

Jahrbuch der  
Heinrich-Heine-Universität  
Düsseldorf  
**2004**

*Heinrich-Heine*

HEINRICH HEINE  
UNIVERSITÄT  
DÜSSELDORF



*Heinrich-Heine*

ISBN 3-9808514-3-5

- LEWENSTEIN, M., D. BRUSS, J.I. CIRAC, B. KRAUS, M. KUS, J. SAMSONOWICZ, A. SANPERA und R. TARRACH, „Separability and distillability in composite quantum systems – a primer“, *Journal of Modern Optics* 47 (2000), 2841.
- PERES, A., „Separability Criterion for Density Matrices“, *Physical Review Letters* 77 (1996), 1413.
- SCHRÖDINGER, E., „Die gegenwärtige Situation in der Quantenmechanik“, *Naturwissenschaften* 23 (1935), 807.
- SHOR, P., „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer“, *Proceedings of the 35<sup>th</sup> Annual Symposium on Foundations in Computer Science* (1994), 124.
- TERHAL, B., „Bell inequalities and the separability criterion“, *Physics Letters A* 271 (2000), 319.
- WERNER, R., „Quantum States With Einstein-Podolsky-Rosen Correlations Admitting a Hidden-Variable Model“, *Physical Review A* 40 (1989), 4277.

### Danksagung

Die in diesem Überblick vorgestellten Arbeiten entstanden gemeinsam mit etlichen Kollegen und Mitarbeitern. Besonders möchte ich mich für die intensive Zusammenarbeit bei Otfried Gühne, Philipp Hyllus, Maciej Lewenstein, Anna Sanpera und Harald Weinfurter bedanken. Weiter danke ich den Mitarbeitern meines Lehrstuhls, Herrmann Kampermann, Matthias Kleinmann, Tim Meyer und Patrick Skwara, für vielfältige Anregungen, spannende Diskussionen und die „Enlightenment-of-the-day-Liste“.

Für finanzielle Unterstützung sei der Deutschen Forschungsgemeinschaft (Schwerpunktprogramm QIV) und der EU (QUPRODIS, Projekt IST 2001-38877; SECOQC, Projekt IST 2002-506813) gedankt.

### Literatur

- ACIN, A., D. BRUSS, M. LEWENSTEIN und A. SANPERA. „Classification of mixed three-qubit states“, *Physical Review Letters* 87 (2001), 040401.
- BELL, J.S. „On the Einstein-Podolski-Rosen Paradox“, *Physics* 1 (1964), 195.
- BENNETT, C.H. und G. BRASSARD. „Quantum Cryptography: Public Key Distribution and Coin Tossing“, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, Indien (IEEE, New York, 1984), 175-179.
- BENNETT, C.H., G. BRASSARD, C. CRÉPEAU, R. JOZSA, A. PERES und W.K. WOOTTERS. „Teleporting an unknown quantum state via dual classical and Einstein-Podolski-Rosen channels“, *Physical Review Letters* 70 (1993), 1895.
- BOURENNANE, M., M. EIBL, C. KURTSIEFER, S. GAERTNER, H. WEINFURTER, O. GÜHNE, P. HYLLUS, D. BRUSS, M. LEWENSTEIN und A. SANPERA. „Witnessing multipartite entanglement“, *Physical Review Letters* 92 (2004), 087902.
- BRUSS, D. „Characterizing Entanglement“, *Journal of Mathematical Physics* 43 (2002), 4237.
- BRUSS, D., J.I. CIRAC, P. HORODECKI, F. HULPKE, B. KRAUS, M. LEWENSTEIN und A. SANPERA. „Reflections upon separability and distillability“, *Journal of Modern Optics* 49 (2002), 1399-1418.
- BRUSS, D. *Quanteninformation*. Frankfurt am Main 2003.
- BRUSS, D., G.M. D'ARIANO, M. LEWENSTEIN, C. MACCHIAVELLO, A. SEN DE und U. SEN. „Distributed quantum dense coding“, *Physical Review Letters* 93 (2004), 210501.
- CLAUSER, J., M. HORNE, A. SHIMONY und R. HOLT. „Proposed Experiment to Test Local Hidden-Variable Theories“, *Physical Review Letters* 23 (1969), 880.
- DÜR, W., G. VIDAL und I. CIRAC. „Three qubits can be entangled in two inequivalent ways“, *Physical Review A* 62 (2000), 062314.
- GÜHNE, O., P. HYLLUS, D. BRUSS, A. EKERT, M. LEWENSTEIN, C. MACCHIAVELLO und A. SANPERA. „Detection of entanglement with few local measurements“, *Physical Review A* 66 (2002), 062305.
- HORODECKI, M., P. HORODECKI und R. HORODECKI. „Separability of mixed states: Necessary and Sufficient conditions“, *Physical Letters A* 223 (1996), 1.
- HYLLUS, P., O. GÜHNE, D. BRUSS und M. LEWENSTEIN. „Relations between Entanglement Witness and Bell Inequalities“, *Physical Review A* 72 (2005), 012321.
- LEWENSTEIN, M., B. KRAUS, J.I. CIRAC und P. HORODECKI. „Optimization of entanglement witnesses“, *Physical Review A* 62 (2000), 052310.

Abbildung 4 zeigt. In diesem Experiment wurden verschränkte Zustände polarisierter Photonen mit Hilfe von parametrischer Fluoreszenz erzeugt. Die Messung in verschiedenen Richtungen erfolgt einfach durch unterschiedliche Orientierung von Polarisatoren vor den Detektoren.

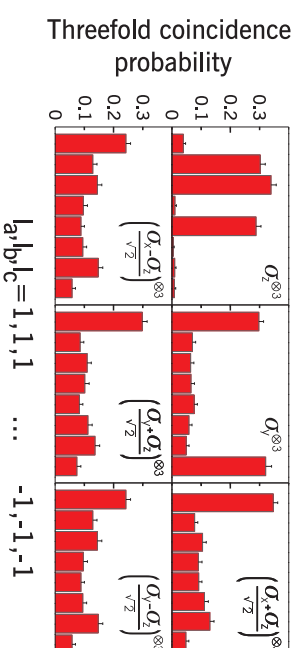


Abb. 4: Konzidenzmessungen für einen W-Zeugen für drei Qubits. Die Reihenfolge der Basiselemente ist 000, 001, 010 usw. Im linken oberen Kasten erkennt man die Form des W-Zustands wie in (5). Die Messrichtungen sind durch die Angaben der Pauli-Operatoren  $\sigma_{x,y,z}$  beschrieben.

Der gemessene Erwartungswert des Zeugen für den W-Zustand ist  $T_{Tr}(W_w \rho) = -0.197 \pm 0.018$ , wobei theoretisch  $T_{Tr}(W_w \rho) = -\frac{1}{3}$  erwartet wurde. Damit wurde echte Mehrteilchenverschränkung zweifelsfrei nachgewiesen. Die Verschiebung des experimentellen gegenüber dem theoretischen Wert kommt durch Rauschen zustande. Die Messung einer Bell-Ungleichung für Mehrteilchensysteme hatte hier nicht zu einer Verletzung geführt. Dies zeigt deutlich, dass die Methode der Zeugenoperatoren der Methode der Bell-Ungleichungen überlegen ist. Ferner wurde auch die echte Vielteilchenverschränkung eines bestimmten Vier-Photonen-Zustands mittels eines Zeugenoperators nachgewiesen. In diesem Fall ist keine Bell-Ungleichung bekannt, die diese Verifizierung erbringen könnte. Es soll noch einmal betont werden, dass Zeugenoperatoren eine zuverlässige Methode für den Nachweis von Verschränkung eines beliebigen Zustands darstellen, wenn man bereits eine gewisse Information über diesen Zustand hat.

### Zusammenfassung

Im Rahmen der Quanteninformationstheorie wurde die neue Methode der Zeugenoperatoren entwickelt, die es erlaubt, Verschränkung theoretisch zu klassifizieren und experimentell zu detektieren. Mit dem kürzlich erfolgten Nachweis von echter Mehrteilchenverschränkung gelang der Brückenschlag von einem abstrakten mathematischen Konzept zu seiner Implementierung im Labor. Wir sind jedoch noch weit von einem vollständigen Verständnis des Phänomens der Verschränkung in höherdimensionalen und multipartiten Quantensystemen entfernt – es bleiben genügend Fragen offen.

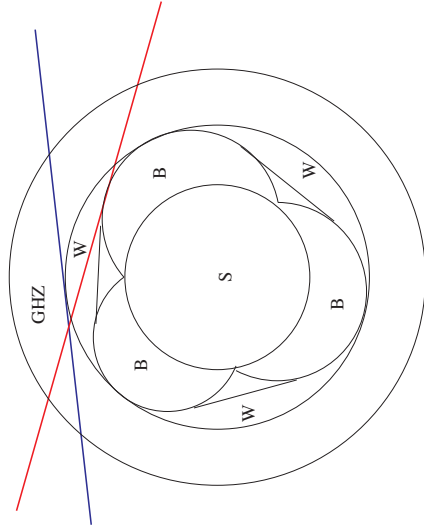


Abb. 3: Klassifizierung von gemischten Drei-Qubit-Zuständen: Menge der separablen (S), biseparablen (B), W- und GHZ-Zustände. Ein optimierter GHZ-Zeuge ist in Blau eingezeichnet, ein optimierter W-Zeuge in Rot.

Die Klassifizierung von gemischten Drei-Qubit-Zuständen mittels Zeugenoperatoren wurde in Acin *et al.* (2001) beschrieben und ist in Abbildung 3 dargestellt. Es wurde gezeigt, dass es vier ineinander eingebettete konvexe Mengen von Zuständen gibt: separable (S), biseparable (B), W- und GHZ-Zustände. Gemischte W-Zustände können nicht in einer Zerlegung geschrieben werden, die nur separable und biseparable Zustände enthält, sondern erfordern mindestens einen reinen W-Zustand in der Mischung. Entsprechendes gilt für GHZ-Zustände.

Nun kann man, in Erweiterung des oben beschriebenen Konzepts der Zeugenoperatoren für bipartite Systeme, Zeugenoperatoren für die verschiedenen verschränkten Untermen- gen konstruieren. In Abbildung 3 ist in Blau ein optimierter GHZ-Zeuge eingezeichnet, der einen negativen Erwartungswert für einige GHZ-Zustände hat, jedoch einen positiven Erwartungswert für die Klassen W, B und S. Ebenso kann ein W-Zeuge (hier in Rot) konstruiert werden, der positiv auf B und S ist, jedoch im Allgemeinen nicht zwischen W und GHZ unterscheiden kann. Ein explizites Beispiel für einen W-Zeugen ist

$$(7) \quad W_w = \frac{2}{3}1 - |W\rangle\langle W|,$$

der eine ähnliche Gestalt wie in (3) und per Konstruktion die erforderlichen Eigenschaften hat. Einen multipartiten Zeugenoperator kann man nun wiederum in eine Summe aus *lokalen* Operatoren zerlegen und dann im Experiment den Erwartungswert des Zeugen bestimmen. Ist beispielsweise der Erwartungswert eines GHZ-Zeugen negativ, ist dies eine eindeutige Signatur für echte Drei-Teilchen-Verschränkung und zeigt insbesondere, dass der erzeugte Zustand in der GHZ-Klasse liegt. Ein Beispiel für die Ergebnisse der Konzidenzmessungen für den Zeugen  $W_w$  aus dem Experiment von H. Weinfurter ist in

# Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2004

Herausgegeben vom Rektor  
der Heinrich-Heine-Universität Düsseldorf  
Univ.-Prof. Dr. Dr. Alfons Labisch

Konzeption und Redaktion:  
em. Univ.-Prof. Dr. Hans Stüssmuth

benötigten Messrichtungen. So reicht es beispielsweise für den Nachweis der Verschränkung eines Werner-Zustands aus, dass Alice und Bob nur drei korrelierte Messrichtungen verwenden.

### Nachweis von Vielteilchenverschränkung

Kürzlich wurde das Konzept der Zeugenoperatoren im Experiment von H. Weinfurter in München eingesetzt, um erstmalig echte Vielteilchenverschränkung gewisser Zustände nachzuweisen.<sup>13</sup> Bisher wurde in diesem Artikel nur beschrieben, wie man bipartite Verschränkung (d. h. Verschränkung eines in zwei Subsysteme unterteilten Gesamtsystems) nachweist. Zeugenoperatoren kann man aber auch für die Klassifizierung und den Nachweis von multipartiter Verschränkung (d. h. Vielteilchenverschränkung) konstruieren und einsetzen. „Echte“ Vielteilchenverschränkung liegt vor, wenn alle Subsysteme untereinander verschränkt sind und der Zustand nicht als Mischung biseparabler Zustände (mit möglicherweise unterschiedlichen Partitionen) geschrieben werden kann.

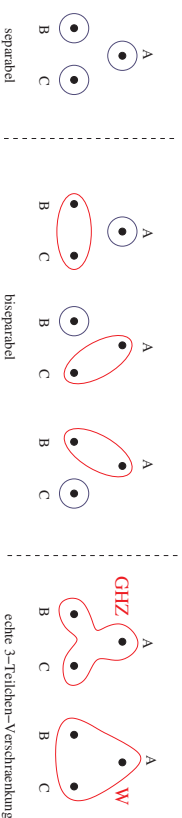


Abb. 2: Verschiedene Verschränkungsklassen für drei Qubits.

In Abbildung 2 ist die Idee der echten Vielteilchenverschränkung für drei Qubits symbolisch dargestellt: Ist keines der drei Subsysteme A, B und C mit einem anderen verschränkt, so nennt man den Zustand separabel. Sind zwei der drei Subsysteme verschränkt, nicht jedoch das dritte, nennt man den Zustand biseparabel. Hier gibt es drei Kombinationsmöglichkeiten. Ein gemischter biseparabler Zustand kann aus Summanden mit unterschiedlichen Partitionen bestehen. Schließlich gibt es zwei Klassen von Zuständen mit echter Drei-Qubit-Verschränkung, die W- und die GHZ-Zustände. Reine W-Zustände haben die Gestalt

$$(5) |W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle),$$

und reine GHZ-Zustände sind von der Form

$$(6) |GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

W- und GHZ-Zustände sind inäquivalent, d. h., sie können nicht durch lokale Transformationen ineinander überführt werden, wie in Dür *et al.* (2000) gezeigt wurde.

<sup>13</sup> Vgl. Bourennane *et al.* (2004).

© Heinrich-Heine-Universität Düsseldorf 2005  
 Einbandgestaltung: Wiedemeier & Martin, Düsseldorf  
 Titelbild: Schloss Mieckeln, Tagungszentrum der Universität  
 Redaktionsassistent: Georg Stütgen  
 Beratung: Friedrich-K. Unterweg  
 Satz: Friedhelm Sowa, L<sup>A</sup>T<sub>E</sub>X  
 Herstellung: WAZ-Druck GmbH & Co. KG, Duisburg  
 Gesetzt aus der Adobe Times  
 ISBN 3-9808514-3-5

liegen auf der Hyperebene. Alle Zustände auf einer Seite der Hyperebene führen zu einem negativen Skalarprodukt  $\text{Tr}(W\sigma)$ , d. h. zu einem negativen Erwartungswert des Operators  $W$ , alle Zustände auf der anderen Seite zu einem positiven Erwartungswert. In Abbildung 1 sind diejenigen Zustände, die durch den Zeugenoperator  $W$  detektiert werden, als blau schraffierter Bereich angegeben. Über die verbleibenden Zustände kann dieser Zeuge keine Aussage treffen: Sie sind entweder separabel oder verschränkt. Zeugenoperatoren liefern ein notwendiges und hinreichendes Kriterium für Verschränktheit: Ein Zustand  $\rho$  ist genau dann verschränkt, wenn ein hermitescher Zeugenoperator  $W$  existiert, für den  $\text{Tr}(W\rho) < 0$  ist, wobei für alle separablen Zustände  $\rho_{sep}$  gilt, dass  $\text{Tr}(W\rho_{sep}) \geq 0$  ist. In der Praxis sind Zeugenoperatoren vor allem dann nützlich, wenn man weiß, wie der Zustand  $\rho$  „ungefähr“ aussieht. Dies ist ja die typische Situation in einem Experiment, in dem man einen gewissen Zustand erzeugen will, der aber durch Imperfektionen der Apparatur oder Wechselwirkung mit der Umgebung leicht verrauscht ist. Wenn man keinerlei Information über den Zustand hat, muss man im Allgemeinen unendlich viele Zeugen konstruieren, um ihn zu detektieren.

Zeugenoperatoren wurden erstmals in Terhal (2000) vorgeschlagen. Systematische Konstruktionsverfahren und die Optimierung von Zeugen wurden in Lewenstein *et al.* (2000) diskutiert. Ein optimierter Zeuge  $W_{opt}$  ist tangential an der Menge der separablen Zustände, und es gibt keinen Zeugen, der zusätzlich zu den von  $W_{opt}$  detektierten Zuständen noch weitere Zustände als verschränkt nachweist.

Ein einfaches Beispiel für einen Zeugenoperator, der den verschränkten Zustand  $|\Psi\rangle$  detektiert, ist gegeben durch

$$(3) \quad W_{|\Psi\rangle} = x \cdot 1 - |\Psi\rangle\langle\Psi|,$$

wobei  $x$  gleich dem maximalen quadrierten Überlapp von  $|\Psi\rangle$  mit einem reinen separablen Zustand ist. Man kann sich leicht davon überzeugen, dass  $\text{Tr}(W_{|\Psi\rangle}\langle\Psi|) = x - 1 < 0$  gilt, aber  $\text{Tr}(W_{|\Psi\rangle}\rho_{sep}) = x - \langle\Psi|\rho_{sep}|\Psi\rangle \geq 0$  ist. Somit ist gezeigt, dass  $W$  den Zustand  $|\Psi\rangle$  detektiert, aber auf allen separablen Zuständen positiv ist.

### Experimentelle Implementierung der Zeugenoperatoren

Das abstrakte mathematische Konzept der Zeugenoperatoren kann auf einfache Weise im Experiment eingesetzt werden: Der Erwartungswert der Observablen  $W$  im Zustand  $\rho$  muss gemessen werden. Ist dieser Erwartungswert negativ, so ist dies ein zweifelsfreier Nachweis für Verschränkung. Die Spektralzerlegung von  $W$  enthält zwar einen verschränkten Zustand, man kann jedoch immer auch eine lokale Zerlegung von  $W$  finden (eine so genannte Pseudomischung, da mindestens ein Koeffizient in der Zerlegung negativ ist, im Gegensatz zu der lokalen Zerlegung eines positiv semidefiniten Operators wie in (1)). Eine Pseudomischung ist also von der Gestalt

$$(4) \quad W = \sum_k c_k |a_k\rangle\langle a_k| \otimes |b_k\rangle\langle b_k|; \quad c_k \in \mathbf{R}; \quad \sum_k c_k = 1, \quad \text{wobei mindestens ein } c_k < 0 \text{ ist.}$$

In Gühne *et al.* (2002) wird beschrieben, wie man Zeugenoperatoren konstruiert und eine optimale lokale Zerlegung findet. Optimierte wurden hier in Bezug auf die Anzahl der

## Inhalt

<b>Vorwort des Rektors</b> .....	11
<b>Gedenken</b> .....	15
<b>Rektorat</b> .....	17
ALFONS LABISCH (Rektor)	
Autonomie der Universität –	
Ein Leitbild für die Heinrich-Heine-Universität Düsseldorf .....	19
VITTORIA BORSÒ	
Internationalisierung als Aufgabe der Universität .....	33
RAIMUND SCHIRMEISTER und LILJA MONIKA HIRSCH	
Wissenschaftliche Weiterbildung –	
Chance zur Kooperation mit der Wirtschaft? .....	51
<b>Medizinische Fakultät</b>	
<i>Dekanat</i> .....	65
<i>Neu berufene Professorinnen und Professoren</i> .....	67
WOLFGANG H.M. RAAB (Dekan)	
Die Medizinische Fakultät – Entwicklung der Lehre .....	77
THOMAS RUZICKA und CORNELIA HÖNER	
Das Biologisch-Medizinische Forschungszentrum .....	81
DIETER HAUSSINGER	
Der Forschungsschwerpunkt Hepatologie .....	87
IRMGARD FÖRSTER, ERNST GLEICHMANN,	
CHARLOTTE ESSER und JEAN KRUTMANN	
Pathogenese und Prävention von umweltbedingten	
Erkrankungen des Immunsystems .....	101
MARKUS MÜSCHEN	
Illusionäre Botschaften in der	
malignen Entartung humaner B-Lymphozyten .....	115

**Mathematisch-Naturwissenschaftliche Fakultät**

Dekant.....	127
<i>Neu berufene Professorinnen und Professoren</i> .....	129
PETER WESTHOFF (Dekan) Die Mathematisch-Naturwissenschaftliche Fakultät – Was hat das Jahr 2004 gebracht? .....	141
DIETER WILLBOLD Die Rolle des Forschungszentrums Jülich für die Mathematisch-Naturwissenschaftliche und die Medizinische Fakultät der Heinrich-Heine-Universität Düsseldorf .....	147
DAGMAR BRUSS Verschränkt oder separabel? Moderne Methoden der Quanteninformationstheorie .....	155
STEPHANIE LÄER Arzneimitteltherapie bei Kindern – Eine Herausforderung besonderer Art für Forschung und Praxis .....	167
HILDEGARD HAMMER „Vor dem Abitur zur Universität“ – Studium für Schülterinnen und Schüler an der Heinrich-Heine-Universität Düsseldorf .....	183
<b>Philosophische Fakultät</b>	
Dekant.....	195
<i>Neu berufene Professorinnen und Professoren</i> .....	197
BERND WITTE (Dekan) Zur Lage von Forschung und Lehre an der Philosophischen Fakultät .....	203
WOLFGANG SCHWENTKER Geschichte schreiben mit Blick auf Max Weber: Wolfgang J. Mommsen .....	209
DETLEF BRANDES „Besinnungsloser Taumel und maßlose Einschüchterung“: Die Studentendutschen im Jahre 1938 .....	221
ANDREA VON HÜLSEN-ESCH, HANS KÖRNER und JÜRGEN WIENER Kunstgeschichte an der Heinrich-Heine-Universität Düsseldorf – Innovationen und Kooperationen .....	241
GERHARD SCHURZ Der Mensch – Ein Vernunftwesen? Kognition und Rationalität aus evolutions-theoretischer Sicht .....	249

so genannten Werner-Zustände – sind eine Mischung aus einem maximal verschränkten Zustand, z. B. dem Singlet, und der Identität. Zum anderen sind Bell-Ungleichungen nur schlecht geeignet, um echte Vielteilchenverschränkung nachzuweisen: mehr dazu in den folgenden Abschnitten.

**Zeugenooperatoren**

Eine neue und sehr leistungsfähige Methode zum Nachweis von Verschränkung ist die Methode der so genannten Zeugenooperatoren. Sie nutzt die konvexe Struktur der Menge der Quantenzustände aus und ist in der Lage, mehr Zustände als mit Hilfe der Bell-Ungleichungen als verschränkt nachzuweisen.<sup>12</sup> Wie oben schon erwähnt, haben Dichtematrizen  $\rho$  die Eigenschaft, hermitesch, d. h.,  $\rho^\dagger = \rho$ , und positiv semidefinit, d. h.,  $\langle \Psi | \rho | \Psi \rangle \geq 0$ , zu sein. Ferner gilt die Normierung  $\text{Tr} \rho = 1$ . Jede Mischung (oder „konvexe Kombination“) aus zwei Dichtematrizen, d. h.,  $\rho = p_1 \rho_1 + p_2 \rho_2$  mit  $p_{1,2} \geq 0$  und  $p_1 + p_2 = 1$ , hat dieselben eben erwähnten Eigenschaften, ist also ebenfalls eine Dichtematrix. Anders ausgedrückt: Die Menge aller Dichtematrizen ist konvex. Auch die Menge der separablen Zustände, definiert durch Gleichung (1), ist konvex: Mischt man zwei separable Zustände, so erhält man wieder eine Summe von Tensorprodukten, also ebenfalls einen separablen Zustand. Diese konvexe Struktur ist in Abbildung 1 schematisch angedeutet. Die Frage „verschränkt oder separabel“ ist gleichbedeutend mit der Frage, ob ein Quantenzustand zur Menge der separablen Zustände (S) gehört oder nicht (die Menge der verschränkten Zustände ist mit E für Englisch *entanglement* abgekürzt).

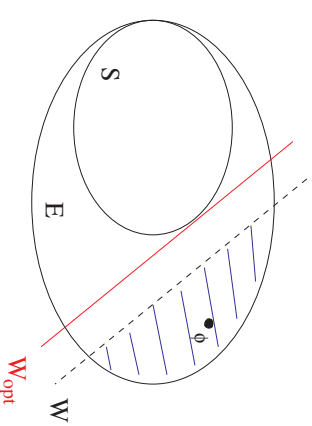


Abb. 1: Menge der separablen (S) und verschränkten (E) Zustände. Der verschränkte Zustand  $\phi$  wird durch den Zeugen  $w$  detektiert. Der Operator  $w$  definiert die eingezeichnete gestrichelte Hyperebene und detektiert alle Zustände im blau schraffierten Bereich. Die rote Hyperebene ist durch einen optimalen Zeugen  $w_{\text{opt}}$  definiert.

Liegt der Zustand  $\phi$  in der Menge der verschränkten Zustände, so existiert eine Hyperebene, die ihn von der Menge S trennt. (Dies ist eine Konsequenz des Hahn-Banach-Theorems.) Eine Hyperebene kann durch einen so genannten Zeugenooperator  $w$  (engl.: *witness operator*), der hermitesch ist, beschrieben werden: Alle Zustände  $\sigma$  mit  $\text{Tr}(w\sigma) = 0$

<sup>12</sup> Vgl. Hylilus *et al.*, (2005).

Gegensatz zur freien Verschränkung von Zuständen mit nicht-positiver Transponierter – die Verschränkung mehrerer identischer Zustände nicht durch lokale Operationen zu höherer Verschränkung einer geringeren Zahl von Zuständen *destilliert* werden kann.

## Bell-Ungleichungen

Wie weist man experimentell nach, ob ein erzeugter Zustand  $\rho$  auch tatsächlich verschränkt ist? Eine Methode ist die Zustandstomographie, bei der man alle Elemente der Dichtematrix vermisst und dann auf theoretische Separabilitätsargumente zurückgreift. Für höherdimensionale Systeme ist dies aber ein zu aufwändiges Verfahren, denn im Allgemeinen ist es nicht notwendig, jeden Eintrag der Dichtematrix zu kennen, um die Frage „verschränkt oder separabel“ beantworten zu können. Ein bekanntes Verfahren ist ein Test der Bell-Ungleichungen, die 1964 von J. Bell vorgeschlagen wurden.<sup>10</sup> Ausgehend von einer rein klassischen Argumentation wird der unter Annahme einer lokalen Theorie maximal erreichbare Erwartungswert eines bestimmten Korrelationsoperators angegeben. Wird bei einer Messung der Korrelation eines verschränkten Quantenzustands diese Obergrenze überschritten (d. h., die entsprechende Bell-Ungleichung ist verletzt), so ist damit nachgewiesen, dass es sich nicht um einen Zustand handelt, der mit Hilfe einer Theorie mit lokalen verborgenen Parametern erklärt werden kann. Besonders einfach lässt sich die Idee der Bell-Ungleichungen am Beispiel der so genannten CHSH-Ungleichungen,<sup>11</sup> benannt nach J. Clauser, M. Horne, A. Shimony und R. Holt, erklären: Seien  $A, A', B$  und  $B'$  Variablen, die die Werte  $a, a', b, b' = \pm 1$  annehmen können. Dann gilt sicher  $a(b+b') + a'(b-b') = \pm 2$ . Mittelt man diese Gleichung über mehrere Zuordnungen von Werten, so erhält man  $|\langle a(b+b') + a'(b-b') \rangle| \leq 2$ , wobei  $\langle ab \rangle$  den gemittelten Wert von  $ab$  bezeichnet. Dies ist schon die CHSH-Ungleichung:

$$(2) \quad S = |\langle ab \rangle + \langle ab' \rangle + \langle a'b \rangle - \langle a'b' \rangle| \leq 2.$$

Bisher war dies eine rein klassische Argumentation. Seien nun  $A, A', B$  und  $B'$  quantenmechanische Observablen, die etwa Projektionsmessungen (wie z. B. im Stern-Gerlach-Versuch) in bestimmten Spin-Richtungen  $\vec{\alpha}, \vec{\alpha}', \vec{\beta}$  und  $\vec{\beta}'$  beschreiben. Auch hier ist das Ergebnis jeder einzelnen Messung wieder  $\pm 1$ .

Wenn man die Messung jedoch an einem verschränkten Zustand durchführt, z. B. dem Singlett  $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ , und die Messrichtungen  $\vec{\alpha}$  und  $\vec{\alpha}'$  für Alice,  $\vec{\beta}$  und  $\vec{\beta}'$  für Bob geschickt wählt, so findet man  $S_{|\Psi^-\rangle} = 2\sqrt{2} > 2$ , also eine Verletzung der CHSH-Ungleichung. Es ist also unmöglich, die Messdaten mit einer klassischen Theorie, etwa unter Zuhilfenahme zusätzlicher (so genannter verborgener) Parameter zu erklären. Somit stellen Bell-Ungleichungen eine Möglichkeit dar, die quantenmechanische Natur eines gegebenen Zustands nachzuweisen.

Die Methode der Bell-Ungleichungen ist jedoch nur bedingt zum Nachweis von Verschränkung geeignet: Zum einen gibt es sogar in Systemen, die aus zwei Qubits zusammengesetzt sind, verschränkte Zustände, die kompatibel mit der Annahme von lokalen verborgenen Parametern sind, also keine Bell-Ungleichung verletzen. Diese Zustände – die

<sup>10</sup> Vgl. Bell (1964).

<sup>11</sup> Vgl. Clauser *et al.* (1969).

RALPH WEISS	Medien – Im blinden Fleck öffentlicher Beobachtung und Kritik? .....	265
REINHOLD GÖRLING	Medienkulturwissenschaft – Zur Aktualität eines interdisziplinären Faches .....	279
BERND WITTE	Deutsch-jüdische Literatur und literarische Moderne. Prolegomena zu einer deutsch-jüdischen Literaturgeschichte .....	293
<b>Gastbeitrag</b>		
WOLFGANG FRÜHWALD	Das Geschenk, „nichts erklären zu müssen“. Zur Neugründung eines Instituts für Jüdische Studien .....	307
<b>Wirtschaftswissenschaftliche Fakultät</b>		
<i>Dekanat</i> .....		321
<i>Neu berufene Professorinnen und Professoren</i> .....		323
HEINZ-DIETER SMEETS und H. JÖRG THIEME (Dekan)	Der Stabilitäts- und Wachstumspakt – Lästiges Übel oder notwendige Schranke? .....	325
GUIDO FÖRSTER	Verlustverrechnung im Beteiligungskonzern .....	341
ALBRECHT F. MICHLEER	Die Effizienz der Fiskalpolitik in den Industrieländern .....	363
GERD RAINER WAGNER, RÜDIGER HAHN und THOMAS NOWAK	Das „Montréal-Projekt“ – Wirtschaftswissenschaftliche Kompetenz im internationalen Studienwettbewerb .....	381
<b>Juristische Fakultät</b>		
<i>Dekanat</i> .....		393
<i>Neu berufene Professorinnen und Professoren</i> .....		395
HORST SCHLEHOFER (Dekan)	Zehn Jahre Juristische Fakultät – Rückblick und Ausblick .....	397
ULRICH NOACK	Publizität von Unternehmensdaten durch neue Medien .....	405
DIRK LOOSCHELDERS	Grenzüberschreitende Kindesentführungen im Spannungsfeld von Völkerrecht, Europäischem Gemeinschaftsrecht und nationalem Verfassungsrecht .....	423

RALPH ALEXANDER LORZ	
Die unmittelbare Anwendbarkeit des Kindeswohl vorrangs nach Art. 3 Abs. 1 der UN-Kinderrechtskonvention im nationalen Recht . . . . .	437
<b>Gesellschaft von Freunden und Förderern der Heinrich-Heine-Universität Düsseldorf e.V.</b>	
OTHMAR KALTHOFF	
Jahresbericht 2004 . . . . .	459
<b>Forschergruppen der Heinrich-Heine-Universität Düsseldorf</b>	
SEBASTIAN LÖBNER	
Funktionalbegriffe und Frames – Interdisziplinäre Grundlagenforschung zu Sprache, Kognition und Wissenschaft . . . . .	463
HANS WERNER MÜLLER, FRANK BOSSE, PATRICK KÜRY, KERSTIN HASENPUSCH-THEIL, NICOLE KLAPKA UND SUSANNE GRESCHAT	
Die Forschergruppe „Molekulare Neurobiologie“ . . . . .	479
ALFONS SCHNITZLER, LARS TIMMERMANN, BETTINA POLLOK,	
MARKUS PLONER, MARKUS BUTZ UND JOACHIM GROSS	
Oszillatorische Kommunikation im menschlichen Gehirn . . . . .	495
MARKUS UHRBERG	
Natürliche Killerzellen und die Regulation der KIR-Rezeptoren . . . . .	509
<b>Institute an der Heinrich-Heine-Universität Düsseldorf – Das Deutsche Diabetes-Zentrum</b>	
GUIDO GIANI, DIRK MÜLLER-WIELAND und WERNER A. SCHERBAUM	
Das Deutsche Diabetes-Zentrum – Forschung und Klinik unter einem Dach . . . . .	521
WERNER A. SCHERBAUM, CHRISTIAN HERDER und STEPHAN MARTIN	
Interaktion von Inflammation, Lifestyle und Diabetes: Forschung an der Deutschen Diabetes-Klinik . . . . .	525
DIRK MÜLLER-WIELAND und JÖRG KOTZKA	
Typ-2-Diabetes und Metabolisches Syndrom als Folgen einer „entgleisten“ Genregulation: Forschung am Institut für Klinische Biochemie und Pathobiochemie . . . . .	533
GUIDO GIANI, HELMUT FINNER, WOLFGANG RATHMANN und	
JOACHIM ROSENBAUER	
Epidemiologie und Public Health des Diabetes mellitus in Deutschland: Forschung am Institut für Biometrie und Epidemiologie des Deutschen Diabetes-Zentrums . . . . .	537

$$(1) \rho = \sum_i p_i \rho_A^i \otimes \rho_B^i, \quad p_i \geq 0, \quad \sum_i p_i = 1,$$

dann ist  $\rho$  separabel. Wenn eine solche *lokale* Zerlegung nicht gefunden werden kann, dann ist  $\rho$  verschränkt. Die obige Definition eines separablen Zustands wurde von R. Werner eingeführt<sup>7</sup> und impliziert, dass er durch lokale Operationen (im jeweiligen Labor von Alice und Bob) und klassische Kommunikation hergestellt werden kann. Ein verschränkter Zustand kann nur durch *nicht-lokale* Operationen, also Wechselwirkungen zwischen den Untersystemen, erzeugt werden: Verschränkung impliziert Nicht-Lokalität.

Wie sieht man es einem gegebenen Zustand  $\rho$  an – sei es theoretisch oder experimentell –, ob er verschränkt ist? Vom theoretischen Standpunkt aus scheint dies einfach zu sein: Wenn man eine Zerlegung der Gestalt (1) angeben kann, ist  $\rho$  separabel. Das Problem ist jedoch, dass es zwar für einen separablen Zustand unendlich viele derartige Zerlegungen gibt (die jedoch oft nicht einfach zu finden sind), es aber im Allgemeinen sehr schwierig ist, für einen verschränkten Zustand zu zeigen, dass eine solche lokale Zerlegung nicht existiert. Nur für niedrigdimensionale Systeme ist das Separabilitätsproblem vollständig gelöst.<sup>8</sup>

Tatsächlich gibt es für Systeme, die aus zwei Qubits oder aus einem Qubit und einem Qutrit (Drei-Niveau-System) zusammengesetzt sind, ein einfaches Kriterium für die Entscheidung „verschränkt oder separabel“, das Kriterium der positiven partiellen Transponierten oder auch Peres-Horodecki-Kriterium.<sup>9</sup> Die partielle Transponierte einer Dichtematrix erhält man, indem man die Transponierte eines der beiden Untersysteme bildet. Ist ein Zustand separabel, lässt er sich also wie in Gleichung (1) zerlegen, so ist die partielle Transponierte in Bezug auf das Untersystem A gegeben durch

$$\rho^{T_A} = \sum_i p_i \rho_A^i{}^T \otimes \rho_B^i.$$

Dies ist wiederum eine „ordentliche“ Dichtematrix (d. h., sie hat die Spur 1, ist hermitesch, d. h.,  $\rho^\dagger = \rho$ , und positiv semidefinit, d. h., alle Eigenwerte sind nicht-negativ). Ist der Zustand jedoch verschränkt, so zeigt sich, dass die partielle Transponierte einen negativen Eigenwert hat. Dies ist unphysikalisch: Die partielle Transponierte eines verschränkten Zustands ist keine Dichtematrix. Wie kann die mathematische Vorschrift der partiellen Transponierten physikalisch interpretiert werden? Die Transposition einer Dichtematrix ist äquivalent zur Zeitumkehroperation. Die partielle Transposition ist somit äquivalent zur Zeitumkehr in einem Subsystem – eine unphysikalische Operation. Falls die Subsysteme quantenmechanisch korreliert sind, stellt die Nicht-Positivität der partiellen Transponierten eine Signatur für diese unphysikalische Operation dar. In höherdimensionalen Systemen ist die Positivität der partiellen Transponierten kein hinreichendes Kriterium für Separabilität mehr: Schon für ein aus zwei Qutrits zusammengesetztes System gibt es verschränkte Zustände mit positiver partieller Transponierter. Diese Art der Verschränkung bezeichnet man auch als *gebundene* Verschränkung. Sie heißt „gebunden“, weil – im

<sup>7</sup> Vgl. Werner (1989).

<sup>8</sup> Vgl. Lewenstein *et al.* (2000), Bruß (2002) sowie Bruß *et al.* (2002).

<sup>9</sup> Vgl. Peres (1996) sowie Horodecki *et al.* (1996).

Systeme) eine noch effizientere Methode zur dichten Kodierung liefern. Diese Frage führt zum Begriff der Kodierungskapazität eines gegebenen Quantenzustands. Ist etwa jeder verschränkte Zustand für die dichte Kodierung geeignet? Dies ist nicht der Fall: Wie gezeigt wurde,<sup>4</sup> gibt es verschränkte Zustände, die zwar nützlich für die Quantenteleportation sind, nicht jedoch für die dichte Kodierung. Eine Klassifizierung von Verschränkung hängt also davon ab, welches informationsverarbeitende Protokoll realisiert werden soll.

Ein wichtiger Meilenstein in der Entwicklung der Quanteninformation war der von P. Shor im Jahr 1994 entwickelte Quantenalgorithmus zur Primzahlzerlegung.<sup>5</sup> Shor zeigte, dass man mit Hilfe von Quantenphysik zur Faktorisierung einer großen Zahl eine Zeit benötigt, die nur *polynomial* mit der Anzahl ihrer Ziffern wächst. Der beste bekannte klassische Algorithmus dagegen hat exponentielle Komplexität. Die Möglichkeit dieses exponentiellen *Speed-ups* hat großes und anhaltendes Interesse an Quantenalgorithmen hervorgerufen. Auch wenn der Shor-Algorithmus bereits mit wenigen Qubits experimentell verwirklicht wurde, ist man jedoch noch weit von einer praktischen kommerziellen Anwendung entfernt. Dies gilt auch für den großen Traum in der Quanteninformation, den Quantencomputer. Immerhin kann man heutzutage schon einfache Quantengatter im Experiment realisieren und verschränkte Zustände von bis zu fünf Qubits erzeugen. Sehr erfolgreich sind hier Implementierungen in der Quantenoptik, so z. B. in einer Falle gefangene Ionen oder polarisierte Photonen. Das große Hindernis für den Quantencomputer, die Dekohärenz der fragilen verschränkten Zustände, kann zumindest theoretisch durch Quantenfehlerkorrektur überwunden werden.

Weitere interessante Themen der Quanteninformationstheorie, auf die hier jedoch nicht im Einzelnen eingegangen werden kann, sind Quantenkommunikationskomplexität, Präzisionsmessungen als Quantentechnologie, Quantenspiele, weitere Quantenalgorithmen, approximatives Quantenklonen und Zustandsabschätzung.

### Verschränkung versus Separabilität

Ein zentrales Konzept in der Quanteninformationstheorie ist das der Verschränkung. Die meisten informationsverarbeitenden Quantenprotokolle beruhen auf der Nutzung verschränkter Zustände. Der Begriff der Verschränkung wurde schon 1935 von E. Schrödinger<sup>6</sup> eingeführt und bezeichnet eine Eigenschaft zusammengesetzter Systeme: In der Quantenmechanik können Korrelationen auftreten, die – in gewisser Weise – stärker als alle klassischen Korrelationen sind. Diese Quantenkorrelationen nennt man Verschränkung. Diese seltsame Eigenschaft wurde in den frühen Jahren der Quantenmechanik als Mysterium gesehen (siehe z. B. das berühmte EPR-Paradoxon) – in der Quanteninformation betrachtet man sie jedoch als Ressource. Diese neue Sichtweise ist von zentraler Bedeutung.

Wann also ist ein quantenmechanischer Zustand, der durch eine Dichtematrix  $\rho$  beschrieben wird, verschränkt? Sei  $\rho$  der Gesamtzustand des aus zwei Teilsystemen zusammengesetzten Gesamtsystems. Wenn  $\rho$  in eine so genannte konvexe Summe aus Tensorprodukten von Dichtematrizen der Teilsysteme zerlegt werden kann, wenn also

<sup>4</sup> Vgl. Brub *et al.* (2004).

<sup>5</sup> Vgl. Shor (1994).

<sup>6</sup> Vgl. Schrödinger (1935).

### Universitätsverwaltung

JAN GERKEN und HERMANN THOLE  
Moderne Universitätsplanung ..... 547

### Zentrale Einrichtungen der Heinrich-Heine-Universität Düsseldorf

JAN VON KNOP und DETLEF LANNERT  
Gefahren für die IT-Sicherheit und Maßnahmen  
zu ihrer Abwehr ..... 567

MICHAEL WETTERN und JAN VON KNOP  
Datenschutz im Hochschulbereich ..... 575

IRMGARD SIEBERT und KLAUS PEERENBOOM

Ein Projekt zur Optimierung der Selbstausleihe.

Zur Kooperation der Universitäts- und Landesbibliothek Düsseldorf  
mit der 3M Deutschland GmbH ..... 591

SILVIA BOOCHS, MARCUS VAILLANT und MAX PLASSMANN

Neue Postkartenserie der Universitäts- und Landesbibliothek Düsseldorf .... 601

### Geschichte der Heinrich-Heine-Universität Düsseldorf

MAX PLASSMANN

Autonomie und ministerielle Steuerung beim Aufbau der neuen Fakultäten  
der Universität Düsseldorf nach 1965 ..... 629

### Chronik der Heinrich-Heine-Universität Düsseldorf

ROLF WILLHARDT  
Jahreschronik 2004 ..... 643

**Autorinnen und Autoren** ..... 657

DAGMAR BRUSS

## Verschränkt oder separabel? Moderne Methoden der Quanteninformationstheorie

### Einleitung: Quanteninformation

Die Physik der Quanteninformation ist eine Forschungsrichtung, die seit dem Beginn der 90er Jahre des letzten Jahrhunderts eine rasante Entwicklung erlebt hat. Bereits 1984 hatten C. Bennett und G. Brassard<sup>1</sup> erkannt, dass die Gesetze der Quantenmechanik die absolut sichere Erstellung eines gemeinsamen Zufallsschlüssels für zwei Parteien erlauben: Das erste Quantenkryptographieprotokoll, heute BB84 genannt, war entstanden. Im Gegensatz zu allen bekannten klassischen Kryptographieverfahren ist die Quantenkryptographie (genauer gesagt, die Verteilung eines geheimen Zufallsschlüssels) prinzipiell vor Lausangriffen eines Spions geschützt: Sobald der Spion Informationen über das gesendete Quantensignal gewinnt, führt er notwendigerweise eine Störung ein und kann somit entdeckt werden. In für die Quanteninformation beispielhafter Weise werden im BB84-Protokoll Ideen aus der Informationstheorie mit Gesetzen der Quantenmechanik verknüpft. Aus dieser Symbiose sind bisher etliche grundlegend neue Verfahren zur Informationsverarbeitung hervorgegangen.<sup>2</sup>

Zu diesen neuen Verfahren gehört unter anderem die Quantenteleportation, die 1993 von C. Bennett *et al.*<sup>3</sup> vorgeschlagen und 1997 im Experiment von A. Zeilingers Arbeitsgruppe in Innsbruck sowie 1998 von F. De Martini und Mitarbeitern in Rom verwirklicht wurde. Hier verwenden zwei Parteien, meist Alice und Bob genannt, einen verschränkten Zustand. Verschränkung ist eine nicht in der klassischen Physik, sondern nur in der Quantenmechanik auftretende Eigenschaft von zusammengesetzten Systemen. Das Ziel der Quantenteleportation ist es, die in einem unbekanntem Quantenzustand  $|\psi\rangle$  enthaltene Information von Alice zu Bob zu senden. Dies gelingt durch eine Messung von  $|\psi\rangle$  zusammen mit einem Subsystem des verschränkten Zustands, in einer ebenfalls verschränkten Basis, der so genannten Bell-Basis. Über einen klassischen Informationskanal (z. B. ein Telefon) teilt Alice Bob das Ergebnis der Messung mit. Dieser rotiert seinen Anteil am verschränkten Zustand in Abhängigkeit von Alice' Ergebnis – und erhält so genau  $|\psi\rangle$ . Wichtig für das Verständnis ist, dass hier *keine* Materie transportiert wird, sondern nur die in einem Zustand enthaltene Information.

Ein weiterer informationsverarbeitender Prozess, der klassisch so nicht möglich ist, ist beispielsweise die superdichte Kodierung. Hier wird Verschränkung genutzt, um zwei klassische Bits in einem quantenmechanischen Zwei-Niveau-System (so genanntes Qubit) zu kodieren. Eine nahe liegende Frage ist, ob höherdimensionale Systeme (also d-Niveau-

<sup>1</sup> Vgl. Bennett und Brassard (1984).

<sup>2</sup> Vgl. Bruß (2003).

<sup>3</sup> Vgl. Bennett *et al.* (1993).