktvektor $|e,f,g\rangle \in V[\rho]$ muß nun orthogonal auf allen Kernvektoren sein, so daß folgende Gleichungen erfüllt sein müssen:

$$
\begin{aligned}
\langle K_i|e,f,g\rangle &= 0, \\
\langle K_{A_i}|e^*,f,g\rangle &= 0, \\
\langle K_{B_i}|e,f^*,g\rangle &= 0, \\
\langle K_{AB_i}|e^*,f^*,g\rangle &= 0.
\end{aligned} \tag{9.29}
$$

Nun entwickelt man $|e,f,g\rangle$ nach der lokalen Basis in Alice und Bob:

$$
\begin{aligned}
|efg\rangle &= (\alpha|0\rangle + |1\rangle) \otimes (\beta|0\rangle + |1\rangle) \otimes |g\rangle \\
&= (\alpha\beta|00\rangle + \alpha|01\rangle + \beta|10\rangle + |11\rangle) \otimes |g\rangle.
\end{aligned}
$$

Jetzt läßt sich (9.29) schreiben als:

$$
A(\alpha,\beta;\alpha^*,\beta^*)|g\rangle = 0, \tag{9.30}
$$

wobei $A(\alpha,\beta;\alpha^*,\beta^*)$ eine $(k(\rho)+k(\rho^{t_A})+k(\rho^{t_B})+k(\rho^{t_{AB}}))\times N$-Matrix ist, welche folgende Form besitzt:

$$
A(\alpha,\beta;\alpha^*,\beta^*) = \begin{pmatrix}
\alpha\beta\langle k_i^{00}| + \alpha\langle k_i^{01}| + \beta\langle k_i^{10}| + \langle k_i^{11}| \\
\alpha^*\beta\langle k_{A_i}^{00}| + \alpha^*\langle k_{A_i}^{01}| + \beta\langle k_{A_i}^{10}| + \langle k_{A_i}^{11}| \\
\alpha\beta^*\langle k_{B_i}^{00}| + \alpha\langle k_{B_i}^{01}| + \beta^*\langle k_{B_i}^{10}| + \langle k_{B_i}^{11}| \\
\alpha^*\beta^*\langle k_{AB_i}^{00}| + \alpha^*\langle k_{AB_i}^{01}| + \beta^*\langle k_{AB_i}^{10}| + \langle k_{AB_i}^{11}|
\end{pmatrix}.
$$

Falls nun (9.29) für einige $|e\rangle \neq 0, |f\rangle \neq 0$ und $|g\rangle \neq 0$ erfüllt ist, muß der Rang von A kleiner sein als N. Dies bedeutet, daß maximal $N-1$ Spaltenvektoren aus der Matrix A linear unabhängig sein müssen. Daraus ergibt sich, daß $(k(\rho)+k(\rho^{t_A})+k(\rho^{t_B})+k(\rho^{t_{AB}}))-N+1$-Minoren aus der Matrix A verschwinden müssen.

Nun betrachtet man den Fall, in dem $k(\rho)+k(\rho^{t_A})+k(\rho^{t_B})+k(\rho^{t_{AB}}) = 2+(N-1)$ gilt.

Es wird z.B. zu den ersten $N-1$-Zeilen jede weitere der übriggebliebenen zwei Zeilen von A hinzugefügt. Gleichzeitig fordert man, daß diese zwei Zeilen linear abhängig zu den ersten $N-1$ sind. Dies kann immer durch die Parameter α und β gewährleistet werden. Auf diese Art und Weise wird der Rang von A kleiner als $N-1$ gemacht. Der Fall, in dem $k(\rho)+k(\rho^{t_A})+k(\rho^{t_B})+k(\rho^{t_{AB}}) \geq 2+(N-1)$, bzw.

$$
(r(\rho)+r(\rho^{t_A})+r(\rho^{t_B})+r(\rho^{t_{AB}}) \leq 15N-1 \tag{9.31}
$$

beinhaltet, hat dann noch mehr Einschränkungen und kann nur eine noch kleinere Menge an Lösungen besitzen.

Wichtig ist nun, daß die $k(\rho)+k(\rho^{t_A})+k(\rho^{t_B})+k(\rho^{t_{AB}})-N+1$-Minoren eine endliche Anzahl von Lösungen in α und β besitzen müssen. Zustände, welche dies beinhalten, werden in diesem Kontext **generisch** genannt. Dadurch wird versucht, eine endliche Anzahl von Produktvektoren im Bildbereich zu erhalten.

Nun kann man wie bei den $C^2 \otimes C^N$-Zuständen eine Analyse auf Separabilität durchführen. Dies wird im folgenden Unterabschnitt für $C^2 \otimes C^2 \otimes C^2$-Zustände durchgeführt.

9.4 Separabilitätstests für $C^2 \otimes C^2 \otimes C^2$-Zustände

Als spezielles Beispiel von $C^2 \otimes C^2 \otimes C^N$-PPT-Zuständen werden in diesem Abschnitt drei q-Bit-Systeme untersucht. Dabei werden zu deren Analyse die Ergebnisse aus den letzteren Kapiteln benutzt. Die drei q-Bit-Systeme sind deshalb von besonderem Interesse, weil sie der erste natürliche Schritt zu mehrfach verschränkten Zuständen, sowohl wie in der Theorie als auch im Labor, darstellen. Desweiteren kann der dritte q-Bit als Ancilla aufgefaßt werden, um auf den Zwei q-Bit-Systemen komplexere POVM-Operationen durchzuführen. Nun wird abhängig vom Rang des jeweiligen Zustandes auf die Separabilitätsbedingungen eingegangen.

9.4.1 Der Fall $r(\rho)=2$

Für diesen Zustand weiß man, daß er separabel sein muß.

9.4.2 Der Fall $r(\rho)=3$

Dieser Zustand ist laut Korollar 20 separabel.

9.4.3 Der Fall $r(\rho)=4$

Ein drei q-Bit-System mit Rang 4 kann als ein $C^2 \otimes C^4$-System mit Rang 4 angesehen werden. Laut Theorem (13) ist aber bekannt, daß dieser Zustand eine eindeutige Produktzerlegung bezüglich $C_A^2 \otimes C_{BC}^4$ besitzt. Da aber der Zustand in Bezug

auf alle Teilsysteme PPT ist, muß dies auch für $C_B^2 \otimes C_{AC}^2$ und $C_C^2 \otimes C_{AB}^2$ gelten. Dies bedeutet daß dieser PPT-Zustand biseparabel daargestellt werden kann in Bezug auf allen drei Systemen.

9.4.4 Der Fall $r(\rho) = r(\rho^{t_A}) = r(\rho^{t_B}) = r(\rho^{t_{AB}}) = 7$

Es wird nun die mögliche Anzahl von Produktzuständen untersucht, die dieser Fall beinhalten könnte. Die Matrix A ist gegeben durch:

$$A(\alpha,\beta;\alpha^*,\beta^*) = \begin{pmatrix} \alpha\beta\langle k_1^{00}| + \alpha\langle k_1^{01}| + \beta\langle k_1^{10}| + \langle k_1^{11}| \\ \alpha^*\beta\langle k_{A_1}^{00}| + \alpha^*\langle k_{A_1}^{01}| + \beta\langle k_{A_1}^{10}| + \langle k_{A_1}^{11}| \\ \alpha\beta^*\langle k_{B_1}^{00}| + \alpha\langle k_{B_1}^{01}| + \beta^*\langle k_{B_1}^{10}| + \langle k_{B_1}^{11}| \\ \alpha^*\beta^*\langle k_{AB_1}^{00}| + \alpha^*\langle k_{AB_1}^{01}| + \beta^*\langle k_{AB_1}^{10}| + \langle k_{AB_1}^{11}| \end{pmatrix}$$

Bezeichnet man die Polinome vom Grad X und Y in den Variablen z und z^* mit $P_{X,Y}(z,z^*)$, dann lassen sich die drei Minoren von A schreiben als:

$$\alpha^2 P_{(1,1)}^{(1)}(\beta) + \alpha P_{(1,1)}^{(2)}(\beta) + P_{(1,1)}^{(3)}(\beta) = 0 \tag{9.32}$$

$$\alpha\alpha^* Q_{(0,1)}^{(1)}(\beta) + \alpha Q_{(0,1)}^{(2)}(\beta) + \alpha^* Q_{(0,1)}^{(3)}(\beta) + Q_{(0,1)}^{(4)}(\beta) = 0 \tag{9.33}$$

$$\alpha\alpha^* R_{(1,1)}^{(1)}(\beta) + \alpha R_{(1,1)}^{(2)}(\beta) + \alpha^* R_{(1,1)}^{(3)}(\beta) + R_{(1,1)}^{(4)}(\beta) = 0. \tag{9.34}$$

Nun multipliziert man (9.34) mit $Q_{(0,1)}^{(1)}(\beta)$ und (9.33) mit $R_{(1,1)}^{(1)}(\beta)$ und subtrahiert dann diese Gleichungen voneinander. Dadurch erhält man eine Gleichung der folgenden Form:

$$\alpha S_{(1,2)}^{(1)}(\beta) + \alpha^* S_{(1,2)}^{(2)}(\beta) + S_{(1,2)}^{(3)}(\beta) = 0. \tag{9.35}$$

Nun bildet man das komplex Konjugierte der Gleichung (9.35) und erhält eine weitere unabhängige Gleichung von der gleichen Form wie (9.35). Durch die gleiche Prozedur entledigt man sich des α^* und erhält dadurch ein Polynom, welches in α linear ist, von folgender Form:

$$\alpha T_{(3,3)}^{(0)}(\beta) + T_{(3,3)}^{(1)} = 0. \tag{9.36}$$

Nun läßt es sich nach α auflösen und in (9.32) einsetzen. Dadurch erhält man eine Polynomialgleichung vom Grade 7 in β und β^*. Diese kann laut Anhang A 896 mögliche Lösungen für β besitzen, was erheblich größer ist als $\min(r(\rho)^2, r(\rho^{t_A})^2, r(\rho^{t_B})^2, r(\rho^{t_{AB}})^2) = 49$.

Dies bedeutet, daß man eine PPT-BSA-Analyse durchführen sollte, nachdem man die Menge der Produktvektoren analysiert hat.

9.5 Zusammenfassung

Die Untersuchungen von $C^2 \otimes C^N$-PPT-Zuständen erwiesen sich bei der Untersuchung von $C^2 \otimes C^2 \otimes C^N$-PPT-Zuständen als nützlich. Desweiteren scheint die Methode “der lokalen Projektionen” auf die jeweiligen zusammengesetzten Teilräume zusammen mit der Bedingung der Erhaltung der PPT-Eigenschaft der Zustände maßgebend für die hier erworbenen Separabilitätskriterien. Die beiden Untersuchungen könnten als besonders starkes mathematisches Hilfsmittel fungieren, wenn es um die PPT-BSA-Untersuchungen von dreifach zusammengesetzten Systemen geht. Jegliche Information über die so erworbene kanonische Struktur von PPT-BSA-Resten, kann bei einer Konstruktion von Witness Operatoren in dreifach zusammengesetzten Systemen beitragen.

Kapitel 10

Ausblick

Durch die PPT-BSA-Formulierung ist es möglich geworden, Witness Operatoren für verschränkte PPT-Zustände zu beschreiben. Der nächste natürliche Schritt wäre, die minimale Menge von Witness Operatoren zu finden, die eine vollständige Charakterisierung von verschränkten Zuständen zuläßt. Die Untersuchungen von niedrigrängigen verschränkten PPT-Zuständen (hier $C^2 \otimes C^N$- und $C^2 \otimes C^2 \otimes C^N$-Zuständen) spielen dabei eine wichtige Rolle. Der Grund dafür, warum dies wichtig ist, liegt darin, daß niedrigrängige verschränkte PPT-Zustände die Oberfläche der konvexen Menge aller verschränkten PPT-Zustände bilden. Kennt man die Oberfläche einer konvexen Menge, so kennt man auch die konvexe Menge selber. Man erkennt also, wie wichtig die Untersuchungen der Zustände mit niedrigen Rängen ist. Ebenfalls wurde gezeigt, wie man Produktvektoren aus dem Bildbereich der PPT-Zustände ermitteln kann. Eine PPT-BSA-Zerlegung ermöglicht dann die Konstruktion eines eventuell vorhandenen PPT-BSA-Restes, wodurch man einen Witness konstruieren kann. Kennt man nun die Eigenschaften der minimalen vollständigen Menge von Witness Operatoren, so wäre es prinzipell möglich, aus einer kleinen Menge von konkret gegebenen PPT-Zuständen diese Menge von Witness Operatoren explizit zu bestimmen. Dadurch würde man das lang ersehnten Ziel der kompletten Charakterisierung von verschränkten Zuständen erreichen. Die ersten Schritte in diese Richtung wurden in den Arbeiten von M. Lewenstein, B. Kraus, J. I. Cirac und P. Horodecki gemacht ([107] und [108]). Der Isomorphismus, der zwischen den Witness Operatoren und den positiven Abbildungen ([80] und [71]) existiert, läßt uns hoffen, daß in naher Zukunft auch alle positiven Abbildungen dadurch klassifiziert werden können. Dies würde bedeuten, daß man eine der wichtigsten offenen Fragen der C^*-Algebra beantworten könnte.

Eines ist auf jeden Fall sicher: Die Quanteninformationstheorie wird uns auch

in Zukunft eine Menge faszinierender Fragen und Antworten über das Wesen der Quantenmechanik liefern!

Anhang A

Reduktion von Polynomen

In diesem Anhang wird gezeigt, daß jedes generische Polynom $P_{X,Y}(\alpha,\alpha^*)$ vom Grad X und Y in α und α^* (d.h. ein Polynom, das nach einer komplexen Konjugation wiederum ein verschiedenes Polynom liefert) maximal $2^{X-1}[X+Y(Y-X+1)]$ Nullstellen haben muß, wobei o.B.d.A. angenommen wurde, daß $Y \geq X$ sei. Die Idee basiert auf einem Verfahren, in dem man ein Polynom $Q(\alpha)$ vom Grade $2^{X-1}[X+Y(Y-X+1)]$ findet, so daß die Nullstellen von P auch Nullstellen von Q sind. Dieses Verfahren wird nun beschrieben.

Die Gleichung, die zu lösen ist, lautet

$$0 = P_{X,Y}(\alpha,\alpha^*) = \sum_{k=0}^{X} \alpha^k P_Y^k(\alpha^*) \tag{A.1}$$

$$= \sum_{k=0}^{N} (\alpha^{*k} Q_X^k(\alpha), \tag{A.2}$$

wobei P_X^k und Q_X^k Polynome vom Grade Y und X sind. Wenn man die letzte Gleichung komplex konjugiert, so erhält man

$$0 = \sum_{k=0}^{Y} \alpha^k \bar{Q}_X^k(\alpha^*). \tag{A.3}$$

$\bar{Q}$ ist das gleiche Polynom wie Q nur mit komplex konjugierten Koeffizienten. Von nun an werden α und α^* als unabhängige Variablen betrachtet, d.h. $\beta \equiv \alpha^*$. Auf diese Art und Weise erhält man folgende zwei Gleichungen:

$$\sum_{k=0}^{X} \alpha^k P_Y^k(\beta) = 0 \tag{A.4}$$

$$\sum_{k=0}^{Y} \alpha^k \bar{Q}_X^k(\beta) = 0. \tag{A.5}$$

Sei nun $X \neq Y$. Dann lassen sich die beiden letzten Gleichungen auf die Form

$$\sum_{k=0}^{X} \alpha^k R_Z^k(\beta) = 0 \tag{A.6}$$

transformieren, wobei $Z = X + Y(Y - X)$ gilt. Um zu diesem Polynom zu gelangen, wird als erstes (A.4) mit $\alpha^{Y-X}\bar{Q}_X^Y(\beta)$ und (A.5) mit $P_Y^X(\beta)$ multipliziert. Nun zieht man diese beiden Gleichungen voneinander ab und erhält so ein Polynom vom Grade $Y - 1$ in α und $Y + X$ in β. Nun benutzt man wieder das Polynom (A.4), um ein Polynom vom Grade $Y - 2$ zu erhalten. Durch sukzessive Wiederholung gelangt man dann zur gewünschten Form (A.6). Für den Fall $Y = X$ erhält man automatisch den Fall $Z = X$.

Nun wird (A.4) mit $R_Z^X(\beta)$ und (A.6) mit $P_Y^X(\beta)$ multipliziert und danach subtrahiert. Ebenso wird (A.5) mit $R_Z^0(\beta)$ und mit $P_Y^0(\beta)$ multipliziert und danach subtrahiert und durch α dividiert. Auf diese Art und Weise erhält man zwei Polynome vom Grad $X - 1$ in α und $Y + Z$ in β. Nun wiederholt man die gleiche Prozedur mit diesen zwei Polynomen bis man ein Polynom $\bar{Q}(\beta) = 0$ von Grad $2^{X-1}(Z + Y)$ erhält. Nun müssen alle Nullstellen des originalen Polynoms auch Nullstellen von Q sein.

Anhang B

Der Algorithmus der paarweisen PPT Maximierung

Nun werden die verschiedenen Fälle der Paarweisen-PPT-Maximalität vorgestellt. Diese müssen gesondert vom Algorithmus untersucht werden.

Seien $P_1 = |e_1, f_1\rangle\langle e_1, f_1|$ und $P_2 = |e_2, f_2\rangle\langle e_2, f_2|$ Projektoren. Die Bedingung, daß Λ_1 in Bezug auf $\rho - \Lambda_2 P_2$ maximal ist, und Λ_2 in Bezug auf $\rho - \Lambda_1 P_1$ maximal ist, liefert die folgende Bedingung an Λ_1 und Λ_2:

$$F(\Lambda_1, \Lambda_2) \equiv 1 - \Lambda_1 D_1^{(0)} - \Lambda_2 D_2^{(0)} + \Lambda_1 \Lambda_2 D^{(0)} = 0. \tag{B.1}$$

Dabei ist $D_1^{(0)} = \langle e_1, f_1|\rho^{-1}|e_1, f_1\rangle$, $D_2^{(0)} = \langle e_2, f_2|\rho^{-1}|e_2, f_2\rangle$, $D_{12}^{(0)} = |\langle e_1, f_1|\rho^{-1}|e_2, f_2\rangle|^2$ und $D^{(0)} = D_1^{(0)} D_2^{(0)} - D_{12}^{(0)}$.

Ebenso gilt aber auch, daß Λ_1 in Bezug auf $\rho^{t_A} - \Lambda_2 P_2^{t_A}$ und Λ_2 in Bezug auf $\rho^{t_A} - \Lambda_1 P_1^{t_A}$ maximal ist. Dies liefert eine weitere Bedingung an Λ_1 und Λ_2:

$$\tilde{F}(\Lambda_1, \Lambda_2) \equiv 1 - \Lambda_1 D_1^{(1)} - \Lambda_2 D_2^{(1)} + \Lambda_1 \Lambda_2 D^{(1)} = 0. \tag{B.2}$$

Dabei ist $D_1^{(1)} = \langle e_1^*, f_1|(\rho^{t_A})^{-1}|e_1^*, f_1\rangle$, $D_2^{(1)} = \langle e_2^*, f_2|(\rho^{t_A})^{-1}|e_2^*, f_2\rangle$, $D_{12}^{(1)} = |\langle e_1^*, f_1|(\rho^{t_A})^{-1}|e_2^*, f_2\rangle|^2$ und $D^{(2)} = D_1^{(1)} D_2^{(1)} - D_{12}^{(1)}$.

Fall 1: Eine der beiden Mannigfaltigkeiten $F = 0$ und $\tilde{F} = 0$ ist echt größer oder größer gleich der anderen. Sei o.B.d.A. dies die Mannigfaltigkeit $\tilde{F} = 0$. Dann ergibt sich die in Abbildung *B*.1 und *B*.2 dargestellte Situation. Tritt dieser Fall auf, so ist die Paarweise-BSA-Maximalität von $F = 0$ zu nehmen (Lemma 4).

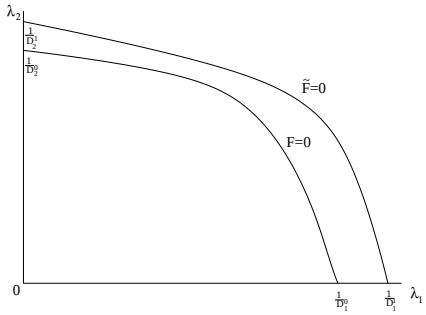

Abbildung B.1: Fall 1 mit echt größer. Hier muß die Mannigfaltigkeit $F = 0$ benutzt werden, um die PPT zu erhalten.

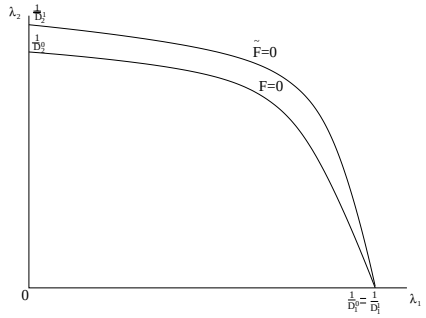

Abbildung B.2: Fall 2 mit größer gleich. Die Mannigfaltigkeiten besitzen einen Schnittpunkt am Rande der konvexen Menge.

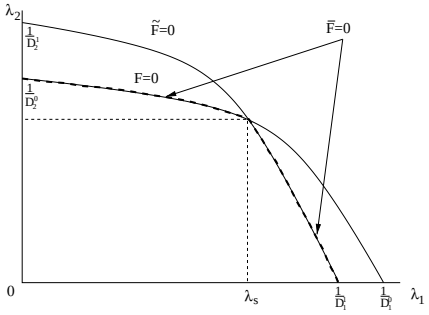

Abbildung B.3: Fall 2 mit Schnittpunkt. Hierbei müssen die jeweiligen Teile der Mannigfaltigkeiten gewählt werden, welche untehalb der maximalen liegen. Dadurch wird die PPT-Eigenschaft erhalten.

Fall 2: Die beiden Mannigfaltigkeiten schneiden sich in einem Punkt, welcher nicht am Rande liegt. Sei o.B.d.A. dann die Situation in Abbildung *B*.3 zutreffend. Der Schnittpunkt λ_s ist durch den folgenden analytischen Ausdruck gegeben:

$$\begin{aligned}\lambda_s &= \frac{1}{2(D_1^0 D^1 - D_1^1 D^0)}((D^1 + D_1^0 D_2^1 - D^0 - D_1^1 D_2^0) \\ &\pm \sqrt{(D^1 + D_1^0 D_2^1 - D^0 - D_1^1 D_2^0) - 4(D_1^0 D^1 - D_1^1 D^0)(D_2^1 - D_2^0)}),\end{aligned}$$

wobei λ_s natürlich nur für den Fall $0 \leq \lambda_s \leq \min(\left(\frac{1}{D_1^0}, \frac{1}{D_1^1}\right))$ zu berücksichtigen ist. Die resultierende Mannigfaltigkeit (durch die volle Linie gekennzeichnet) besitzt nun die Eigenschaft, daß sie im Schnittpunkt nicht differenzierbar ist. Für die Ermittlung der Paarweisen-PPT-Maximalen Λ's auf dieser Mannigfaltigkeit sind nun folgende Fälle zu berücksichtigen:

- Für den Fall, daß beide Maxima "links" vom Schnittpunkt liegen, ist das BSA-Maxima von $F = 0$ zu nehmen.
- Für den Fall, daß beide Maxima "rechts" vom Schnittpunkt liegen, ist wiederum das Maxima von $\tilde{F} = 0$ zu nehmen.
- Für den Fall, daß das Maximum von ρ^{t_A} "rechts" und das Maximum von ρ "links" vom Schnittpunkt liegt, fällt das Maximum mit dem Schnittpunkt überein.
- Der Fall, daß das Maximum von ρ^{t_A} "links" und das Maximum von ρ "rechts" vom Schnittpunkt liegt, kann für diesen Fall nicht eintreffen.
- Der letzte Fall ist, daß beide Maxima im Schnittpunkt übereinstimmen.

Dieser Algorithmus kann auch für mehrfach zusammengesetzte Systeme ausgearbeitet werden. Durch die PPT-Bedingungen erhält man mehrere Schnittflächen, die wiederum gesondert untersucht werden müssen.

Literaturverzeichnis

[1] M. Lewenstein und A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).

[2] R. Feynman, Found. Phys. **16**, 507 (1986).

[3] P. W. Shor. SIAM J. Computing **26**, 1484 (1997).

[4] L. K. Grover, Phsy. Rev. Lett. **78**, 325 (1997).

[5] P. Benioff, J. Statist. Phys. **22**, 563 (1980).

[6] L. K. Grover, Phsy. Rev. Lett. **78**, 325 (1997).

[7] D. Deutsch, Proc. Roy. Soc. London A**400**, 96 (1985).

[8] D. R. Simon, SIAM J. Computing **26**, 1474 (1997).

[9] J. I. Cirac und P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[10] J. F. Poyatos, J. I. Cirac und P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998).

[11] S. Lloyd, Science **273**, 1073 (1996).

[12] D. S. Abrams und S. Lloyd, Phys. Rev. Lett. **79**, 2586 (1997).

[13] M. Brune, E. Hagley, J. Dreyer, X. Maitre, A. Maali, C. Wunderlich, J. M. Raimond und S. Haroche, Phys. Rev. Lett. **77**, 4887 (1996).

[14] C. Zalka, Proc. Poy. Soc. Lond. A**454**, 313 (1998).

[15] S. Wiesner, quant-ph/9603028.

[16] B. M. Boghosian und W. Taylor, Physica D**120**, 30 (1998).

[17] Dominic Welsh, “Codes and Cryptography”, Oxford Science Publications (1989).

[18] A. Ekert und C. Macchiavello, quant-ph/9602022.

[19] P. W. Shor, Phys. Rev. A**52**, 2493 (1995).

[20] B. Scneier, “Angewante Kryptographie”, Addison-Wesley (1998).

[21] J. Buchmann, “Einführung in die Kryptographie”, Springer (1999).

[22] G. W. Selke, “Kryptographie”, O’Reilly (2000).

[23] C. H. Bennett, G. Brassard und N. D. Mermin, Phys. Rev. Lett. **68** 557 (1992).

[24] A. K. Ekert, Phys. Rev. Lett. **67** 661 (1991).

[25] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail und J. Smolin, J. Crypto. **5**, 3 (1992).

[26] C. H. Bennett, Phys. Rev. Lett. **68** 3121 (1992).

[27] B. Schumacher, Phys. Rev. A**51**, 2738 (1995).

[28] R. B. Ash, “Information theory”, Dover Publication, (1965).

[29] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin und W. K. Wootters, Phys. Rev. A**54**, 3824 (1996).

[30] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres und W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[31] M. Horodecki, P. Horodecki und R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).

[32] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin und W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[33] D. Deutsch, A. Ekert, R. Jozsa, Ch. Macchiavello, S. Popescu und A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[34] P. Horodecki, M. Horodecki und R. Horodecki. Phys. Rev. Lett. **82**, 1056 (1999).

[35] D. Jonathan und M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).

[36] Jens Eisert und Martin Wilkens /quant-ph9912080.

[37] A. Elitzur und L. Vaidman, “Quantum mechanical interaction-free measurements”, Tel-Aviv University preprint (1991).

[38] A. Elitzur und L. Vaidman, Found. Phys. **23**, 987 (1993).

[39] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger und M. Kasevich, Phys. Rev. Lett. **74**, 4763 (1995).

[40] E. H. du Marchie Van Voorthuysen, Am. J. Phys. **64**, 1504 (1996).

[41] M. Hafner und J. Summhammer, Phys. Lett. A**235**, 563 (1997).

[42] T. K. Tsegaye, E. Goobar, A. Karlson, G. Bjork, M. Y. Loh und K. H. Lim, Phys. Rev. A**57**, 3987 (1998).

[43] P. G. Kwiat, A. G. White, J. R. Mitchell, O. Nairz, G. Weihs, H. Weinfurter und A. Zeilinger, Phys. Rev. Lett. **83**, 4725 (1999).

[44] L. D. Landau und R. Peierls. Z. Phys. **69** 56 (1931).

[45] V. B. Braginsky, Y. I. Vorontsov und K. S. Thorne, Science **209**, 547 (1980).

[46] A. La Porta, R. E. Slusher und B. Yurke, Phys. Rev. Lett. **62**, 28 (1989).

[47] H. A. Haus, K. Watanabe und Y. Yamamoto, J. Opt. Soc. Am. B**6**, 1138 (1989).

[48] P. Grangier, J. F. Roch und G. Roger, Phys. Rev. Lett. **66**, 1418 (1991).

[49] A. Shimizu, Phys. Rev. A**43** 3819 (1991).

[50] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935).

[51] B. Kraus, J. I. Cirac, S. Karnas und M. Lewenstein quant-ph/9912010.

[52] M. Lewenstein, J. I. Cirac und S. Karnas, /quant-ph9903012.

[53] J. M. Jauch und C. Piron, Helv. Phys, Acta **40**, 559 (1967).

[54] E. B. Davies und J. T. Lewis, Comm. Math. Phys. **17**, 239 (1970).

[55] E. B. Davies und J. T. Lewis, IEEE Trans. Inform. Theory **IT-24**, 596 (1978).

[56] A. Peres, “Quantum Theory: Concepts and Methods”, Kluwer Academic Publishers (1995).

[57] M. Brooks, “Quantum computing and communications”, Springer (1999).

[58] H. Lo, S. Popescu und T. Spiller,”Quantum computing and communications “, World Scientific (1998).

[59] D. Bouwmeester, A. Ekert und A. Zeilinger, “The Physics of Quantum Information”, Springer (2000).

[60] A. Einstein, B. Podolsky und N. Rosen, Phys. Rev. **47**, 777 (1935).

[61] J.S. Bell, “ On the Einstein Podolsky Rosen Experiment”, Physics **1**, 195 (1964).

[62] A. Peres, quant-ph/9807017.

[63] A. Garg und N. D. Mermin, Foundations of Physics **14**, 1 (1984).

[64] J. F. Clauser, M. A. Horne, A. Shimony und R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[65] J. F. Clauser und A. Shimony, Rep. Prog. Phys. **41**, 1881 (1978).

[66] A. Aspect, J. Dalibard und G. Roger, Phys. Rev. Lett. **49** (1982).

[67] Y. H. Shih und C. O. Alley, Phys. Rev. Lett. **61**, 2921 (1988).

[68] J. G. Rarity und P. R. Tapster, Phys. Rev. Lett. **64**, 2495 (1990).

[69] R. Werner, Phys. Rev. A**40** 4277, (1989).

[70] A. Peres Phys. Rev. Lett. **76** 1413, (1996).

[71] M. Horodecki, P. Horodecki und R. Horodecki, Phys. Lett. A**223**, 1 (1996).

[72] P. Horodecki Phys. Lett. A**232**, 333 (1997).

[73] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin und B. M. Terhal, Phys. Rev. Lett. **83**, 3081 (1999).

[74] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin und B. M. Terhal, quant-ph/9908070.

[75] C. H. Bennett, D. P. DiVincenzo, Ch. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin und W. K. Wootters, quant-ph/9804053.

[76] R. Horodecki, M. Horodecki und P. Horodecki, quant-ph/9811004.

[77] D. Bruß und A. Peres, Phys. Rev A**61**, 30301(R) (2000).

[78] D. Luenberger, “Introduction to Linear and Nonlinear Programming”, Addison-Wesley (1984).

[79] D. Gale, “The Theory of Linear Economic Models”, MC Graw-Hill, New York, (1960).

[80] S. L. Woronowicz, Rep. Math. Phys. **10**, 165 (1976).

[81] G. Lindblad, Comm. Math. Phys. **40**, 147 (1975).

[82] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter und A. Zeilinger, Natutr **390**, 575 (1997).

[83] D. Boschi, S. Branca, F. De Martini, L. Hardy und S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[84] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble und E. S. Polzik, Science **282**, 706 (1998).

[85] M. Nielsen, E. Knill und R. Laflamme, Nature **395**, 5 (1998).

[86] W. K. Wootters und W. H Zurek, Nature **299**, 802 (1982).

[87] D. Dieks, Phys. Letters A**92**, 271 (1982).

[88] D. Bruß, A. Ekert und C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

[89] W. Dür, H. J. Briegel, J.I. Cirac und P. Zoller, Phys. Rev. Lett. **80**, 2988 (1998).

[90] M. Horodecki, P. Horodecki und R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[91] W. Dür, J.I. Cirac, M. Lewenstein und D. Bruss, Phys. Rev. A**61**, 62313 (2000).

[92] C. S. Yannoni, M. H. Sherwood, L. M. K. Vandersypen, D. C. Miller, M. G. Kubinec und I. L. Chuang, Appl. Phys. Lett. **22**, 3563 (1999).

[93] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[94] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin und W. K. Wootters, Phys. Rev. A**54**, 3824 (1996).

[95] V. Vedral und M. B. Plenio, Phys. Rev. A**57**, 3 (1998).

[96] G. Vidal, J. Mod. Opt. **47**, 355 (2000).

[97] G. Vidal und R. Tarrach, Phys.Rev. A**59**, 141 (1999).

[98] R. I. Werner und K. G. H. Vollbrecht, quant-phy/0006046.

[99] M. Horodecki, P. Horodecki und R. Horodecki, Phys. Rev. Lett. **85**, 433 (2000).

[100] B.G. Englert und N. Metwally, quant-ph 9912089.

[101] B.G. Englert und N. Metwally, quant-ph 0007053.

[102] A. Sanpera, R. Tarrach und G. Vidal, Phys. Rev. A**58**, 826 (1998).

[103] P. Horodecki, M. Lewenstein, G. Vidal und I. Cirac, Phys. Rev. A**62**, 32310 (2000).

[104] M. Horodecki, P. Horodecki und R. Horodecki, Phys. Lett. A**223**, 8 (1996).

[105] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972).

[106] B. terhal, quant-ph 9810091.

[107] M. Lewenstein, B. Kraus, J.I. Cirac und P. Horodecki, quant-phy/0005014.

[108] M. Lewenstein, B. Kraus, J.I. Cirac und P. Horodecki, quant-phy/0005112.

[109] B. M. Terhal, Phys. Lett. A**271**, 319 (2000).

[110] M. Horodecki und P. Horodecki, Phys. Rev. A**52**, 4206 (1999).

Danksagungen

Zunächst möchte ich mich bei Herrn Prof. Dr. Maciej Lewenstein für die Vergabe des Themas, die hervorragende Betreuung und für die wertvollen physikalischen Kenntnisse, die ich durch Ihn erworben habe, bedanken.

Ebenfalls möchte ich mich bei Prof. Dr. Ignacio Cirac und Frau Barbara Kraus aus der Arbeitsgruppe in Innsbruck für die fruchtvolle Zusammenarbeit am $C^2 \otimes C^N$-Problem bedanken.

Danken möchte ich auch Frau Dr. Anna Sanpera und Frau Dr. Dagmar Bruß für viele interessante Diskussionen und Anregungen zum Thema der Quanteninformationstheorie. Weiterhin bedanke ich mich bei der gesamten Arbeitsgruppe für die letzten wundervoll verbrachten Jahre an der Universität Hannover.

Ein besonderes Dankeschön richte ich an Herrn Prof. Dr. Martin Wilkens, meinen Koreferenten, für die Zeit, die er sich genommen hat, diese Arbeit zu lesen und zu bewerten.

Meiner Frau Marijana Karnas danke ich für das mühselige Korrekturlesen.

Ihnen allen gilt mein Dank!