



universität  
wien

# MASTERARBEIT

Titel der Masterarbeit

„Quantenkommunikationskomplexität  
mit nichtidealen Detektoren“

Verfasser

Michael Epping B.Sc.

angestrebter akademischer Grad

Master of Science (M.Sc.)

Wien, 2012

Studienkennzahl lt. Studienblatt: A 066 876

Studienrichtung lt. Studienblatt: Physik

Betreuer: Ao. Univ.-Prof. Mag. Dr. Caslav Brukner



# Inhaltsverzeichnis

<b>Einleitung</b>	<b>4</b>
<b>1 Grundlagen</b>	<b>7</b>
1.1 Benötigter Formalismus der Quantenmechanik . . . . .	7
1.2 Klassische physikalische Theorien . . . . .	9
1.3 Bellsche Ungleichungen . . . . .	10
1.3.1 Nichtdeterministische Theorien . . . . .	14
1.3.2 Argumentation mit Wahrscheinlichkeitsdichte . . . . .	14
1.3.3 Verallgemeinerung auf mehr Parteien und Messeinstellungen . . . . .	15
1.4 Kommunikationskomplexität . . . . .	16
1.4.1 Anwendungen . . . . .	18
<b>2 Bell-Ungleichungen und Kommunikationskomplexität</b>	<b>19</b>
2.1 Klassische Erfolgswahrscheinlichkeit . . . . .	20
2.2 Funktionen für Bell-Ungleichungen ohne Kommunikation . . . . .	22
2.3 Quantenmechanische Erfolgswahrscheinlichkeit . . . . .	24
2.4 Beispiele . . . . .	25
<b>3 Detektoreffizienz und Kontrast</b>	<b>29</b>
3.1 Kritische Detektoreffizienz des Detektor-Schlupfloches . . . . .	31
3.2 Protokolle für niedrige Detektoreffizienz . . . . .	36
3.2.1 Zwei Parteien mit langem Input . . . . .	36
3.2.2 Mermin Ungleichung . . . . .	38
3.3 Zusätzliche Kommunikation . . . . .	39
3.4 Das Toner-Bacon-Modell . . . . .	42
<b>4 Diskussion</b>	<b>45</b>
<b>Danksagung</b>	<b>48</b>
<b>Literaturverzeichnis</b>	<b>49</b>
<b>Anhang</b>	<b>51</b>
A Zusammenfassung . . . . .	51
B Abstract . . . . .	51
C Notationsübersicht . . . . .	52
D Algorithmus zum Berechnen der klassischen Schranke für zwei Parteien . . . . .	53
E Mögliche Messwerte zur CHSH-Ungleichung . . . . .	54
F Beweis zu Abschnitt 3.2.1 . . . . .	56

# Einleitung

In einer klassischen Beschreibung der Wirklichkeit, wie in der Newtonschen Mechanik oder der Relativitätstheorie, besitzen messbare Größen zu jedem Zeitpunkt wohldefinierte Werte. Intuitiv neigt man dazu anzunehmen, diese Werte existierten unabhängig von einer Messung, allein weil diese Messung möglich wäre. Albert Einstein definierte „Elemente der Realität“ als die Werte von Messungen, die mit Sicherheit vorhergesagt werden können und fordert, dass diese Elemente der Realität in einer vollständigen Theorie eine Entsprechung haben müssen.

Zusammen mit Podolsky und Rosen stellte Einstein ein Gedankenexperiment vor, welches die Unvollständigkeit der Quantenmechanik verdeutlichen sollte. In dem Gedankenexperiment werden zwei Teilchen, die zuerst wechselwirken konnten, räumlich getrennt. Anschließend werden zwei komplementäre Messungen an ihnen durchgeführt, zum Beispiel eine Ortsmessung und eine Impulsmessung. Die Heisenbergsche Unbestimmtheitsrelation verhindert eine gleichzeitige genaue Bestimmung beider Größen an einem Teilchen. Sind diese allerdings korreliert, so lässt sich über die Impulsmessung an einem Teilchen der Impuls des Anderen mit Sicherheit vorhersagen. Andererseits hätte aber auch eine Ortsmessung den Ort des anderen Teilchens gezeigt. In diesem Sinne sind sowohl Ort als auch Impuls Elemente der Realität. In einer quantenmechanischen Beschreibung des Teilchens finden sich aber keine genauen Werte für beide Größen. Auf diese Weise argumentieren Einstein, Podolsky und Rosen, dass die Quantenmechanik unvollständig ist[1].

Eine Vervollständigung der Theorie scheint möglich. Diese Theorie würde ausgehend von uns verborgenen Parametern die Vorhersagen der Quantenmechanik reproduzieren. Bell zeigte jedoch, dass die Annahmen von Einstein, Podolsky und Rosen zu einer Ungleichung über Erwartungswerte führen, die von den von der Quantenmechanik vorausgesagten Erwartungswerten verletzt wird[2]. An dieser Stelle entsteht also ein Widerspruch zwischen den „vernünftigen“ Annahmen von Einstein, Podolsky und Rosen und den Vorhersagen der -meist wenig intuitiven- Quantenmechanik. Wer nun Recht hat kann nur durch Fragen an die Natur, also durch Experimente, entschieden werden. Zahlreiche Experimente, die in ihrer einfachsten Variante schon Studenten als Praktikumsversuch zugänglich sind[3] (siehe Abbildung 1), sind vereinbar mit den Vorhersagen der Quantenmechanik und zeigen eine Verletzung einer Bellschen Ungleichung (u.a. [4, 5]).

Über die fundamentale Bedeutung für die Grundprinzipien der Physik hinaus sind Bellsche Ungleichungen auch für Anwendungen nützlich. Es hat sich gezeigt, dass die Quantenmechanik in einigen Fällen Möglichkeiten bietet, die in gewissem Sinne über die Möglichkeiten klassischer Theorien hinausgehen. Wichtige Beispiele sind Quantenalgorithmien[9, 10] und Quantenkommunikation[11]. Das liegt oft an der sogenannten Verschränkung, eine Korrelation räumlich getrennter Systeme die stärker ist als klassisch möglich. Bellsche Ungleichungen können nur von solchen verschränkten Zuständen verletzt werden.

Auch in dieser Arbeit werden Bellsche Ungleichungen eine zentrale Rolle spielen, wenn es darum geht Fragestellungen der Quantenkommunikationskomplexität zu behandeln. Die (klassische) Kommunikationskomplexität beschäftigt sich mit Problemen der folgenden

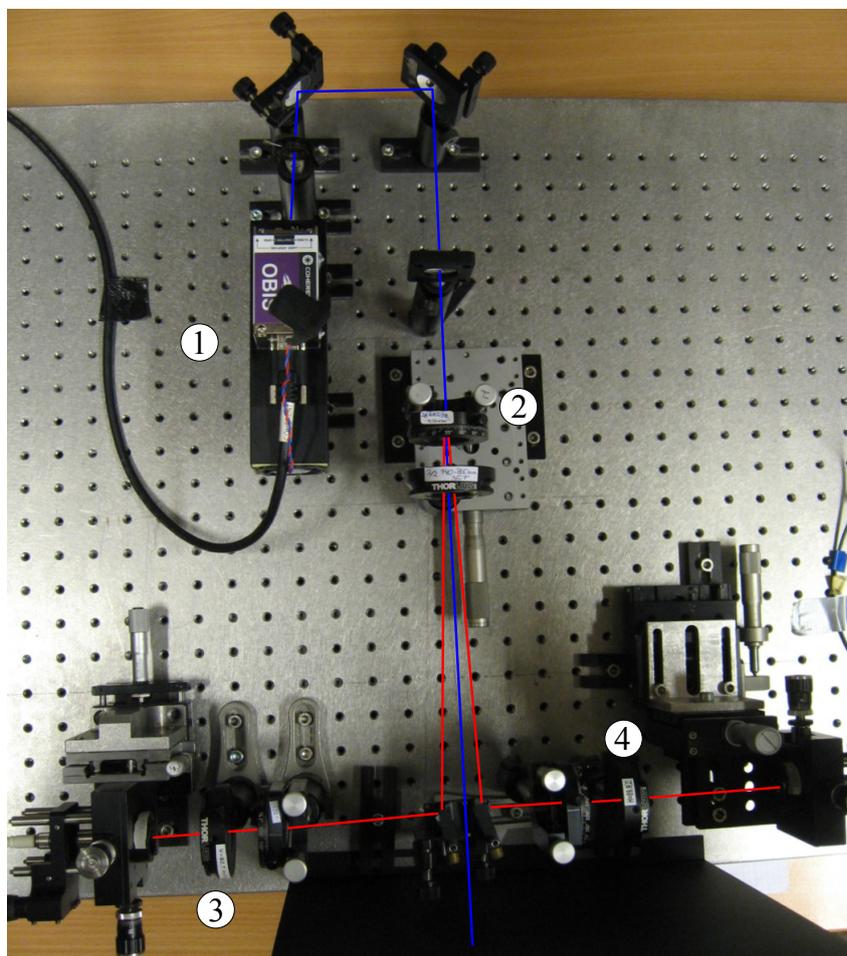


Abbildung 1: Foto eines einfachen Bell-Experiments von [12] im Rahmen eines Laborpraktikums mit eingezeichnetem Laserstrahlengang. Beginnend beim Laser (1) wird der Strahl in einem Beta-Bariumborat-Kristall fokussiert (2), wo Paare polarisationsverschränkter Photonen erzeugt werden. Die Polarisation von je einem Photon des Paares wird bei Alice (3) und bei Bob (4) gemessen. Die Erwartungswerte der Korrelationen in der Polarisation beider Photonen, gemessen unter verschiedenen Winkeln verletzen die im Text erwähnte Ungleichung.

Art. Es gebe mehrere Parteien (Menschen, Computer, Teile eines elektronischen Chips, ...) die alle eine Funktion berechnen sollen. Jede erhält jedoch nur einen Teil der Argumente der Funktion („Input“). Man kann sich fragen, wieviel Information die Parteien austauschen müssen bis jeder das Ergebnis bekannt geben kann[13]. Eine triviale Lösung ist, dass jede Partei einer bestimmten Partei ihren Teil des Inputs zusendet, die dann allen Parteien das Ergebnis mitteilt. Für die meisten Funktionen gibt es jedoch bessere Protokolle, die mit weniger Kommunikation auskommen. Andererseits kann man Situationen betrachten, in denen nur eine gewisse Menge Information ausgetauscht werden darf. Dann stellt sich die Frage mit welcher Wahrscheinlichkeit alle Parteien zu dem richtigen Ergebnis kommen können. In der vorliegenden Arbeit werden nur Probleme letzterer Art untersucht. Die Quantenkommunikationskomplexität untersucht, in welchen Fällen die Quantenmechanik bessere Lösungen des Kommunikationskomplexitätsproblems erlaubt als klassisch möglich.

Eine Verbesserung gegenüber klassischen Verfahren konnte gezeigt werden, wenn statt klassischen Bits Quantenbits (Qubits) übertragen werden[14] und wenn, wie in dieser Arbeit, klassische Bits kommuniziert werden, sich die Parteien aber zusätzlich einen verschränkten Zustand teilen[15]. Probleme der letzten Art haben den Vorteil, dass die Verschränkung schon vor Beginn des Protokolls hergestellt werden kann und sie eindeutiger mit klassischen Verfahren verglichen werden können.

Kritisch bei der experimentellen Realisierung ist die Qualität der Detektoren. Die Messungen gelingen zum Beispiel für Photonen nur in etwa 40 % bis 50 % der Fälle<sup>1</sup>. Für einen quantenmechanischen Vorteil wäre aber meist eine Detektoreffizienz von über 80 % nötig (siehe Kapitel 3). Diese Schwierigkeit ist Schwerpunkt dieser Arbeit. Eine Frage, der in dieser Arbeit nachgegangen werden soll, lautet „Kann zusätzliche Kommunikation mit Information über den Messerfolg ein Vorteil für quantenmechanische Protokolle sein?“.

Nach einer Einführung in die benötigten Grundlagen in Kapitel 1 wird in Kapitel 2 die Verbindung zwischen Bellschen Ungleichungen und speziellen Problemen der Kommunikationskomplexität hergestellt und an neuen, natürlichen Beispielen verdeutlicht. Darauf aufbauend wird dann in Kapitel 3 die oben gestellte Frage angegangen. Es wird die Möglichkeit von Kommunikationsproblemen untersucht, die schon mit geringer Detektoreffizienz Vorteile gegenüber klassischen Protokollen zeigen und beschrieben, warum solche Protokolle möglich sein sollten. Ein konkretes Protokoll mit dieser Eigenschaft konnte nicht gefunden werden.

In Anhang C befindet sich eine Übersichtstabelle über die in dieser Arbeit verwendete Notation, die beim Lesen der Arbeit nützlich sein kann.

---

<sup>1</sup>Für APD-Module unter Berücksichtigung der verwendeten Wellenlänge und Verlusten in Fiberglassleitungen[16]

# Kapitel 1

## Grundlagen

In diesem Kapitel wird benötigte Theorie eingeführt sowie einige Begriffe definiert, die für das Verständnis der Arbeit grundlegend sind.

### 1.1 Benötigter Formalismus der Quantenmechanik

Zu Beginn wird eine Einführung in den Formalismus der Quantenmechanik gegeben. Die Quelle ist [17]. Hier wird aber nur eingeführt, was für das Verständnis der Arbeit wichtig ist. Die Darstellung ist also weder vollständig noch eine gute Einführung in die Quantenmechanik im Allgemeinen (z.B. fehlt eine kontinuierliche Zeitentwicklung).

Eine *Observable* bezeichnet eine messbare Größe eines Systems, wie zum Beispiel Ort, Impuls, Orientierung von Spin und Polarisation, etc.. In der Quantenmechanik besitzt eine Observable im Allgemeinen keinen festen Wert. Stattdessen legt der (physikalische) *Zustand* eines Systems die Wahrscheinlichkeiten aller möglichen Messwerte fest. Es wird nun der Raum der (reinen) Zustände definiert.

#### Definition 1.1

Ein Hilbertraum  $\mathcal{H}$  über  $\mathbb{C}$  ist ein vollständiger<sup>1</sup>  $\mathbb{C}$ -Vektorraum zusammen mit einem Skalarprodukt  $\langle \cdot, \cdot \rangle$ .

Es wird die Dirac-Notation verwendet. Die Vektoren des Hilbertraums, die Zustände, werden als „kets“  $|\psi\rangle$  geschrieben. Ein „bra“-Vektor  $\langle\psi|$  ist eine Linearform auf den Ket-Vektoren, die ein  $|\varphi\rangle$  auf das Skalarprodukt von  $|\psi\rangle$  mit  $|\varphi\rangle$ ,  $\langle\psi|\varphi\rangle$ , abbildet.

In dieser Arbeit tauchen ausschliesslich endlich dimensionale Hilberträume der Dimension  $M \in \mathbb{N}$  auf. Oft ist eine Anschauung in Matrixform einer speziellen Basis  $\{e_k\}$  hilfreich. Der Zusammenhang ist

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_M \end{pmatrix} \quad \text{und} \quad \langle\psi| = ( \bar{\psi}_1 \quad \bar{\psi}_2 \quad \dots \quad \bar{\psi}_M ),$$

---

<sup>1</sup>d.h. jede Folge in  $\mathcal{H}$  konvergiert in  $\mathcal{H}$

wobei  $\psi_k = \langle k | \psi \rangle$  die Komponenten von  $|\psi\rangle$  in der Basis  $\{e_k\}$  sind. Das hier verwendete Standard-Skalarprodukt lautet dann

$$\langle u | v \rangle = \sum_{i=1}^M \bar{u}_i v_i.$$

Mit  $\bar{\cdot}$  ist die komplexe Konjugation gemeint. Eine Observable  $\mathcal{A}$  ist ein selbstadjungierter Operator auf  $\mathcal{H}$ , hier also eine hermitesche<sup>2</sup>  $M \times M$ -Matrix  $A$ . Nur die Eigenwerte von  $A$  sind mögliche Messwerte. Die Bornsche Regel gibt die Wahrscheinlichkeit, einen Messwert  $\lambda_i$  im Zustand  $|\psi\rangle$  zu messen mit

$$p_{\lambda_i} = \langle \psi | E_i | \psi \rangle = \langle \psi | \left( \sum_k |\psi_{i,k}\rangle \langle \psi_{i,k}| \right) | \psi \rangle$$

an. Hier ist  $|\psi_{i,k}\rangle$  der  $k$ -te Eigenvektor zum Eigenwert  $\lambda_i$ , d.h.  $E_i$  ist der Projektor auf den Eigenraum zum Eigenwert  $\lambda_i$ . Die Erwartungswerte der Observablen  $\mathcal{A}$  im Zustand  $|\psi\rangle$  sind

$$E = \langle A \rangle_\psi = \langle \psi | A | \psi \rangle = \sum_{i,j=1}^M \bar{\psi}_i(A)_{ij} \psi_j.$$

Nicht immer ist der Zustand eines Systems genau bekannt. Ursachen dafür sind zum Beispiel Unwägbarkeiten eines Experiments<sup>3</sup>. Dann wird der Zustand im sogenannten Dichtematrix-Formalismus als statistische Mischung aller vorkommenden Zustände beschrieben. Ist  $p_i$  die Wahrscheinlichkeit, dass der Zustand  $|\psi_i\rangle$  vorliegt, so ist die Dichtematrix

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

und der Erwartungswert ist jetzt

$$E = \sum_i p_i \langle A \rangle_{\psi_i} = \text{spur}(A\rho).$$

Eine solche Mischung von Zuständen wird *gemischter Zustand* genannt, in Abgrenzung zu den zuvor behandelten *reinen Zuständen*.

Sind zwei Systeme mit Hilberträumen  $\mathcal{H}_1$  und  $\mathcal{H}_2$  gegeben, so wird der Hilbertraum des Gesamtsystems  $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$  mit Hilfe des Tensorproduktes<sup>4</sup> gebildet. Die Vektoren von  $\mathcal{H}$  können in der Produktbasis angegeben werden. Sei  $\{|\psi_i\rangle\}_i$  eine Basis von  $\mathcal{H}_1$  und  $\{|\phi_j\rangle\}_j$  eine Basis von  $\mathcal{H}_2$  dann ist  $\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{ij}$  die Produktbasis von  $\mathcal{H}$  und

$$|\psi\rangle = \sum_{i,j} c_{ij} |\psi_i\rangle \otimes |\phi_j\rangle.$$

<sup>2</sup>Eine quadratische Matrix  $A$  die gleich ihrer transponierten und komplex konjugierten Matrix  $A^\dagger$  ist.

<sup>3</sup>Man erhält auch einen gemischten Zustand, wenn man ein Teilsystem eines verschränkten Zustandes betrachtet.

<sup>4</sup>In Matrixform wird das Tensorprodukt  $a \otimes b$  ausgerechnet, indem jede Komponente von  $a$  durch das Produkt von dieser Komponente und dem gesamten Objekt  $b$  ersetzt wird.

Wenn die (komplexen) Koeffizienten  $c_{ij}$  die Form  $c_{ij} = d_i \cdot e_j$  haben, so nennt man den Zustand  $|\psi\rangle$  *separabel*. Andernfalls ist der Zustand *verschränkt*. Besteht die Messung der Observablen  $\mathcal{A}$  darin, an Teilsystem Eins  $\mathcal{A}_1$  und an Teilsystem Zwei  $\mathcal{A}_2$  zu messen, so wird sie beschrieben durch die Matrix  $A = A_1 \otimes A_2$ .

Systeme die im zweidimensionalen Hilbertraum  $\mathcal{H}$  beschrieben werden nennt man auch *Qubit*. Sie sind das quantenmechanische Analogon zum Bit. Die kanonische Rechenbasis wird hier mit

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{und} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

bezeichnet. In dieser Arbeit werden Systeme aus  $n$  Qubits auftauchen, die also im Hilbertraum  $\mathcal{H}^{\otimes n}$  beschrieben werden. Ein Beispiel für ein Qubit ist der Spin eines Spin-1/2 Teilchens. Die Messung des Spins, zum Beispiel in einem Stern-Gerlach-Apparat, wird durch die Pauli-Matrizen

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{und} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

beschrieben, wobei jede Matrix zur Messung in die entsprechende Richtung gehört. Sie werden zusammengefasst zu  $\vec{\sigma} = (X, Y, Z)$ . Zur Messung des Spins in eine allgemeine Richtung  $\vec{a} = (x, y, z)$  mit  $|\vec{a}| = 1$  gehört

$$A(\vec{a}) = \frac{\mathbb{1} + xX + yY + zZ}{2}$$

mit Eigenwerten 0 und 1 bzw.

$$A(\vec{a}) = xX + yY + zZ$$

mit Eigenwerten  $-1$  und  $1$ .

## 1.2 Klassische physikalische Theorien

Eine physikalische Theorie liefert Vorhersagen über Messergebnisse verschiedener Observablen. Um bereits die spätere Notation zu verwenden, werden die Observablen anhand eines Parameters  $x$  systematisiert, der zunächst völlig beliebig ist, später jedoch eine natürliche Zahl einschliesslich Null sein wird. Dann wird eine  $m$ -Bit lange Zahl vorgegeben welche Observable zu messen ist. Es wird also eine von  $2^m$  Observablen  $\mathcal{A}(x)$  mit  $x \in \{0, 1, \dots, 2^m - 1\}$  gemessen.

Es werden nun plausible Annahmen über physikalische Theorien vorgestellt, die eine zentrale Rolle in der Arbeit spielen. Zuerst die philosophische Position, die annimmt es gäbe eine Wirklichkeit unabhängig von einem Beobachter, die (ontologischer) Realismus genannt wird[18]. Was dies konkret für eine physikalische Theorie bedeutet, sagt die folgende Definition.

### Definition 1.2 (*Realismus*)

Eine physikalische Theorie heisst *realistisch*, wenn jede mekbare Grösse  $\mathcal{A}(x)$  zu jeder Zeit (unabhängig von einer Messung) einen festen Wert  $a(x)$  besitzt. Man nennt die Theorie „Theorie verborgener Variablen“ (HVT, von engl. *hidden variable theory*), wenn die  $a(x)$  in deterministischer Weise durch verborgene Variablen bestimmt werden. Die verborgenen Variablen werden als  $\lambda$  zusammengefasst.

In realistischen Theorien ist es also erlaubt, mit den Ergebnissen von Messungen zu rechnen, die nicht durchgeführt wurden. Es ist sogar erlaubt mit mehreren Messergebnissen zu rechnen, die laut Quantenmechanik prinzipiell nicht gemeinsam gemessen werden können. Außerdem wurden hier sogenannte verborgene Variablen (auch verborgene Parameter) eingeführt. Diese sind Variablen die auf deterministische Weise das Messergebnis festlegen<sup>5</sup>. In der Quantenmechanik tauchen solche Variablen nicht auf. Sie werden einer tieferliegenden Theorie zugeschrieben.

Eine weitere plausible Annahme über die Natur ist die sogenannte Lokalität.

**Definition 1.3 (Lokalität)**

*Es gebe zwei räumlich voneinander getrennte Systeme. Eine physikalische Theorie heißt lokal, wenn keine an dem einen System durchgeführte Aktion Einfluss auf die versteckten potentiellen Messergebnisse des anderen Systems hat.*

Gegeben sei ein System bestehend aus  $n$  Teilsystemen, die räumlich getrennt sind. An jedem Teilsystem  $i \in \{1, \dots, n\}$  werde eine Messung  $\mathcal{A}_i(x_i)$  durchgeführt. Das Messergebnis  $a_i$  eines Teilsystems  $i$ , hängt in einer lokalen und realistischen Theorie insbesondere nicht von der Wahl der Observablen  $x_j$   $j \neq i$  der anderen Parteien ab. D.h.  $a_i(x_1, \dots, x_n) = a_i(x_i)$ . In einer nichtlokalen aber realistischen Theorie wäre dies erlaubt.

Mit „klassischen Theorien“ sind im Folgenden lokale realistische Theorien (LRT) gemeint. Streng genommen wird noch eine weitere Eigenschaft benötigt, die meist als „Freier Wille“ bezeichnet wird: Die Möglichkeit frei zu entscheiden, welche Observable gemessen werden soll. In dieser Arbeit wird diese Eigenschaft wie in [19] nur mit „Freiheit“ bezeichnet und wie folgt definiert.

**Definition 1.4 (Freiheit)**

*Die Wahl der Observablen (hier also  $x_1, \dots, x_n$ ) ist stochastisch unabhängig von den versteckten potentiellen Messergebnissen. Das heisst*

$$P(x_1, \dots, x_n | a_1(0), \dots, a_1(2^m - 1), \dots, a_n(0), \dots, a_n(2^m - 1)) = P(x_1, \dots, x_n).$$

### 1.3 Bellsche Ungleichungen

Wie später sichtbar wird muss jede LRT in bestimmten Experimenten Vorhersagen machen, die sich von denen der Quantenmechanik unterscheiden. Dieser Unterschied kann sich in Ungleichungen ausdrücken, die in der folgenden Definition genauer definiert werden.

**Definition 1.5 (Bellsche Ungleichung)**

*Eine Ungleichung heißt „Bellsche Ungleichung“, wenn sie von jeder lokalen und realistischen Theorie erfüllt wird und von der Quantenmechanik verletzt wird.*

Die Annahmen in Definition 1.5 unterscheiden sich von den ursprünglichen Annahmen in [2], denn die Annahme von perfekten Antikorrelationen wird hier nicht benötigt. Allerdings bedeutet dies, dass die zuerst von Bell genannte Ungleichung keine Bellsche Ungleichung im Sinne von Definition 1.5 ist. Perfekte Antikorrelationen werden zwar von der Quantenmechanik z.B. für zwei Spins im Singlet Zustand vorhergesagt, sind aber im Labor nicht (perfekt) beobachtbar. Für eine experimentelle Überprüfung lokalrealistischer Theorien

<sup>5</sup>Richtiger wäre also  $a(x, \lambda)$  statt  $a(x)$  zu schreiben, an den Rechnungen in dieser Arbeit ändert sich dadurch nichts. Man kann sich vorstellen, die Funktionen  $a_i$  würden in Abhängigkeit von  $\lambda$  ausgewählt.

eignet sich die ursprüngliche Ungleichung also nicht [19]. Den Gedanken von Bell drückt der folgende Satz aus.

**Satz 1.1 (John Bell)**

Es existiert eine Bellsche Ungleichung.

Beweis: Als Beweis des Satzes dient hier die Herleitung der Clauser-Horne-Shimony-Holt-Ungleichung (CHSH-Ungleichung), die zugleich ein wichtiges Beispiel ist. Der Beweis richtet sich nach [20], wobei die Notation an die in dieser Arbeit verwendete angepasst wurde.

Den schematischen Aufbau des Experimentes zeigt Abbildung 1.1. Die zwei Parteien, Alice und Bob, erhalten jeweils ein Teilchen (z.B. ein Photon) und können daran eine von zwei verschiedenen Messungen ausführen. Unter Annahme von Realismus liegen die Ergebnisse der Messung schon vor dieser fest. Diese ungemessenen Messwerte bezeichnen wir mit  $a_1(0)$  und  $a_1(1)$  bei Alice und mit  $a_2(0)$  und  $a_2(1)$  bei Bob. Der Index steht also für die Partei, das Argument für die Messung. Da  $a_i$  nur ein Argument hat, hängt es insbesondere nicht von der Wahl der Messung bei einer anderen Partei ab. Dies ist die Lokalität. Es sind bei jeder Messung nur zwei verschiedene Ausgänge möglich, die mit  $+1$  und  $-1$  bezeichnet werden.

Der Ausdruck

$$\begin{aligned} & a_1(0)a_2(0) + a_1(0)a_2(1) + a_1(1)a_2(0) - a_1(1)a_2(1) \\ &= a_1(0)(a_2(0) + a_2(1)) + a_1(1)(a_2(0) - a_2(1)) \end{aligned}$$

nimmt nur die Werte  $\pm 2$  an, denn genau einer der beiden Ausdrücke  $a_2(0) + a_2(1)$  und  $a_2(0) - a_2(1)$  ist 0, der andere  $\pm 2$ . Wie der Ausdruck selber ist auch dessen Erwartungswert nach oben durch 2 beschränkt, denn

$$\begin{aligned} & E(a_1(0)a_2(0) + a_1(0)a_2(1) + a_1(1)a_2(0) - a_1(1)a_2(1)) \\ &= \sum_{a_i(j)=-1,1} P(a_1(0), a_1(1), a_2(0), a_2(1)) (a_1(0)a_2(0) + a_1(0)a_2(1) + a_1(1)a_2(0) - a_1(1)a_2(1)) \\ &\leq \sum_{a_i(j)=-1,1} P(a_1(0), a_1(1), a_2(0), a_2(1)) \cdot 2 = 2. \end{aligned}$$

Außerdem ist

$$\begin{aligned} & E(a_1(0)a_2(0) + a_1(0)a_2(1) + a_1(1)a_2(0) - a_1(1)a_2(1)) \\ &= E(a_1(0)a_2(0)) + E(a_1(0)a_2(1)) + E(a_1(1)a_2(0)) - E(a_1(1)a_2(1)), \end{aligned}$$

weshalb insgesamt die Bell-Ungleichung von Clauser, Horne, Shimony und Holt,

$$E(a_1(0)a_2(0)) + E(a_1(0)a_2(1)) + E(a_1(1)a_2(0)) - E(a_1(1)a_2(1)) \leq 2 \quad (1.1)$$

folgt. Die Schranke für den Ausdruck auf der linken Seite wurde ausgehend von den Grundannahmen Realismus und Lokalität hergeleitet. Es folgt jetzt eine quantenmechanische Beschreibung des Experimentes.

Der gemeinsame Zustand von Alices und Bobs Systemen sei  $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$ . Die den Messergebnissen  $a_i(j)$  entsprechenden Observablen seien  $\mathcal{A}_i(j)$  repräsentiert durch

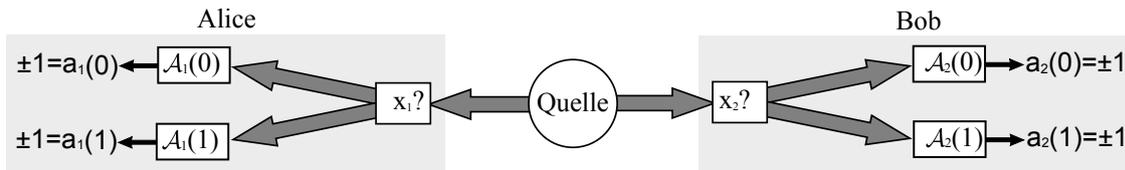


Abbildung 1.1: Schematischer Aufbau des Experiments zur CHSH-Ungleichung. Die Quelle sendet je einen Teil des Zustands  $|\psi^-\rangle$  an Alice (links) und Bob (rechts). Bei jeder Partei  $i$  bestimmt die Variable  $x_i$  welche der beiden Observablen  $\mathcal{A}_i(0)$  oder  $\mathcal{A}_i(1)$  gemessen wird. Die Messung dieser Observablen fördert  $a_i(0)$  bzw.  $a_i(1)$  zu Tage, dessen Wert  $+1$  oder  $-1$  ist.

Matrizen  $A_i(j)$ :

$$\begin{aligned} A_1(0) &= Z \\ A_1(1) &= X \\ A_2(0) &= \frac{-Z - X}{\sqrt{2}} \\ A_2(1) &= \frac{Z - X}{\sqrt{2}} \end{aligned}$$

Die Erwartungswerte der Observablen im Zustand  $|\psi^-\rangle$  lauten

$$\begin{aligned} \langle A_1(0) \otimes A_2(0) \rangle &= \frac{1}{\sqrt{2}}, \\ \langle A_1(1) \otimes A_2(0) \rangle &= \frac{1}{\sqrt{2}}, \\ \langle A_1(0) \otimes A_2(1) \rangle &= \frac{1}{\sqrt{2}} \\ \text{und } \langle A_1(1) \otimes A_2(1) \rangle &= -\frac{1}{\sqrt{2}}. \end{aligned}$$

Einsetzen in Gleichung 1.1 führt zu dem Widerspruch  $2\sqrt{2} \leq 2$ . Die CHSH-Ungleichung wird also von den quantenmechanischen Erwartungswerten der angegebenen Observablen im  $|\psi^-\rangle$ -Zustand verletzt.  $\square$

Es gibt also Vorhersagen der Quantenmechanik, die mit Lokalität und Realismus gemeinsam nicht vereinbar sind. Diese Vorhersagen lassen sich im Experiment überprüfen und bisher stützen alle Experimente die Quantenmechanik. Dies bedeutet, dass mindestens eine der Annahmen die zur Bell-Ungleichung führten von der Natur nicht verwirklicht ist. Die Experimente zeigen also, dass die Natur nicht Freiheit, Realismus *und* Lokalität erfüllt. Die Frage welche dieser Annahmen man fallen lassen möchte ist zur Zeit noch Geschmackssache, da es dazu keine Experimente gibt. Es lohnt sich, sofern nicht schon geschehen, an dieser Stelle darüber nachzudenken, welche Annahme man persönlich als wichtiger erachtet. Es gibt für beide schwerwiegende Argumente.

Realismus ist eine unter Naturwissenschaftlern verbreitete Ansicht. Schliesslich hat man sich als Ziel gesetzt die Natur zu untersuchen. Die Ansicht diese habe die gemessenen Eigenschaften nicht unabhängig von der Beobachtung scheint dann sinnlos. Allerdings ist ein Realist wegen dem Kochen-Specker-Theorem[21] gezwungen Kontextualität, d.h.

einen Einfluss der Messung auf die Messergebnisse, zuzulassen. Das aber eine realistische Beschreibung der Naturerscheinungen möglich ist zeigt die von David Bohm ausgearbeitete Interpretation der Quantenmechanik, die deren Vorhersagen vollständig reproduziert[22].

Auch die Lokalität ist eine Annahme, die sich in der Entwicklung der Naturwissenschaften bewährt hat. Ein Grund für den Erfolg der Naturwissenschaften ist, dass man die komplexe Welt in kleine, lösbare Probleme eingeteilt hat. Diese konnte man dann insbesondere auch räumlich isoliert betrachten. In der speziellen Relativitätstheorie kommt der Lokalität eine besondere Bedeutung zu. Hier können sich Wirkungen nicht schneller als mit Lichtgeschwindigkeit ausbreiten. Deshalb können Objekte an Raumzeitpunkten, die nicht mit einem Lichtstrahl verbunden werden können, auch keinen Einfluss aufeinander ausüben.

Die Quantenmechanik enthält in ihrem Formalismus weder Realismus noch Lokalität. Wenn von Quanten-Nichtlokalität die Rede ist, ist meist der instantane Kollaps der Wellenfunktion gemeint. Dadurch lassen sich keine Informationen übermitteln und diese „Nichtlokalität“ widerspricht nicht der hier definierten Lokalität.

Bei der experimentellen Überprüfung einer Bell-Ungleichung muss darauf geachtet werden, dass die gemessenen Daten in dem konkreten experimentellen Aufbau wirklich nicht mit einer lokalrealistischen Theorie erklärt werden können. Erfüllt das Experiment nicht die in der Herleitung der Bell-Ungleichung vorausgesetzten Bedingungen, so kann vielleicht eine Verletzung dieser Ungleichung gezeigt werden, diese Verletzung ist dann aber in Einklang mit einer lokalrealistischen Theorie. Zuverlässige Messung der Observablen und die räumliche Trennung der Systeme sind möglicherweise nicht vollständig verwirklicht worden. Diese Ansatzpunkte für Kritik werden Schlupflöcher genannt und wurden im Detail untersucht. Jedes dieser Schlupflöcher wurde bereits in einem Experiment geschlossen und die Ergebnisse sind in Übereinstimmung mit den Vorhersagen der Quantenmechanik[5].

### **Gerechte-Stichprobe-Schlupfloch**

Die verwendeten Detektoren sind nicht perfekt und weisen deshalb nicht alle Teilchen nach. Es wäre denkbar, dass die Bell-Ungleichung nicht verletzt wird wenn alle Messungen erfolgreich wären, sie aber aus einem unbekanntem Grund ausgerechnet von den Messungen verletzt wird, die erfolgreich waren. Dieses Schlupfloch wird gerechte-Stichprobe-Schlupfloch („fair sampling loophole“) oder Detektor-Schlupfloch genannt und lässt sich schliessen, wenn die Detektoreffizienz hoch genug ist.

### **Einstein-Lokalität-Schlupfloch**

Oft wird in einem Experiment nicht sichergestellt, dass zwischen den zwei Parteien keine Informationen über das Messergebnis ausgetauscht werden kann. Da die Messung einer Partei vor der der anderen durchgeführt wird ist es möglich, dass ein irgendwie geartetes Signal mit Informationen über diese Messung das andere Teilchen erreicht, bevor es gemessen wird. Dann könnten die Messungen stärker korreliert sein als in der Herleitung der Bellschen Ungleichung. Dieses Einstein-Lokalität-Schlupfloch wird geschlossen, indem die Messungen weit genug räumlich getrennt werden, sodass die Information schneller als Licht wandern müsste, was die Relativitätstheorie ausschliesst.

### **Freier-Wille-Schlupfloch**

In einem einfachen Experiment wird die Messeinstellung (zum Beispiel die Drehung von Polarisatoren) gewählt, lange bevor das Teilchenpaar erzeugt wird. Wenn Information über die Art der Messung die Teilchen erreicht bevor sie getrennt sind, könnte das Messergebnis

zu diesem Zeitpunkt festgelegt werden und die Verletzung der Bell-Ungleichung wäre wieder in Einklang mit einer lokalrealistischen Theorie. Dieses Schlupfloch wird Freier-Wille-Schlupfloch genannt, weil die Annahme, dass die Messeinstellung unabhängig von den verborgenen Variablen ist, verletzt wird. Ähnlich wie beim Einstein-Lokalität-Schlupfloch wird dieses Schlupfloch geschlossen, indem die Wahl der Messung zufällig und raumartig zur Erzeugung des Photonenpaars geschieht.

Geht man weit genug in die Vergangenheit, so findet man immer einen Punkt der zeitartig zur Wahl der Messung und Erzeugung der Teilchen liegt. Ausgehend von diesem Punkt können sowohl Wahl der Messeinstellung als auch die Eigenschaften der Teilchen durch gemeinsame verborgene Parameter vorbestimmt sein. Diese Art des Freier-Wille-Schlupfloches kann nicht geschlossen werden. Nimmt man diese Art von Vorbestimmung an, so verneint man allerdings jede Möglichkeit überhaupt ein sinnvolles Experiment durchführen zu können. Dies ist also ein Standpunkt der aus naturwissenschaftlicher Sicht nicht sinnvoll ist.

### 1.3.1 Nichtdeterministische Theorien

In der Herleitung der CHSH-Ungleichung wurden nur deterministische lokalrealistische Theorien beachtet. Trotzdem gilt das Ergebnis auch für nichtdeterministische Theorien[23]. Eine klassische Theorie ist gegeben durch  $a_1(x_1)$  und  $a_2(x_2)$ . Die Wahrscheinlichkeit bei tatsächlichen Messergebnissen  $a$  bei Alice und  $b$  bei Bob richtig zu liegen ist  $P_{a,b|x_1,x_2} = \delta_{a_1(x_1),a} \delta_{a_2(x_2),b}$ . Alle Komponenten von  $P$  lassen sich als Vektor  $\vec{p}$  auffassen. Die deterministischen Theorien bilden eine endliche Menge an Vektoren. Die nichtdeterministischen Theorien sind konvexe Kombinationen dieser Theorien, insgesamt bilden die Theorien also ein konvexes Polytop in diesem Vektorraum. Eine Bellsche Ungleichung entspricht einer Hyperebene, die den Vektorraum in zwei Halbräume einteilt. Theorien eines Halbraums erfüllen die Ungleichung, Theorien des anderen nicht. Da alle deterministischen LRT auf einer Seite der Hyperebene liegen, liegt auch die gesamte konvexe Menge auf dieser Seite. Dies bedeutet, dass auch die nichtdeterministischen LRT die Bellsche Ungleichung einhalten müssen. Wenn die Hyperebene mit einer Fläche des Polytop zusammenfällt wird sie enge Bell-Ungleichung genannt (von engl. „tight Bell inequality“).

### 1.3.2 Argumentation mit Wahrscheinlichkeitsdichte

In dieser Arbeit tauchen die verborgenen Variablen meist nicht explizit auf. Statt auf die genaue Ursache der Messergebnisse einzugehen wird die Wahrscheinlichkeit der Messergebnisse als gegeben vorausgesetzt. In vielen Quellen findet man eine Beschreibung, in der die verborgenen Variablen  $\lambda$  als Argument in die Berechnung der Messergebnisse (in der hier verwendeten Notation  $a_i(x_i, \lambda)$ ) eingehen. Um Erwartungswerte zu bilden wird dann über den Raum  $\Gamma$  aller Variablen  $\lambda$  integriert, wobei die  $\lambda$  gemäß der Wahrscheinlichkeitsverteilung  $\rho(\lambda)$  mit Normierung

$$\int_{\Gamma} \rho(\lambda) d\lambda = 1$$

verteilt sind. Alice messe die Observable  $x_1$  und erhalte  $a_1(x_1, \lambda) = \pm 1$  und Bob  $x_2$  mit Ergebnis  $a_2(x_2, \lambda) = \pm 1$ . Der Erwartungswert von  $a_1 a_2$  ist dann

$$E(x_1, x_2) = \int_{\Gamma} \rho(\lambda) a_1(x_1, \lambda) a_2(x_2, \lambda) d\lambda.$$

Auch in dieser Formulierung kann man die CHSH-Ungleichung

$$E(0,0) + E(0,1) + E(1,0) - E(1,1) \leq 2$$

herleiten (vgl. [3]).

### 1.3.3 Verallgemeinerung auf mehr Parteien und Messeinstellungen

Der experimentelle Aufbau wird nun auf  $n$ -Parteien mit jeweils  $2^m$  Messeinstellungen verallgemeinert. Jede Partei erhält ein Teilsystem des Ausgangszustands  $|\psi\rangle$ . Es werden Ungleichung betrachtet, die sich in der Form

$$\sum_{x_1 \dots x_n = 0}^{2^m - 1} g(x_1, \dots, x_n) E(x_1, \dots, x_n) \leq B(n, m, g) \quad (1.2)$$

schreiben lassen, wobei  $g(x_1, \dots, x_n)$  zunächst beliebige reelle Koeffizienten sind,  $E(x_1, \dots, x_n)$  den Erwartungswert in der durch die  $x_i$  angegebenen Messeinstellung bezeichnet und  $B(n, m, g)$  eine zu  $g$  gehörende klassische Schranke ist. Eine solche Schranke erhält man, indem man über alle klassischen Strategien maximiert. Eine klassische Strategie meint hier die Zuweisung der Werte  $a_i(x_i) = \pm 1$  für alle  $i$  und alle  $x_i$ .

$$B(n, m, g) = \max_{a_i(x_i)} \sum_{x_1 \dots x_n = 0}^{2^m - 1} g(x_1, \dots, x_n) \prod_{i=1}^n a_i(x_i) \quad (1.3)$$

Die  $a_i(x_i)$  sind die Messergebnisse der  $i$ -ten Partei bei Messeinstellungen  $x_1, \dots, x_n$ . Nur in einer klassischen Theorie macht es Sinn von diesen Werten zu sprechen (Realität). Wegen der Lokalität ist  $a_i$  nur von  $x_i$  abhängig.

Die Schranke gilt nicht für die Quantenmechanik. Diese erreicht für die linke Seite der Ungleichung einen anderen Wert, den sogenannten Bell-Parameter.

#### Definition 1.6 (Bell-Parameter)

Der Wert

$$S = \max_{|\psi\rangle, \mathcal{A}(x_1, \dots, x_n)} \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) E(x_1, \dots, x_n)$$

der quantenmechanisch durch Maximierung über den Zustand  $|\psi\rangle$  und die Wahl der Observablen  $\mathcal{A}(x)$  erreicht werden kann wird Bell-Parameter genannt.

Dass dieser Wert mindestens so groß ist wie die klassische Schranke sichert der folgende Satz.

#### Satz 1.2

Der Bell-Parameter  $S$  ist immer mindestens so groß wie die lokalrealistische Schranke  $B$  ( $S \geq B$ ).

Beweis: Im GHZ<sup>6</sup>-Zustand

$$|GHZ_n^+\rangle := \frac{1}{\sqrt{2}} (|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) \quad (1.4)$$

ist der Erwartungswert von

$$\mathcal{A}_n = \bigotimes_{i=1}^n (\cos(\phi_i)X + \sin(\phi_i)Y),$$

also einer simultanen Messung aller  $n$  Parteien in der selben Ebene in Richtungen mit Winkeln  $\phi_i$ ,  $1 \leq i \leq n$ ,

$$E(\phi_1, \dots, \phi_n) = \langle GHZ_n^+ | \mathcal{A}_n | GHZ_n^+ \rangle = \cos\left(\sum_i \phi_i\right).$$

Mit der Wahl  $\phi_i = \pi/2(a_i(x_i) + 1)$  (also umgerechnet in  $\{0, \pi\}$  statt  $\{-1, 1\}$ ) wird die lokalrealistische Schranke  $B$  erreicht:

$$\begin{aligned} S &= \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) E(x_1, \dots, x_n) \\ &= \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) \cos\left(\sum_i \phi_i(x_i)\right) \\ &= \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) \cos\left(\pi/2 \sum_i (a_i(x_i) + 1)\right) \\ &= \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) \prod_i a_i(x_i) \\ &= \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) A(x_1, \dots, x_n) \end{aligned}$$

Wenn die  $a_i(x_i)$  entsprechend der optimalen klassischen Strategie gewählt werden, folgt der Satz.  $\square$

Hier noch ein kleiner Satz, der manchmal leicht entscheiden kann, ob es sich bei Gleichung 1.2 für ein bestimmtes  $g$  um eine Bellsche Ungleichung handelt.

### Satz 1.3

Sei  $2 \mid \sum g(x)$ ,  $g(x) \in \{0, \pm 1\}$  und  $2 \nmid S$ , dann ist  $S > B$ .

Beweis: Jede Multiplikation von einem  $g(x)$  mit einem Vorzeichen ändert die Summe um  $\pm 2$ , damit bleibt  $2 \mid \sum g(x)a(x)$ . Da  $2 \nmid S$  ist  $S \neq B$  und wegen Satz 1.2 ist dann  $S > B$ .  $\square$

Bei einer Ungleichung mit den im Satz geforderten Bedingungen genügt es also  $S$  zu berechnen um zu zeigen, dass es sich um eine Bellsche Ungleichung handelt.

## 1.4 Kommunikationskomplexität

Es gebe zwei Parteien, wie üblich Alice und Bob genannt, die gemeinsam eine Funktion  $f(x_1, x_2) \in \{-1, 1\}$  berechnen wollen. Alice erhalte einen Teil der Eingabe  $x_1$  und Bob den zweiten Teil  $x_2$ . Die zentrale Fragestellung aus dem Gebiet der Kommunikationskomplexität lautet „Wieviele Informationen müssen Alice und Bob austauschen, damit beide

<sup>6</sup>Der Zustand ist benannt nach den Physikern Daniel Greenberger, Michael Horne und Anton Zeilinger. Siehe auch GHZ-Experiment[6].

<sup>7</sup>Die Notation  $a|b$  bedeutet, dass  $b$  ein ganzzahliges Vielfaches von  $a$  ist. Man sagt  $a$  Teiler von  $b$ ,  $a$  teilt  $b$  oder  $b$  ist teilbar durch  $a$ . Mit  $a \nmid b$  ist  $\neg(a|b)$  gemeint.

das Ergebnis  $f(x_1, x_2)$  angeben können?“. Diese Menge an Information heisst Kommunikationskomplexität der Funktion  $f$ .

Im Folgenden wird eine leicht abgewandeltes Problem betrachtet. Es soll die Funktion  $f(x_1, \dots, x_n)$  berechnet werden. Wobei jede Partei ein  $x_i \in \{0, \dots, 2^m - 1\}$  erhält. Die Menge an erlaubter Kommunikation wird vorgegeben. Dann ist die Frage, wie groß die Wahrscheinlichkeit ist auf das richtige Ergebnis zu kommen. Mögliche Regeln sind:

1. Jede der  $n$  Parteien erhält einen  $m$ -Bit langen Input  $x_i$ ,  $1 \leq i \leq n$ .
2. Jede Partei  $i$  darf ein Bit  $e_i$  senden, d.h. allen anderen Parteien mitteilen.
3. Jede Partei muss ein Ergebnis bekanntgeben. Die Berechnung gilt als erfolgreich, wenn alle Parteien das richtige Ergebnis nennen.

Hier ist zunächst nicht sichergestellt, dass alle Parteien zum selben Ergebnis kommen. In dieser Arbeit werden deshalb die (vereinfachten) Regeln verwendet, in denen nur eine vorher festgelegte Partei nach dem Ergebnis gefragt wird. Die Regeln sind also:

1. Vorbereitung: Jede der  $n$  Parteien erhält einen  $m$ -Bit langen Input  $x_i$ ,  $1 \leq i \leq n$ .
2. Kommunikation: Jede Partei  $i \neq 1$  darf ein Bit  $e_i$  an Partei 1 senden.
3. Ausgabe: Die Partei 1 muss ein Ergebnis  $A$  bekanntgeben. Die Berechnung gilt als erfolgreich, wenn  $A = f(x_1, \dots, x_n)$ .

Ein Protokoll ist die vor Beginn festgelegte Vorschrift, gemäß der die Parteien ihre zu sendenden Bits berechnen, zusammen mit der Antwortfunktion von Partei 1. Wie erfolgreich ein Protokoll eine gegebene Funktion  $f$  berechnet hängt davon ab, wie gut die Antwortfunktion  $A$  mit dieser Funktion  $f$  übereinstimmt. Diesen Zusammenhang präzisiert der folgende Satz. Er ist eine Verallgemeinerung der in dem Beweis von [7] erwähnten Gleichung.

**Satz 1.4 (Erfolgswahrscheinlichkeit)**

Sei  $A(x_1, \dots, x_n)$  die Antwortfunktion von Partei 1 (welche die Regeln erfüllt) und  $Q(x_1, \dots, x_n)$  mit  $\sum_{x_1, \dots, x_n=0}^1 Q(x_1, \dots, x_n) = 1$  die Wahrscheinlichkeitsverteilung des Inputs. Dann ist die Erfolgswahrscheinlichkeit des zu  $A$  gehörenden Protokolls

$$P(f = A) = \frac{1}{2} (1 + (f, A)),$$

wobei

$$(f, A) := \sum_{x_1, \dots, x_n=0}^1 Q(x_1, \dots, x_n) f(x_1, \dots, x_n) A(x_1, \dots, x_n),$$

das mit  $Q$  gewichtete Skalarprodukt von  $f$  und  $A$  ist.

Beweis:

$$\begin{aligned}
 P(f = A) &= \sum_x Q(x) \begin{cases} 1 & \text{falls } f(x) = A(x), \quad \text{d.h. } f(x)A(x) = 1 \\ 0 & \text{falls } f(x) \neq A(x), \quad \text{d.h. } f(x)A(x) = -1 \end{cases} \\
 &= \sum_x Q(x) \frac{1 + f(x)A(x)}{2} = \frac{1}{2} \left( \underbrace{\sum_x Q(x)}_{=1} + \sum_x Q(x)f(x)A(x) \right) \\
 &= \frac{1}{2} (1 + (f, A))
 \end{aligned}$$

□

Der Satz 1.4 ist für spätere Beweise nützlich.

### 1.4.1 Anwendungen

Neben den offensichtlichen Anwendungen im parallelen Berechnen von Funktionen auf verteilten Eingaben gibt es noch weitere Anwendungen der Kommunikationskomplexität bei endlichen Automaten und Turingmaschinen, Entscheidungsbäumen und geordneten binären Entscheidungsdiagrammen, VLSI Chips und Komparator-Schaltkreisen[13]. Diese lassen sich allerdings nicht unmittelbar auf die Erfolgswahrscheinlichkeit bei vorgegebener Menge Kommunikation übertragen.

## Kapitel 2

# Bell-Ungleichungen und Kommunikationskomplexität

In [7] wird ein Zusammenhang zwischen Bellschen Ungleichungen und den Erfolgswahrscheinlichkeiten dazu passender Kommunikationsprotokolle hergestellt. Dort werden Protokolle für  $n$  Parteien betrachtet, bei denen jede Partei ein Bit kommunizieren darf. Dieser Abschnitt soll eine Verallgemeinerung der Ergebnisse sein.

Im Folgenden wird das Problem betrachtet, die Funktion  $f : \{0, 1, \dots, 2^m - 1\}^n \rightarrow \{-1, 1\}$  zu berechnen. Sie lässt sich schreiben als

$$f(x_1, \dots, x_n) = \text{sgn}(g(x_1, \dots, x_n)), \quad (2.1)$$

mit der Vorzeichen-Funktion<sup>1</sup>

$$\text{sgn}(x) := \begin{cases} 1 & \text{falls } x > 0 \\ 0 & \text{falls } x = 0 \\ -1 & \text{falls } x < 0 \end{cases} \quad (2.2)$$

und bei der Wahl von  $g$  bleibt noch die Freiheit, den Betrag von  $g(x)$  so zu wählen, dass

$$Q(x_1, \dots, x_n) = \frac{|g(x_1, \dots, x_n)|}{\sum_{x_1, \dots, x_n=0}^{2^m} |g(x_1, \dots, x_n)|} =: \frac{1}{\Sigma} |g(x_1, \dots, x_n)| \quad (2.3)$$

der Wahrscheinlichkeitsverteilung für die Inputs  $x_i$  der  $n$  Parteien entspricht. Der Betrag eines Funktionswertes  $g(x_1, \dots, x_n)$  gibt also an, wie wahrscheinlich der Input  $x_1, \dots, x_n$  ist.

---

<sup>1</sup>Mit dieser Definition der Vorzeichen-Funktion ist  $f \notin \{-1, 1\}$  falls  $g(x) = 0$  ist. Wir ignorieren diese Schwierigkeit, weil die Wahrscheinlichkeit für diesen Input Null ist.

## 2.1 Klassische Erfolgswahrscheinlichkeit

Es soll nun die beste klassische Erfolgswahrscheinlichkeit angegeben werden. Dafür wird eine Verallgemeinerung der klassischen Schranke eingeführt.

### Definition 2.1 (Klassische Schranke mit Kommunikation)

Es sei die von den Parteien zu berechnende Funktion  $f(x_1, \dots, x_n)$  und die Wahrscheinlichkeitsverteilung  $Q(x_1, \dots, x_n)$  vorgegeben und  $g$  die über Gleichung 2.1 und Gleichung 2.3 definierte Funktion. Das gegebene Kommunikationskomplexitätsproblem definiert Regeln, die die Antwortfunktion  $A$  erfüllen muss. Insbesondere darf die Kommunikationskomplexität von  $A$  nicht größer sein, als in den Regeln festgelegt (z.B. nur ein Bit Kommunikation pro Partei).

Die klassische Schranke mit Kommunikation zur Funktion  $f$  ist definiert als

$$B_A(n, m, g) = \max_{A(x_1, \dots, x_n) \text{ erlaubt}} \sum_{x_1 \dots x_n = 0}^{2^m - 1} g(x_1, \dots, x_n) A(x_1, \dots, x_n). \quad (2.4)$$

Hier wird also über alle innerhalb der Regeln zulässigen Antwortfunktionen maximiert.

Die Bedeutung der Schranke  $B_A$  wird klar, wenn der folgende Satz einen Zusammenhang zwischen der Schranke und der Erfolgswahrscheinlichkeit eines Protokolls herstellt.

### Satz 2.1 (Klassische Erfolgswahrscheinlichkeit)

Es gebe  $n$  Parteien, von denen jede einen Teil des  $Q$ -verteilten Input  $x_1, \dots, x_n \in \{0, 1, 2, \dots, 2^m - 1\}$  erhält. Es soll die Funktion

$$f = \text{sgn}(g(x_1, \dots, x_n)) \quad (2.5)$$

berechnet werden. Dann ist die beste klassische Erfolgswahrscheinlichkeit

$$P_C = \frac{1}{2} + \frac{B_A(n, m, g)}{2 \sum_{x_1, \dots, x_n = 0}^{2^m - 1} |g(x_1, \dots, x_n)|}.$$

Beweis: Sei  $g, f = \text{sgn}(g)$  gegeben und  $A$  eine Antwortfunktion die alle geforderten Einschränkungen, insbesondere die Kommunikationskomplexität, erfüllt. Für die Erfolgswahrscheinlichkeit der Antwortfunktion gilt

$$P(A = f) \leq \max_{A \text{ erlaubt}} P(A = f)$$

und mit

$$P(A = f) = \frac{1}{2} (1 + (f, A)) \quad (\text{Satz 1.4})$$

folgt

$$\begin{aligned}
P(A = f) &\leq \max_A \frac{1}{2} (1 + (f, A)) \\
&= \max_A \frac{1}{2} \left( 1 + \sum_{x_1, \dots, x_n} Q(x_1, \dots, x_n) f(x_1, \dots, x_n) A(x_1, \dots, x_n) \right) \\
&= \frac{1}{2} + \frac{1}{2} \max_A \sum_{x_1, \dots, x_n} Q(x_1, \dots, x_n) f(x_1, \dots, x_n) A(x_1, \dots, x_n) \\
&= \frac{1}{2} + \frac{\max_A \sum_{x_1, \dots, x_n} |g(x_1, \dots, x_n)| \operatorname{sgn}(g(x_1, \dots, x_n)) A(x_1, \dots, x_n)}{2 \sum_{x_1, \dots, x_n} |g(x_1, \dots, x_n)|} \\
&= \frac{1}{2} + \frac{\max_A \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) A(x_1, \dots, x_n)}{2 \sum_{x_1, \dots, x_n} |g(x_1, \dots, x_n)|} \\
&= \frac{1}{2} + \frac{B_A(n, m, g)}{2 \sum_{x_1, \dots, x_n} |g(x_1, \dots, x_n)|}
\end{aligned}$$

□

Mit Hilfe von  $B_A$  wird also das Maximierungsproblem von  $P(A = f)$  umformuliert. Das folgende Beispiel soll dies veranschaulichen.

### Beispiel 2.1

Dieses Beispiel richtet sich nach Kapitel 5 in [8]. Die zwei Parteien Alice und Bob erhalten einen zwei Bit langen Input  $x_1$  bzw.  $x_2$ . Es sei  $x_i^{(1)}$  das erste Bit von  $x_i$  und  $x_i^{(2)}$  das Zweite. Die zwei Parteien haben die Aufgabe die Funktion

$$f(x_1, x_2) = 2 \left( x_1^{(1)} x_2^{(1)} + x_1^{(2)} x_2^{(2)} \pmod{2} \right) - 1$$

zu berechnen. Es gilt das Versprechen, dass  $x_1, x_2 \neq 0$  ist. Jede Partei darf ein Bit senden. Gefragt ist nach der maximalen Wahrscheinlichkeit, mit der das richtige Ergebnis berechnet wird.

Zunächst veranschaulichen wir uns die durch  $f$  und  $Q$  (das Versprechen) definierte Funktion  $g$  als Matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & -1 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}.$$

In dieser Matrix steht an der Stelle  $(x_1, x_2)$  der Funktionswert  $g(x_1, x_2)$ . Eine allgemeine zulässige Antwortfunktion hat die Form  $A(x_1, a_2(x_2))$  wo  $a_2$  das von Bob gesendete Bit ist.  $a_2$  ist eine binäre Funktion mit einem zwei Bit großen Argument, sodass es  $2^{2^2} = 16$  verschiedene Möglichkeiten für  $a_2$  gibt. Ausführen des Maximums in Gleichung 2.4 liefert als eine optimale Antwortfunktion

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

und die Schranke mit Kommunikation ist  $B_A = 5$ . Nach Satz 2.1 ist  $P_C = \frac{7}{9} \approx 78\%$ . Es kann nun noch die Erfolgswahrscheinlichkeit eines Protokolls mit Verschränkung untersucht werden. Obwohl dies ein Vorgriff auf die folgenden Abschnitte darstellt, soll hier ein quantenmechanisches Protokoll der Vollständigkeit halber erwähnt werden. Alice und Bob besitzen jetzt jeder einen Teil des Zustandes  $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$  und führen jeder an seinem Teil eine von vier verschiedenen Messungen durch. Welche Messung sie durchführen bestimmt ihr Input  $x_1$  bzw.  $x_2$ . Nun sendet Bob sein Messergebnis ( $\pm 1$ ) an Alice, die dieses mit ihrem Messergebnis (ebenfalls  $\pm 1$ ) multipliziert und das Produkt als Antwort bekannt gibt. Die Antwort ist also immer  $+1$  oder  $-1$ . Bei geschickter Wahl der Observablen ergibt sich der Erwartungswert der Antwort in Matrixdarstellung

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0.5 & -1. & 0.5 \\ 0 & -1. & 0.5 & 0.5 \\ 0 & 0.5 & 0.5 & -1. \end{pmatrix}.$$

Die positiven Funktionswerte von  $f$  werden also mit Wahrscheinlichkeit 75 % richtig berechnet, die Negativen immer. Insgesamt ist die Antwort also in 83 % der Fälle richtig.

## 2.2 Funktionen für Bell-Ungleichungen ohne Kommunikation

Die in [7] beschriebenen Funktionen sind ein Spezialfall der bisher betrachteten Funktionen. Hier ist gewährleistet, dass die optimale Antwortfunktion die Form  $A(x_1, \dots, x_n) = \prod_i y_i a_i(x_i)$  hat, sodass die Schranke  $B_A$  der Schranke  $B$  einer Bellschen Ungleichung ohne Kommunikation entspricht. Man beachte, dass diese spezielle Antwortfunktion im Allgemeinen eine Kommunikationskomplexität  $n$  hat, d.h. jede Partei muss  $a_i$  kommunizieren. Trotzdem entspricht diese Antwortfunktion dem Erwartungswert eines Bell-Experimentes, in dem keine Kommunikation möglich ist.

### Satz 2.2

Seien  $y_1, \dots, y_n$  gleichverteilte Zufallsbits und  $x_1, \dots, x_n$   $m$ -Bit lange Inputs, die  $Q$ -verteilt sind. Jede Partei  $i$  der  $n$ -Parteien erhält  $y_i$  und  $x_i$ . Hat die zu berechnende Funktion die Form

$$f(y_1, \dots, y_n, x_1, \dots, x_n) = \prod_i y_i \operatorname{sgn}(g(x_1, \dots, x_n)),$$

so ist für ein Bit Kommunikation pro Partei  $B_A = B$ .

Beweis: Der Beweis geht wie in [7]. Jede binäre Funktion  $A : \{-1, 1\}^n \rightarrow \{-1, 1\}$  lässt sich entwickeln als

$$A(a_1, \dots, a_n) = \sum_{j_1, \dots, j_n=0,1} A_{j_1, \dots, j_n} \prod_{i=1}^n a_i^{j_i} \quad (2.6)$$

mit den Entwicklungskoeffizienten

$$A_{j_1, \dots, j_n} = \frac{1}{2^n} \sum_{a_1, \dots, a_n = \pm 1} A(a_1, \dots, a_n) \prod_{i=1}^n a_i^{j_i}.$$

Die Antwortfunktion  $A$  von Alice ist eine Funktion  $A(y_1, x_1, e_2, \dots, e_n)$ . Die gesendeten Bits  $e_i$  der anderen Parteien sind Funktionen  $e_i(x_i, y_i)$ . Sie werden in einen von  $y$  abhängigen Teil und einen  $y$ -unabhängigen Teil aufgespalten und als  $e_i(x_i, y_i) = a_i(x_i)y_i + b_i(x_i)$  geschrieben. In der Entwicklung nach Gleichung 2.6 können diese Teile identifiziert werden.

$$\begin{aligned} e_i(x_i, y_i) &= \sum_{j_0, j_1, \dots, j_m = 0, 1} E_{j_0, \dots, j_m} y_i^{j_0} \prod_{r=1}^m (x_i^{(r)})^{j_r} \\ &= \underbrace{\left( \sum_{j_1, \dots, j_m = 0, 1} E_{1, j_1, \dots, j_m} y_i^{j_0} \prod_{r=1}^m (x_i^{(r)})^{j_r} \right)}_{a_i(x_i)} y_i + \underbrace{\sum_{j_1, \dots, j_m = 0, 1} E_{0, j_1, \dots, j_m} \prod_{r=1}^m (x_i^{(r)})^{j_r}}_{b_i(x_i)} \end{aligned}$$

Mit  $x_i^{(r)}$  ist das  $r$ -te Bit von  $x_i$  redefiniert auf die Werte  $\{-1, 1\}$  gemeint. Es werden die Abkürzungen

$$\begin{aligned} \sum_x &= \sum_{x_1, \dots, x_n = 0}^{2^m - 1}, & \sum_y &= \sum_{y_1, \dots, y_n = -1, 1}, \\ \sum_j &= \sum_{j_1, \dots, j_{m+n} = 0, 1}, & x &= x_1, \dots, x_n, \\ y &= y_1, \dots, y_n & \text{und} & j = j_1 \dots j_{n+m} \end{aligned}$$

verwendet. Es wird nun das Skalarprodukt  $(f, A)$  für das optimale  $A$  in der allgemeinen Form von Gleichung 2.6 abgeschätzt.

$$\begin{aligned} B_A &= \Sigma(f, A) \\ &= \Sigma \sum_x \sum_y Q(x) f(x, y) A(x_1, y_1, e_2(x_2, y_2), \dots, e_n(x_n, y_n)) \\ &= \frac{1}{2^n} \sum_{x, y} g(x) \prod_{l=1}^n y_l A(x_1, y_1, e_2, \dots, e_n) \end{aligned}$$

Einsetzen der Entwicklung von  $A$  nach Gleichung 2.6 und die Aufspaltung nach  $y$ -Abhängigkeit der gesendeten Bits  $e_i$  gibt:

$$\begin{aligned} &= \frac{1}{2^n} \sum_{x, y} g(x) \prod_{l=1}^n y_l \sum_j A_j \prod_{r=1}^m (x_1^{(r)})^{j_r} y_1^{j_{m+1}} \prod_{i=2}^n e_i^{j_{i+m}} \\ &= \frac{1}{2^n} \sum_{x, y} g(x) \prod_{l=1}^n y_l \sum_j A_j \prod_{r=1}^m (x_1^{(r)})^{j_r} \prod_{i=2}^n (a_i(x_i)y_i + b_i(x_i))^{j_{i+m}} \end{aligned}$$

Zusammenfassen der Produkte über  $l$  und  $i$ :

$$= \frac{1}{2^n} \sum_x g(x) \sum_j A_j \prod_{r=1}^m \left(x_1^{(r)}\right)^{j_r} \sum_y y_1 y_1^{j_{m+1}} \prod_{i=2}^n y_i (a_i(x_i) y_i + b_i(x_i))^{j_{i+m}}$$

Die Summe über  $y_1, \dots, y_n$  kann jetzt ausgeführt werden, denn  $\sum_{y_i=-1,1} y_i^1$  ist 0 und  $\sum_{y_i=-1,1} y_i^0 = 2$ :

$$= \sum_x g(x) \sum_{j_1, \dots, j_m} A_{j_1, \dots, j_m, 1 \dots 1} \prod_{r=1}^m \left(x_1^{(r)}\right)^{j_r} \prod_{i=2}^n a_i(x_i)$$

Es sei  $g_j(x) = \prod_{r=1}^m \left(x_1^{(r)}\right)^{j_r} g(x)$ . Diese veränderten Koeffizienten sind Koeffizienten einer anderen Bellschen Ungleichung, die aber die selbe klassische Schranke besitzt. Ist für ein  $x_1$  der veränderte Koeffizient  $g_j(x_1, \dots, x_n) = -g(x_1, \dots, x_n)$ , so wird das Vorzeichen von  $a_1(x_1)$  gewechselt.

$$\begin{aligned} &= \sum_{j_1, \dots, j_m} A_{j_1, \dots, j_m, 1 \dots 1} \sum_x g_j(x) \prod_{i=2}^n a_i(x_i) \\ &\leq B \sum_{j_1, \dots, j_m} A_{j_1, \dots, j_m, 1 \dots 1} \end{aligned}$$

Hier wurde zuletzt die Bellsche Ungleichung angewendet. Wegen

$$\begin{aligned} &\left| \sum_{j_1, \dots, j_m} A_{j_1, \dots, j_m, 1 \dots 1} \right| \\ &= \left| \sum_{j_1, \dots, j_m} \frac{1}{2^{n+m}} \sum_{a_1, \dots, a_{n+m} = \pm 1} A(a_1, \dots, a_{n+m}) \prod_{i=1}^m a_i^{j_i} \prod_{i=m+1}^{m+n} a_i \right| \\ &\leq \left| \sum_{j_1, \dots, j_m} \frac{1}{2^{n+m}} \sum_{a_1, \dots, a_{n+m} = \pm 1} \prod_{i=1}^m a_i^{j_i} \right| \\ &= 1 \end{aligned}$$

folgt weiter in der Abschätzung des Skalarproduktes

$$\leq B.$$

Insgesamt wurde also  $B_A \leq B$  gezeigt. Andererseits gilt  $B_A \geq B$ , denn die Korrelationsfunktion  $A(x) = \prod_i a_i(x_i)$  erfüllt die Anforderungen an die Antwortfunktion.  $\square$

### 2.3 Quantenmechanische Erfolgswahrscheinlichkeit

In dem quantenmechanischen Protokoll erhält jede Partei einen Teil des Gesamtsystems. An diesem Teilsystem führt jede Partei eine Messung durch. Anschliessend sendet jede Partei  $y_i a_i$ , wobei  $a_i$  das Messergebnis ist. Als Ergebnis der Funktion  $f$  wird dann  $\prod_i y_i a_i$

bekannt gegeben. Die Erfolgswahrscheinlichkeit dieses Protokolls ist

$$\begin{aligned}
 P_Q &= \frac{1}{2} + \frac{1}{2} \sum_{x_1, \dots, x_n} Q(x_1, \dots, x_n) f(x_1, \dots, x_n) E(x_1, \dots, x_n) \\
 &= \frac{1}{2} + \frac{\sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) E(x_1, \dots, x_n)}{2 \sum_{x_1, \dots, x_n} |g(x_1, \dots, x_n)|} \\
 &= \frac{1}{2} + \frac{S}{2 \sum_{x_1, \dots, x_n} |g(x_1, \dots, x_n)|}. \tag{2.7}
 \end{aligned}$$

In der letzten Zeile wurde der Bell-Parameter  $S = \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) E(x_1, \dots, x_n)$  eingesetzt. Die quantenmechanische Erfolgswahrscheinlichkeit ist genau dann größer als klassisch möglich, wenn die Bell-Ungleichung  $S \leq B$  verletzt wird. Die maximale Verletzung wird gefunden, indem über die Observablen und den Zustand des Gesamtsystems (numerisch) maximiert wird.

## 2.4 Beispiele

Die Vorgehensweise zum Ermitteln der klassischen und quantenmechanischen Erfolgswahrscheinlichkeit kann an folgenden Beispielen noch einmal nachvollzogen werden. Die vorgezeichneten Beispiele sind Standardfunktionen aus der Kommunikationskomplexität (siehe auch [13]). In drei von vier Beispielen wird ein Vorteil des quantenmechanischen Protokolls festgestellt.

### Beispiel 2.2 (Die Größer-Gleich-Funktion)

Ein Beispiel für ein Kommunikationskomplexitätsproblem zwischen zwei Parteien ist die Funktion

$$GEQ = y_1 y_2 \begin{cases} 1 & \text{falls } x_1 \geq x_2 \\ -1 & \text{sonst} \end{cases}, \tag{2.8}$$

die bis auf den Faktor  $y_1 y_2$  der Größer-Gleich-Funktion entspricht. Für  $m = 1$  ist dies die CHSH-Ungleichung. Sei nun  $m = 2$ . Der von  $y$  unabhängige Teil der Funktion lässt sich als Matrix

$$(GEQ)_{x_1, x_2} = \begin{pmatrix} 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix}_{x_1, x_2}$$

darstellen, wobei die Indizes  $x_1, x_2 \in \{0, 1, 2, 3\}$  sind. Man erkennt hier, dass eine optimale klassische Strategie mit einem Bit Kommunikation darin besteht, die Messergebnisse von Alice konstant 1 zu setzen, während Bobs Messergebnis für die Messeinstellung zu  $x_2 = 3$  auf  $-1$  gesetzt wird. Eine optimale klassische Strategie lautet also

$$A(x_1, x_2) = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \end{pmatrix}_{x_1, x_2}.$$

Damit ist die lokalrealistische Schranke in diesem Beispiel  $B = 8$ . Nach Satz 2.1 ist die klassische Erfolgswahrscheinlichkeit also  $P_C = 3/4$ . Durch numerische Optimierung über Winkel und Zustand in Gleichung 2.7 erhält man eine optimale quantenmechanische Strategie

$$E(x_1, x_2) = \begin{pmatrix} 0.382683 & -0.382683 & -0.92388 & -0.92388 \\ 0.92388 & 0.382683 & -0.382683 & -0.92388 \\ 0.92388 & 0.92388 & 0.382683 & -0.382683 \\ 0.382683 & 0.92388 & 0.92388 & 0.382683 \end{pmatrix}_{x_1, x_2} .$$

Diese Strategie führt zu  $S = 10.4525$  und die quantenmechanische Erfolgswahrscheinlichkeit ist  $P_Q = 0.826641$ . In diesem Beispiel kann die Erfolgswahrscheinlichkeit also mit Verschränkung größer sein als klassisch möglich.

### Beispiel 2.3 (*Das innere Produkt*)

Das innere Produkt zweier Zahlen  $x_1$  und  $x_2$  ist definiert als

$$IP(x_1, x_2) = \sum_{i=1}^m x_1^{(i)} x_2^{(i)} \pmod{2},$$

wobei  $x_1^{(i)}$  das  $i$ -te Bit von  $x_1$  bezeichnet. Es soll die Funktion  $f(x_1, x_2, y_1, y_2) = y_1 y_2 IP(x_1, x_2)$  berechnet werden. Für  $m = 3$  ist der  $y$ -unabhängige Teil der Funktion

$$(IP)_{x_1, x_2} = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix}_{x_1, x_2} .$$

Maximierung über alle klassischen Strategien liefert  $B = 20$ , also  $P_C = 0.65625$ , während  $S = 22.6274$  ist, was einer Erfolgswahrscheinlichkeit  $P_Q = 0.676777$  entspricht. Das quantenmechanische Protokoll hat also eine höhere Erfolgswahrscheinlichkeit als alle klassischen Protokolle.

### Beispiel 2.4 (*Disjunktheit*)

Wir definieren die Funktion „Disjunktheit“ mit Hilfe des bitweisen Und & als

$$DISJ(x_1, x_2) = \begin{cases} 1 & x_1 \& x_2 = 0 \\ -1 & x_1 \& x_2 \neq 0 \end{cases} .$$

Interpretiert man  $x_1$  bzw.  $x_2$  als charakteristische Vektoren<sup>2</sup> von Teilmengen von  $\{1, \dots, m\}$ , so gibt  $DISJ$  an ob die beiden Mengen disjunkt sind. Es soll die Funktion  $f(x_1, x_2, y_1, y_2) = y_1 y_2 DISJ(x_1, x_2)$  berechnet werden. Für  $m = 3$  erhalten wir

als  $y$ -unabhängigen Teil von  $f$

$$(DISJ)_{x_1, x_2} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{pmatrix}_{x_1, x_2}$$

und der zu dieser Matrix gehörende Bell-Parameter ist  $S = 38.3274$ . Weil dieser nicht durch zwei teilbar ist, handelt es sich um eine Bellsche-Ungleichung (Satz 1.3). Tatsächlich ist  $P_Q = 0.799433 > P_C = 0.796875$ .

### Beispiel 2.5 (Gleichheit)

Für die Funktion

$$f(x_1, x_2, y_1, y_2) = y_1 y_2 EQ(x_1, x_2)$$

mit

$$EQ(x_1, x_2) = \begin{cases} 1 & x_1 = x_2 \\ -1 & x_1 \neq x_2 \end{cases}$$

erhält man durch Maximierung  $B = S = 48$  ( $P_C = P_Q = 0.875$ ). Die zu  $EQ$  gehörende Ungleichung ist also keine Bellsche Ungleichung und Verschränkung bietet bei der Berechnung der Funktion keinen Vorteil.

<sup>2</sup>Die  $i$ -te Komponente des charakteristischen Vektors ist 1, wenn  $i$  Element der Menge ist und sonst 0



## Kapitel 3

# Detektoreffizienz und Kontrast

Die vorangegangenen Überlegungen werden in diesem Kapitel erweitert um das reale Experiment genauer modellieren zu können. Der gewünschte Zustand  $|\psi\rangle$  kann experimentell nicht perfekt präpariert werden. Stattdessen wird mit einer gewissen Wahrscheinlichkeit ein anderer Zustand vorliegen. Wir nehmen an, dass alle Zustände dieses Rauschens gleich wahrscheinlich sind. Die Sichtbarkeit des Zustandes  $|\psi\rangle$  gegenüber dem Rauschen wird Kontrast von  $|\psi\rangle$  genannt.

### Definition 3.1 (*Kontrast*)

*Kann der experimentell vorliegende Zustand durch die Dichtematrix*

$$\rho = V |\psi\rangle \langle\psi| + \frac{1-V}{2^n} \mathbb{1}$$

*beschrieben werden, so heißt  $V$  Kontrast des Zustandes  $|\psi\rangle$ .*

Für die hier wichtige Observable  $A = (\vec{a} \cdot \vec{\sigma})^{\otimes n}$  ist der Erwartungswert des verrauschten Zustandes

$$\begin{aligned} E_\rho &= \text{spur}(A\rho) = V \langle\psi| A |\psi\rangle + \frac{1-V}{2^n} \text{spur} A \\ &= V \langle\psi| A |\psi\rangle. \end{aligned}$$

Der Erwartungswert wird also hier mit dem Faktor  $V$  geschwächt. Zusätzlich zu dem Rauschen sind die Detektoren nicht ideal, sodass einige Messungen scheitern. Wir betrachten hier nur den Fall, dass der Detektor nicht feuert, obwohl er von einem Teilchen getroffen wurde<sup>1</sup>. Wir definieren ein Maß für die Qualität eines Detektors, die Detektoreffizienz.

### Definition 3.2 (*Detektoreffizienz*)

*Die (intrinsische) Detektoreffizienz  $\eta$  ist das Verhältnis der Anzahl detektierter Teilchen zur Gesamtzahl der Teilchen die den Detektor erreichen.*

Das in Abschnitt 2.2 eingeführte quantenmechanische Protokoll kann nicht durchgeführt werden, wenn eine Messung nicht erfolgreich ist. Um insgesamt eine hohe Erfolgswahrscheinlichkeit zu erhalten, können sich die Parteien auf folgendes Protokoll einigen[11]. Jeder führt zunächst das quantenmechanische Protokoll durch. Sollte dabei seine Messung scheitern, so fährt er mit dem klassischen Protokoll fort. Falls alle Messungen erfolgreich

<sup>1</sup>Es ist auch denkbar, dass ein Detektor ein falsches Messergebnis liefert. Und zusätzlich könnte man auch die sogenannten „dark counts“ berücksichtigen, wenn der Detektor feuert obwohl die Quelle ausgeschaltet ist.

sind, wird das quantenmechanische Protokoll durchgeführt. Falls alle Messungen scheitern wird das klassische Protokoll durchgeführt. In allen anderen Fällen ist der Ausgang des Protokolls zufällig. Der Erwartungswert dieses Protokolls ist

$$E'(x_1, \dots, x_n) = \eta^n V \underbrace{E(x_1, \dots, x_n)}_{\text{QM-EW}} + (1 - \eta)^n \underbrace{A(x_1, \dots, x_n)}_{\text{kl. Antwortfunktion}} + (1 - \eta^n V - (1 - \eta)^n) \cdot \underbrace{0}_{\text{zufälliges Bit}}$$

und Einsetzen in die linke Seite der Bellschen Ungleichung liefert einen neuen Bell-Parameter

$$S' = \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) E'(x_1, \dots, x_n)$$

mit der dazugehörigen Erfolgswahrscheinlichkeit

$$\begin{aligned} P'_Q = P(E' = f) &= \frac{1}{2} \left( 1 + \frac{S'}{\Sigma} \right) \\ &= \frac{1}{2} \left( 1 + \frac{\eta^n V S}{\Sigma} + \frac{(1 - \eta)^n B}{\Sigma} + 0 \right) \\ &= \frac{1}{2} \left( 1 + \frac{\eta^n V (2P_Q - 1)\Sigma}{\Sigma} + \frac{(1 - \eta)^n (2P_C - 1)\Sigma}{\Sigma} \right) \\ &= \eta^n V P_Q + (1 - \eta)^n P_C + (1 - \eta^n V - (1 - \eta)^n) \frac{1}{2}. \end{aligned} \quad (3.1)$$

Den qualitativen Verlauf von  $P'_Q$  in Abhängigkeit von  $\eta$  zeigt Abbildung 3.1. Für  $\eta = 0$

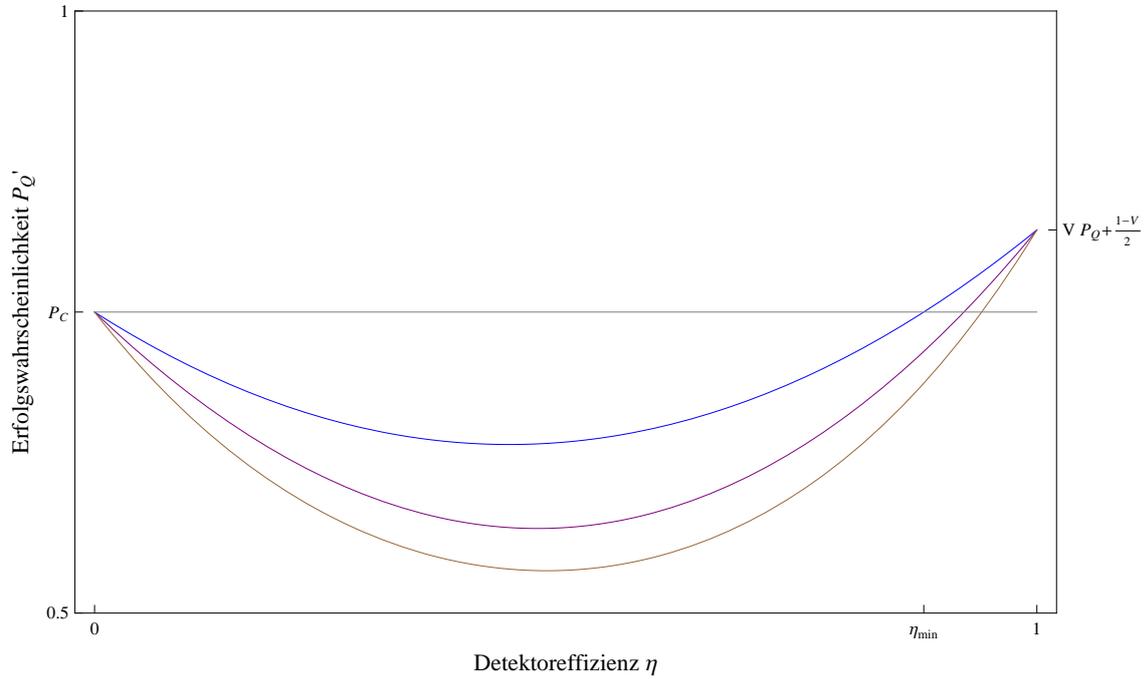


Abbildung 3.1: Die  $\eta$ -Abhängigkeit der Erfolgswahrscheinlichkeit des quantenmechanischen Protokolls mit nichtidealen Detektoren  $P'_Q$  für  $n = 2$  (blau),  $n = 3$  (purpur) und  $n = 4$  (braun) Parteien. Unabhängig von der Anzahl der Parteien wurde hier  $P_C = 75\%$  und  $P_Q = 85\%$  angenommen. Ab einer bestimmten Detektoreffizienz  $\eta_{\min}$  ist das quantenmechanische Protokoll erfolgreicher als jedes klassische Protokoll.

ist  $P'_Q = P_C$ , d.h. das quantenmechanische Protokoll kann nie angewendet werden. Für etwas höhere Detektoreffizienz mehren sich die Fälle, in denen die Parteien unterschiedliche Protokolle anwenden. Dadurch verkleinert sich die Erfolgswahrscheinlichkeit zunächst mit wachsendem  $\eta$ . Erst ab einem bestimmten  $\eta_{\min}$  wird das quantenmechanische Protokoll häufig genug erfolgreich durchgeführt, sodass die Erfolgswahrscheinlichkeit jetzt höher ist als klassisch möglich. Die Bedingung  $P'_Q = P_C$  lässt sich für kleine  $n$  auflösen nach  $\eta$ . Für  $n = 2$  erhält man

$$\eta_{\min}^{(2)} = \frac{4P_C - 2}{-1 + 2P_C - V + 2P_Q V} = \frac{2B}{B + VS} \quad (3.2)$$

und für  $n = 3$

$$\begin{aligned} \eta_{\min}^{(3)} &= \frac{6(2P_C - 1)}{3(2P_C - 1) + \sqrt{3}\sqrt{(2P_C - 1)(1 - 4V - 2P_C + 8VP_Q)}} \\ &= \frac{6B}{3B + \sqrt{3}\sqrt{B(4VS - B)}}. \end{aligned} \quad (3.3)$$

### 3.1 Kritische Detektoreffizienz des Detektor-Schlupfloches

Das Detektor-Schlupfloch wurde in Abschnitt 1.3 beschrieben. Kurz gesagt ist es die mögliche Kritik an einem Bellexperiment zu argumentieren, dass unter Berücksichtigung der verworfenen Messdaten (wenn nicht alle Detektionen eines Paares/Systems erfolgreich waren) die Bellsche Ungleichung auch nicht verletzt worden wäre. Es gibt eine kritische Detektoreffizienz, ab der das Schlupfloch geschlossen wird (siehe auch Anhang E). Genauer gibt es einen Wert  $\eta_{\text{crit}}$ , sodass für eine Detektoreffizienz  $\eta > \eta_{\text{crit}}$  ausgeschlossen werden kann, dass eine lokalrealistische Theorie den ungemessenen Daten Werte zuordnen kann, mit denen dann insgesamt die Bellungleichung eingehalten wird. Der folgende Satz stellt einen Zusammenhang zwischen  $\eta_{\text{crit}}$  und dem oben betrachteten  $\eta_{\min}$  her.

#### Satz 3.1

Die kritische Detektoreffizienz  $\eta_{\text{crit}}$ , die benötigt wird um das Detektor-Schlupfloch zu schließen ist genauso groß wie oder kleiner als die minimale Detektoreffizienz  $\eta_{\min}$ , ab der das beschriebene quantenmechanische Protokoll erfolgreicher ist als jedes klassische Protokoll ( $\eta_{\text{crit}} \leq \eta_{\min}$ ).

Beweis: Es wird eine Bellsche Ungleichung angegeben, die das Detektor-Schlupfloch ab  $\eta_{\min}$  schliesst. Sie ist (ähnlich wie bei [24])

$$\left| \sum_{x_1, \dots, x_n=0}^1 g(x_1, \dots, x_n) e(x_1, \dots, x_n) \right| \leq B \quad (3.4)$$

und berücksichtigt nichtideale Detektoren, indem die neuen Erwartungswerte

$$e(x_1, \dots, x_n) = \frac{1}{1 - P'(0, 0, \dots, 0)} \sum_{a_1, \dots, a_n = -1, 0, 1} a_1 \dots a_n P'_{x_1, \dots, x_n}(a_1, \dots, a_n) \quad (3.5)$$

auch das Ereignis „nicht-Detektion“ enthalten, welches mit 0 gewertet wird. Die neue Ungleichung ist die natürliche Erweiterung der ursprünglichen Ungleichung  $\sum gE \leq B$  auf die gesamten Messdaten. Sie besitzt kein Detektor-Schlupfloch, weil alle Messungen, auch die „gescheiterten“ einfließen. Wird die Ungleichung von den Messdaten verletzt, so kann

eine lokalrealistische Erklärung ausgeschlossen werden. Der mit Hilfe dieser speziellen Ungleichung aus den Messdaten berechnete Wert kann von einer klassischen Theorie erklärt werden, wenn die Ungleichung eingehalten wird. Es kann aber eine bessere Ungleichung geben, die mit den selben Messdaten verletzt wird.

Der Wert der klassischen Schranke  $B$  ändert sich durch das neue Messergebnis „0“ (Nichtdetektion) nicht. Größen, die sich auf die Gesamtheit der Messwerte und die verworfenen Messungen beziehen, werden im Folgenden mit einem Strich gekennzeichnet. Mit  $P'(\neq 0, \dots, \neq 0)$  ist die Wahrscheinlichkeit gemeint, dass alle Messergebnisse ungleich Null sind, d.h. dass die Messung an jedem Teilchen erfolgreich ist. Der Erwartungswert auf allen Messergebnissen (inklusive Nichtdetektion)  $e$  wird auf die Messungen normiert, in denen mindestens ein Teilchen nachgewiesen wurde (andere Messdaten liegen auch nicht vor!). Er lässt sich auf den Erwartungswert im Fall der idealen Detektoren zurückführen, wie folgende Rechnung zeigt.

$$\begin{aligned} e(x_1, \dots, x_n) &= \frac{1}{1 - P'(0, 0, \dots, 0)} \sum_{a_1, \dots, a_n = -1, 0, 1} a_1 \dots a_n P'_{x_1, \dots, x_n}(a_1, \dots, a_n) \\ &= \frac{P'(\neq 0, \dots, \neq 0)}{1 - P'(0, 0, \dots, 0)} \sum_{a_1, \dots, a_n = -1, 0, 1} a_1 \dots a_n \frac{P'_{x_1, \dots, x_n}(a_1, \dots, a_n)}{P'(\neq 0, \dots, \neq 0)} \\ &= \frac{P'(\neq 0, \dots, \neq 0)}{1 - P'(0, 0, \dots, 0)} \sum_{a_1, \dots, a_n = -1, 1} a_1 \dots a_n P_{x_1, \dots, x_n}(a_1, \dots, a_n) \\ &= \frac{\eta^n}{1 - (1 - \eta)^n} E(x_1, \dots, x_n) \end{aligned}$$

Einsetzen in Gleichung 3.4 liefert

$$\begin{aligned} \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) e(x_1, \dots, x_n) &= \frac{\eta^n}{1 - (1 - \eta)^n} \sum_{x_1, \dots, x_n} g(x_1, \dots, x_n) E(x_1, \dots, x_n) \\ &= \frac{\eta^n}{1 - (1 - \eta)^n} VS \leq B. \end{aligned} \quad (3.6)$$

Die neue Ungleichung wird nur verletzt, wenn  $\eta > \eta_{\text{crit}}$ . Das heisst, dass die gemessenen und verworfenen Daten zusammen eine lokalrealistische Erklärung nicht ausschließen, wenn die Detektoreffizienz  $\eta$  kleiner als oder gleich  $\eta_{\text{crit}}$  ist. Gleichheit in Ungleichung 3.6 gilt genau dann wenn  $\eta = \eta_{\text{crit}}$ . Also

$$B = \frac{\eta_{\text{crit}}^n}{1 - (1 - \eta_{\text{crit}})^n} VS.$$

Andererseits kann man in die Bedingung  $P'_Q \geq P_C$  (siehe Gleichung 3.1) die klassische Erfolgswahrscheinlichkeit  $P_C = \frac{1}{2} \left(1 + \frac{B}{S}\right)$  und die quantenmechanische Erfolgswahrscheinlichkeit  $P_Q = \frac{1}{2} \left(1 + \frac{S}{\Sigma}\right)$  einsetzen. Man erhält so eine Ungleichung mit der klassischen Schranke  $B$  und dem Bell-Parameter  $S$ . Auflösen nach  $B$  liefert

$$B = \frac{\eta_{\text{min}}^n}{1 - (1 - \eta_{\text{min}})^n} VS.$$

Der Vergleich zeigt  $\eta_{\text{min}} = \eta_{\text{crit}}$  (für diese Ungleichung), d.h. diese neue Ungleichung bietet eine Möglichkeit mit der Detektoreffizienz  $\eta_{\text{min}}$  das Detektor-Schlupfloch zu schließen. Allerdings könnte es für die selbe physikalische Situation (Anzahl an Teilchen, Messeinstellungen, etc.) bessere Ungleichungen oder Methoden geben, die eine niedrigere Detek-

toeffizienz benötigen um klassische Erklärungen auszuschließen. □

Die im Beweis genannte Ungleichung kann auch eingehalten werden, wenn das Rauschen groß genug ist. Der Bereich in dem  $\eta$  und  $V$  gemeinsam eine Verletzung der Ungleichung erlauben ist in Abbildung 3.2 dargestellt. Auch hier gilt, dass eine bessere Ungleichung oder andere Methode mehr Rauschen „vertragen“ könnte. Für die CHSH-Ungleichung wird bei idealen Detektoren ein Untergrund kleiner als etwa 0.3 benötigt (in Übereinstimmung mit [25]). Es folgen einige Beispiele zur kritischen Detektoreffizienz.

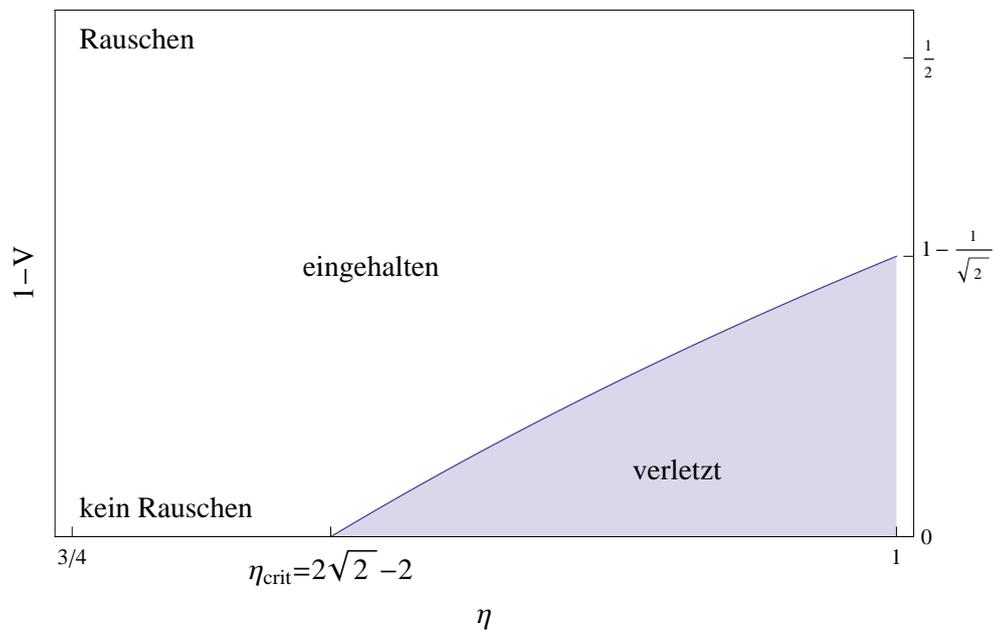


Abbildung 3.2: Aufgetragen ist der Untergrund  $1 - V$  gegenüber der Detektoreffizienz  $\eta$ . In dem blau eingefärbten Bereich wird die Ungleichung 3.6 verletzt. Die eingetragenen Werte gelten für die CHSH-Ungleichung.

### Beispiel 3.1

Sei

$$(g)_{x_1, x_2} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$

also die CHSH-Ungleichung gegeben. Die Erfolgswahrscheinlichkeiten sind

$$P_C = \frac{3}{4}$$

und  $P_Q = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{2}} \right).$

Bei perfektem Kontrast  $V = 1$  ist die minimale Detektoreffizienz

$$\eta_{\min} = 2(\sqrt{2} - 1) \approx 83\%.$$

Dieses Ergebnis stimmt mit dem Ergebnis von [24] für  $\eta_{\text{crit}}$  überein.

**Beispiel 3.2**

Eine weitere Bell-Ungleichung, für die  $\eta_{\text{crit}}$  bekannt ist, ist die Braunstein-Caves Kettenungleichung für 2 Parteien und  $K$  Messeinstellungen,

$$|E(A_{2K-1}, B_{2K}) - E(A_1, B_{2K})| + \sum_{k=2}^K |E(A_{2k-3} B_{2k-2}) + E(A_{2k-1} B_{2k-2})| \leq 2K - 1.$$

Es wurde bereits von [26] gezeigt, dass

$$\eta_{\text{crit}}(K) = \frac{2}{\frac{K}{K-1} \cos\left(\frac{\pi}{2K}\right) + 1}$$

ist. Verwendet man die Schranke und den Bell-Parameter aus [26] so erhält man

$$P_C = \frac{1}{2} \left( 1 + \frac{2K-2}{2K} \right)$$

und  $P_Q = \frac{1}{2} \left( 1 + 2K \cos\left(\frac{\pi}{2K}\right) \frac{1}{2K} \right),$

was zu einer minimalen Detektoreffizienz von

$$\begin{aligned} \eta_{\text{min}} &= \frac{-2 + 4P_C}{-1 + 2P_C - V + 2P_Q V} \\ &= \frac{2}{1 + V \frac{K}{K-1} \cos\left(\frac{\pi}{2K}\right)} \\ &\stackrel{V=1}{=} \frac{2}{1 + \frac{K}{K-1} \cos\left(\frac{\pi}{2K}\right)} = \eta_{\text{crit}} \end{aligned}$$



sches Modell existieren kann, welches dies für Detektoreffizienzen über  $\eta_{\text{crit}}$  leistet. Da  $\eta_{\text{crit}} < \eta_{\text{min}}$  gilt ist die von Cabello et. al. verwendete Methode hier besser geeignet um die Detektoreffizienz zu bestimmen, die zum Schließen des Detektor-Schlupflochs benötigt wird.

## 3.2 Protokolle für niedrige Detektoreffizienz

Es gibt verschiedene denkbare Ansätze um Protokolle zu suchen, die eine kleine Detektoreffizienz  $\eta_{\text{min}}$  erfordern. Im folgenden Abschnitt werden Überlegungen zu zwei-Parteien-Problemen mit einer großen Anzahl Messeinstellungen  $m$  vorgestellt. Anschließend wird gezeigt, dass die Mermin Ungleichung zu einer Detektoreffizienz führt, die kleiner ist als die der CHSH-Ungleichung. Dort wird also nicht  $m$  vergrößert, sondern die Anzahl an Parteien  $n$ .

### 3.2.1 Zwei Parteien mit langem Input

Die minimale Detektoreffizienz als Funktion von  $P_C$  und  $P_Q$  zeigt Abbildung 3.3. Je kleiner  $P_C$  ist, desto kleiner wird  $\eta_{\text{min}}$ . Für  $P_C \approx \frac{1}{2}$  könnten kleine Abstände  $P_Q - P_C$  schon für  $\eta_{\text{min}} \approx 0$  ausreichen. Um Funktionen für niedrige Detektoreffizienz zu finden liegt es deshalb nahe, Funktionen zu betrachten, die mit wachsender Inputgröße  $m$  aber nur einem Bit Kommunikation immer seltener korrekt berechnet werden können.

Wenn  $S(m)$  schneller wächst als  $B(m)$  (und  $P_C \xrightarrow{m \rightarrow \infty} \frac{1}{2}$ ) geht  $\eta_{\text{min}}(m)$  gegen 0. Wenn  $S(m)$  und  $B(m)$  ein ähnliches Wachstumsverhalten zeigen, genauer wenn immer  $S(m) = h \cdot B(m)$  mit dem selben Faktor  $h$ , dann bleibt  $\eta_{\text{min}}$  gerade konstant, wie folgende Überlegung zeigt.

$$\begin{aligned} VS(m) \frac{\eta_{\text{min}}^n}{1 - (1 - \eta_{\text{min}})^n} &= B(m) \\ \Rightarrow VhB(m) \frac{\eta_{\text{min}}^n}{1 - (1 - \eta_{\text{min}})^n} &= B(m) \\ \Rightarrow Vh \frac{\eta_{\text{min}}^n}{1 - (1 - \eta_{\text{min}})^n} &= 1 \\ \Rightarrow \eta_{\text{min}} &= \text{const.} \Big|_m \end{aligned}$$

Es ist bekannt, dass es Probleme gibt, deren quantenmechanische Kommunikationskomplexität exponentiell langsamer ansteigt als klassisch [28]. Es scheint daher möglich Funktionen zu finden, für die  $S(m)$  exponentiell schneller wächst als  $B(m)$ . Dies ist mir innerhalb des für diese Arbeit vorgesehenen Zeitraums leider nicht gelungen. Ein verfolgter Ansatz wird im Folgenden kurz skizziert. Es sei eine Funktion  $g$  für zwei Parteien, zum Beispiel

$$g = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

gegeben. Die Parteien sollen  $f = y_1 y_2 g$  berechnen, wie in Abschnitt 2.2. Daraus wird über  $g_i = g^{\otimes i}$  eine Folge von Funktionen gebildet. Die Winkel für die Messungen der  $i$ -ten Iteration berechnen sich gemäß

$$\phi_{x_{1/2}}^{A/B} = \sum_{k=0}^{i-1} \phi_{\frac{x_{1/2}}{d^k}}^{A/B} \pmod{d}$$

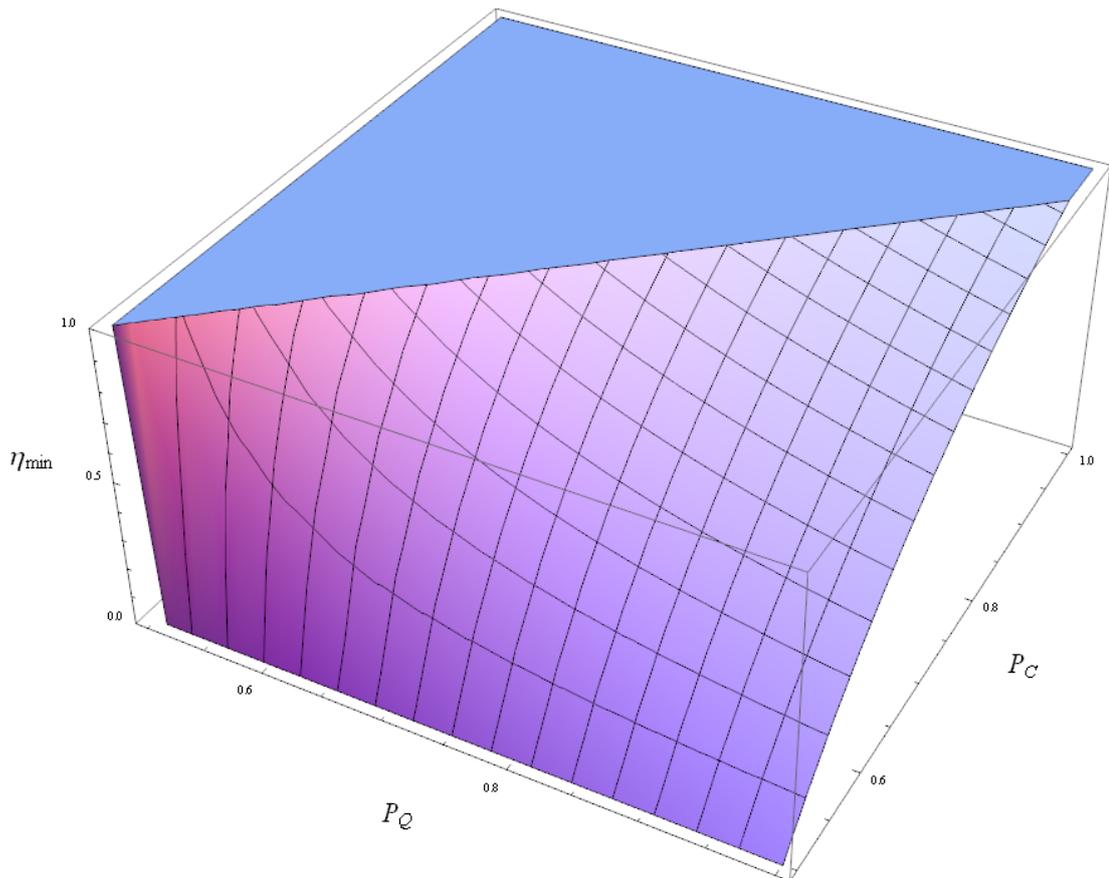


Abbildung 3.3:  $\eta_{\min}$  als Funktion von  $P_C$  und  $P_Q$ . Es wurde für die Darstellung  $V = 0.9$  gewählt. Man sieht, dass die benötigte Detektoreffizienz gegen 0 geht, wenn  $P_C$  gegen  $\frac{1}{2}$  geht.

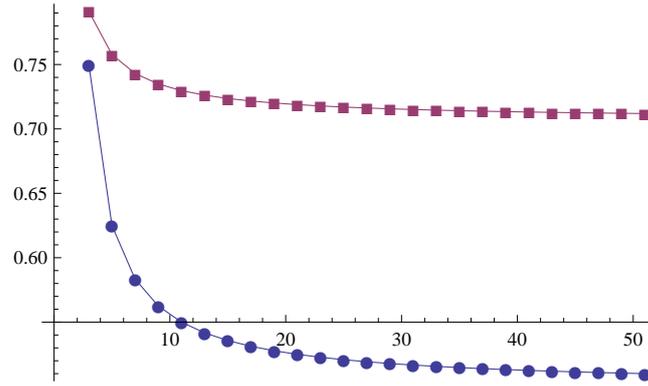


Abbildung 3.4: Die minimale Detektoreffizienz  $\eta_{\min}$  des zur Mermin-Ungleichung gehörenden Kommunikationskomplexitätsproblem (purpur) und die kritische Detektoreffizienz des Detektorschleppfloches  $\eta_{\text{crit}} = \frac{n}{2n-2}$  [27]. Obwohl mit wachsendem  $n$  immer mehr Messungen erforderlich werden sinkt  $\eta_{\min}$ , weil die Verletzung der Bell-Ungleichung exponentiell zunimmt.

aus den optimalen Winkeln für  $g$  und man erhält damit den Bell-Parameter in Abhängigkeit der Iteration  $i$ :  $S_i = S^i$  (Beweis in Anhang F).

Es scheint zunächst auch  $B_i = B^i$  zu gelten. Dann würde

$$\eta_{\min,i} = \frac{2B_i}{B_i + VS_i} = \frac{2B^i}{B^i + VS^i}$$

für  $i \rightarrow \infty$  gegen 0 konvergieren, d.h. für einen Kontrast  $V > 0$  und eine Detektoreffizienz  $\eta > 0$  gibt es ein  $i$  sodass  $P'_{Q,i} > P_{C,i}$ . Für das oben angegebene  $g$  ändert sich aber ab einem bestimmten  $i$  die klassische Strategie und  $B_i > B^i$ . Mir ist nicht klar, wie man für ein anderes  $g$  die Schranke  $B_i = B^i$  beweisen könnte, falls so ein  $g$  überhaupt existiert.

### 3.2.2 Mermin Ungleichung

Die Funktion mit der mir geringsten bekannten Detektoreffizienz  $\eta_{\min}$  bisher ist für ungerades  $n$

$$g(x_1, \dots, x_n) = \sqrt{2^{n+1}} \cos\left(\frac{\pi}{2}(x_1 + \dots + x_n)\right).$$

Der Vorfaktor ist hier nur aus Gründen der einfacheren Vergleichbarkeit mit anderen Quellen, zum Beispiel [11], angegeben. Hier ist

$$S = \sqrt{2^{n+1}} \cdot 2^{n-1}$$

und  $B = 2^n$ ,

was bedeutet, dass  $P_Q = 1$  und  $P_C = 1/2(1 + 1/\sqrt{2^{n-1}})$  ist. Obwohl immer mehr Messungen erforderlich sind sinkt die minimale Detektoreffizienz  $\eta_{\min}$  für wachsendes  $n$  (siehe Abbildung 3.4). Im Grenzwert ist  $\eta_{\min} = 1/\sqrt{2}$ , wie folgende Rechnung zeigt.

$$\frac{\eta^n}{1 - (1 - \eta)^n} V = \sqrt{2^{1-n}}$$

$$\Rightarrow \eta = V^{-1/n} (1 - (1 - \eta)^n)^{1/n} 2^{\frac{1-n}{2n}}$$

$$\Rightarrow \eta \stackrel{n \rightarrow \infty, V \neq 0}{=} \frac{1}{\sqrt{2}}$$

### 3.3 Zusätzliche Kommunikation

Eine Ausgangsfrage dieser Arbeit war: Kann zusätzliche Kommunikation einen Vorteil für quantenmechanische Protokolle bieten? Genauer ist gefragt, ob mit zusätzlicher Kommunikation ein Vorteil der Protokolle mit Verschränkung schon bei geringerer Detektoreffizienz sichtbar wird. Hier könnte zusätzliche Information von den Parteien dazu verwendet werden den Anderen mitzuteilen, ob die Messung erfolgreich war.

Auch dem klassischen Protokoll stehen jetzt zwei Bit statt einem Bit zur Verfügung. In Abschnitt 3.4 wird begründet, warum das klassische Protokoll mit einem zusätzlichen Bit immer eine Erfolgswahrscheinlichkeit  $\tilde{P}_C$  so groß wie  $P_Q$  oder größer besitzt. So entsteht also noch kein Vorteil. Deshalb wird jetzt der Fall betrachtet, dass ein Protokoll  $k$ -mal mit unabhängigen Argumenten wiederholt wird und für alle Wiederholungen gemeinsam ein weiteres Bit kommuniziert werden darf. Das Ziel der Parteien ist weiterhin die einzelnen Funktionswerte aller  $k$  Wiederholungen zu bestimmen.

Die gesendeten Bits können jetzt von den Inputs aller Wiederholungen abhängen. Da diese aber stochastisch unabhängig sind, kann die mittlere Erfolgswahrscheinlichkeit so wohl nicht gesteigert werden. Im Folgenden wird deshalb angenommen, dass jedes gesendete Bit nur von Input einer Wiederholung abhängt, also nur Information über diese Wiederholung enthält.

Wie bisher kann für jede Wiederholung ein Bit Kommunikation verwendet werden. Jede Partei kann für eine dieser Wiederholungen noch das zusätzliche Bit Kommunikation einsetzen. Das zusätzliche Bit verschiedener Parteien kann Informationen über verschiedene Wiederholungen enthalten, was zu einer größeren Erfolgswahrscheinlichkeit führen kann. Zum Beispiel könnte für eine Wahl von  $f$  die Erfolgswahrscheinlichkeit einer Wiederholung auf 1 gesteigert werden, wenn eine einzige Partei ein zusätzliches Bit versendet. Dann können  $n$  Wiederholungen statt eine der  $k$  Wiederholungen die Erfolgswahrscheinlichkeit 1 besitzen, wenn die Parteien ihr zusätzliches Bit auf verschiedene Wiederholungen beziehen.

Hier schränken wir diese Möglichkeiten ein, indem wir dem zusätzlichen Bit Kommunikation eine spezielle Rolle zuteilen. Wir fordern, dass das zusätzliche Bit jeder Partei zuerst und von allen gleichzeitig gesendet wird. Allerdings empfangen die Parteien nicht die Bits  $e_i \in \{0, 1\}$  aller Mitspieler, sondern nur ein Bit

$$h(e_1, \dots, e_n) = e_1 \cdot \dots \cdot e_n.$$

Den Parteien ist also nur bekannt, ob eine Partei das Bit auf 0 gesetzt hat, nicht jedoch welche. Da dieses Bit  $h$  also „anonym“ ist, muss es sich für alle Parteien auf die selbe Wiederholung beziehen. Diese Wiederholung hat jetzt die Erfolgswahrscheinlichkeit  $P_2 \geq$

$P_C$ . Im Mittel ist die neue Erfolgswahrscheinlichkeit

$$\begin{aligned}\tilde{P}_C &= \left(1 - \frac{1}{k}\right) P_C + \frac{1}{k} P_2 \\ &\leq \left(1 - \frac{1}{k}\right) P_C + \frac{1}{k}.\end{aligned}\tag{3.7}$$

In einem quantenmechanischen Protokoll kann das zusätzliche Bit verwendet werden, um mitzuteilen, ob die eigene Messung erfolgreich war. Jede Partei beginnt nur dann mit dem quantenmechanischen Protokoll, wenn die Messungen bei allen Parteien erfolgreich waren. Die Erfolgswahrscheinlichkeit dieses Protokolls ist

$$\tilde{P}'_Q = \eta^{kn} V P_Q + (1 - \eta^{kn}) P_C + (1 - V) \eta^{kn} \frac{1}{2}\tag{3.8}$$

Wegen  $P_Q \geq P_C$  gilt  $\tilde{P}'_Q \geq P_C$ , allerdings muss  $\tilde{P}'_Q$  mit  $\tilde{P}_C$  verglichen werden, da auch dem klassischen Protokoll ein Bit zusätzliche Kommunikation zur Verfügung steht. Auflösen der Bedingung  $\tilde{P}'_Q = \tilde{P}_C$  nach  $\eta$  liefert die neue minimale Detektoreffizienz

$$\tilde{\eta}_{\min} = \left( \frac{2}{k} \frac{P_2 - P_C}{2(P_Q V - P_C) + 1 - V} \right)^{\frac{1}{nk}},\tag{3.9}$$

jetzt also mit dem einen Bit zusätzlicher Kommunikation. Die Bedingung  $\tilde{\eta}_{\min} > \eta_{\min}$  ist für manche Werte von  $P_Q$ ,  $P_C$  und  $k$  erfüllt. In diesem Bereich bietet Kommunikation also dem quantenmechanischen Protokoll einen Vorteil in dem Sinne, dass es dann eine niedrigere Detektoreffizienz benötigt. Abbildung 3.5 zeigt diesen Bereich exemplarisch für  $V = 0.9$ . Ein Protokoll aus diesem Bereich betrachtet das folgende Beispiel.

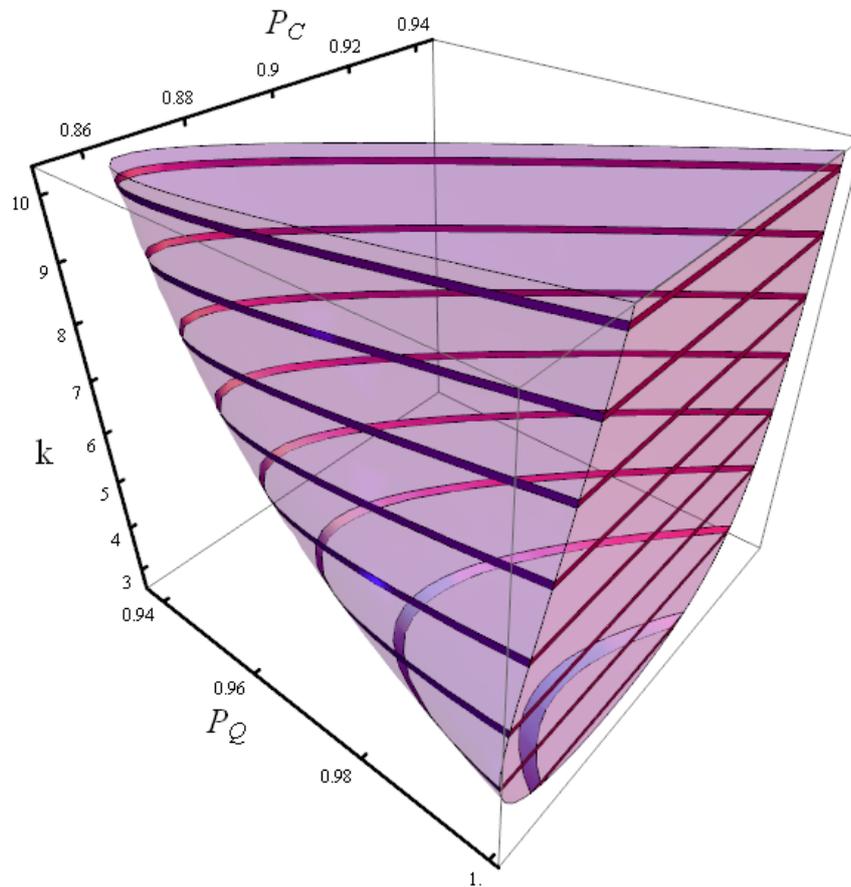


Abbildung 3.5: Für Protokolle mit klassischer Erfolgswahrscheinlichkeit  $P_C$  und quantenmechanischer Erfolgswahrscheinlichkeit  $P_Q$ , die innerhalb des eingezeichneten Bereichs liegen, lohnt sich ein Bit zusätzliche Kommunikation für das quantenmechanische Protokoll mit nichtidealen Detektoren. Damit ist gemeint, dass bei  $k$ -mal wiederholtem Durchführen des Protokolls mit unabhängigem Input ein Protokoll mit insgesamt  $k + 1$  Bit erlaubter Kommunikation pro Partei eine geringere Detektoreffizienz benötigt um alle klassischen Protokolle zu schlagen als das ursprüngliche Protokoll. Annahmen über die klassische Erfolgswahrscheinlichkeit beschreibt der Text. Der Kontrast ist  $V = 0.9$ .

**Beispiel 3.4**

Sei

$$f = \text{sgn}(g(x_1, x_2, x_3))$$

die von drei Parteien zu berechnende Funktion,  $x_i \in \{0, 1\}$  und

$$g(x_1, x_2, x_3) = \left(x_1 + \frac{1}{3}\right) \cos\left(\frac{\pi}{2}(x_1 + x_2 + x_3)\right).$$

Eine Strategie, die das Maximum von Gleichung 1.2 liefert besteht darin, alle  $a_i(x_i) = -1$  zu wählen. Die Schranke ist also

$$B = - \sum_{x_1, x_2, x_3=0}^1 g(x_1, x_2, x_3) = \frac{8}{3}.$$

Die klassische Erfolgswahrscheinlichkeit ist  $P_C = 0.9$ , die quantenmechanische  $P_Q = 1$ . Zunächst werde keine zusätzliche Kommunikation erlaubt. Für  $V = 0.9$  muss hier  $\eta > 0.961481$  sein, damit  $P'_Q > P_C$ . Der Kontrast ist nicht willkürlich, er muss größer als 0.85 sein, damit das Beispiel das gewünschte Ergebnis zeigt. Es werden nun  $k = 6$  Wiederholungen des Protokolls durchgeführt und mit einem zusätzlichen Bit mitgeteilt, ob das klassische oder das quantenmechanische Protokoll verwendet werden soll. Letzteres nur, wenn alle Detektionen erfolgreich waren. Jetzt ist die neue Erfolgswahrscheinlichkeit wie in Gleichung 3.8. Da  $P_C$  nahe an Eins ist, ist die Annahme, dass mit einem weiteren Bit Kommunikation  $P_2 = 1$  gilt, plausibel. Damit  $\tilde{P}'_Q > \tilde{P}_C$  gilt, das neue Protokoll also besser ist als klassisch möglich, muss  $\eta > 0.940791$  sein. Um eine Überlegenheit gegenüber klassischen Protokollen zu zeigen benötigt das neue Protokoll also eine geringere Detektoreffizienz.

Auf Abbildung 3.6 sieht man, dass der Bereich für  $V = 0.9$  nicht vollständig in dem Bereich für  $V = 0.99$  enthalten ist. Vorausgesetzt es gilt  $P_2 = 1$  bedeutet dies, dass es Protokolle gibt, für die sich zusätzliche Kommunikation bei  $V = 0.9$  lohnt, nicht aber bei  $V = 0.99$ . Die folgende Funktion ist ein Beispiel dafür.

**Beispiel 3.5**

Die Regeln sind wie in Beispiel 3.4. Nur die Funktion  $g$  ist jetzt

$$g(x_1, x_2, x_3) = (x_1 + 0.62) \cos\left(\frac{\pi}{2}(x_1 + x_2 + x_3)\right) + 0.05 \begin{cases} 1 & \text{für } x_1 \geq x_2 \geq x_3 \\ -1 & \text{sonst} \end{cases}.$$

Um ein gewünschtes Paar  $P_Q$  und  $P_C$  zu erhalten, können Funktionen mit unterschiedlichen Eigenschaften passend gemischt werden. Die Funktion  $g$  besteht hier aus drei Bausteinen. Der Teil  $x_1 \cdot (\cdot)$  hat für sich  $P_C = P_Q = 1$ . Der Teil mit Kosinus ist eine Bellsche Ungleichung mit  $P_Q = 1$ . Der dritte Teil hat für sich  $P_C = P_Q = 3/4$ . Die Position im  $P_C$ - $P_Q$ -Raum dieses Beispiels zeigt Abbildung 3.7.

**3.4 Das Toner-Bacon-Modell**

Während Bellsche Ungleichungen verwendet werden um zu zeigen, dass Korrelationen von lokalen Messungen an einem Quantensystem nicht durch lokalrealistische Theorien erklärt werden können, kann man sich auch die Frage stellen, wieviel klassische Kommunikation

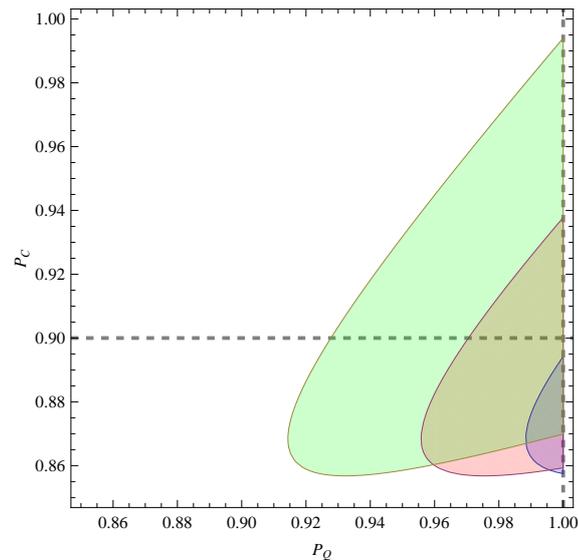


Abbildung 3.6: Die in Beispiel 3.4 auftauchenden Werte von  $P_C = 0.9$  und  $P_Q = 1.0$  sind in diesem Diagramm markiert. Die blaue ( $V = 0.84$ ), rote ( $V = 0.9$ ) und grüne ( $V = 0.99$ ) Kontur begrenzen den Bereich innerhalb dessen das neue Protokoll bei  $k = 6$  Wiederholungen eine geringere Detektoreffizienz als das Alte benötigt um eine Überlegenheit gegenüber klassischen Protokollen zu zeigen. Das Beispiel liegt ausserhalb des blau markierten Bereiches, was bedeutet, dass bei diesem Kontrast kein Vorteil durch zusätzliche Kommunikation entsteht. Die angenommene klassische Erfolgswahrscheinlichkeit  $\tilde{P}_C$  ist in Gleichung 3.7 angegeben.

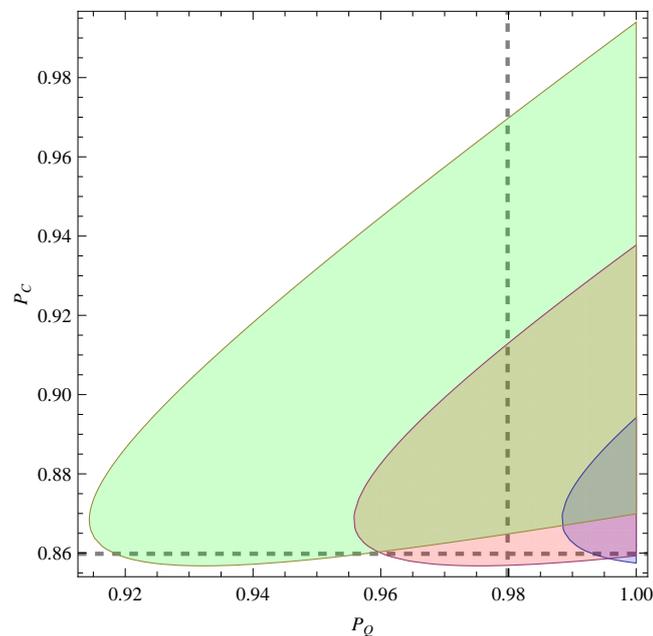


Abbildung 3.7: Position des zweiten Beispiels ( $P_C = 0.86$ ,  $P_Q = 0.98$ ). Die blaue ( $V = 0.84$ ), rote ( $V = 0.9$ ) und grüne ( $V = 0.99$ ) Kontur begrenzen den Bereich innerhalb dessen das neue Protokoll bei  $k = 6$  Wiederholungen eine geringere Detektoreffizienz als das Alte benötigt um eine Überlegenheit gegenüber klassischen Protokollen zu zeigen. Die angenommene klassische Erfolgswahrscheinlichkeit  $\tilde{P}_C$  ist in Gleichung 3.7 angegeben.

erforderlich ist, um diese Korrelationen ohne Verschränkung zu produzieren.

Toner und Bacon haben in [29] gezeigt, dass dafür schon ein einziges Bit Kommunikation genügt. Dafür teilen sich Alice und Bob zwei Zufallsvektoren  $\vec{\lambda}_1$  und  $\vec{\lambda}_2$  die gleichmäßig über die Einheitskugel verteilt sind. Sie wollen Messwerte produzieren, die wie zwei Messungen eines Singlett-Zustandes in Richtungen  $\vec{a}$  und  $\vec{b}$  korreliert sind. Das Protokoll besteht nun aus folgenden drei Schritten.

1. Alice gibt  $\alpha = -\text{sgn}(\vec{a} \cdot \vec{\lambda}_1)$  aus.
2. Alice sendet Bob  $c = \text{sgn}(\vec{a} \cdot \vec{\lambda}_1)\text{sgn}(\vec{a} \cdot \vec{\lambda}_2)$ .
3. Bob gibt  $\beta = \text{sgn}(\vec{b} \cdot (\lambda_1 + c\lambda_2))$  aus.

Der Erwartungswert der beiden ausgegebenen Zahlen ist  $\langle \alpha\beta \rangle = -\vec{a} \cdot \vec{b}$ , genau wie bei einer quantenmechanischen Messung (Beweis siehe [29]).

Da ein Bit Kommunikation ausreicht, um eine quantenmechanische Messung zu simulieren und das oben besprochene quantenmechanische Protokoll zu Kommunikationskomplexitätsproblemen auf diesen Messungen beruht, kann die Erfolgswahrscheinlichkeit  $P_Q$  mit einem zusätzlichen Bit Kommunikation pro Partei immer erreicht werden. Mit dem ersten Bit wird die quantenmechanische Messung simuliert, mit dem zweiten Bit wird das quantenmechanische Protokoll durchgeführt. Das heisst  $\tilde{P}_C \geq P_Q$  für  $n = 2$  Parteien (also auch  $S \leq B_A$  für zwei Bit Kommunikation).

# Kapitel 4

## Diskussion

Die vorliegende Arbeit behandelt Probleme der Quantenkommunikationskomplexität der folgenden Form. Es gebe eine binäre Funktion  $f$  mit  $n$  Argumenten, die jeweils aus  $m$  Bit bestehen. Dieser Input wird gleichmäßig auf  $n$  räumlich getrennte Parteien verteilt. Deren gemeinsame Aufgabe ist es die Funktion  $f$  zu berechnen. Dazu ist ihnen aber nur eine begrenzte Anzahl Bits Kommunikation erlaubt. Gefragt ist nach der maximalen Wahrscheinlichkeit, mit der die Parteien das richtige Ergebnis bekannt geben.

In Kapitel 2 wurde gezeigt, wie aus der Schranke einer Bellschen Ungleichung für  $n$  Parteien und  $m$  verschiedene Messeinstellungen mit jeweils zwei möglichen Messergebnissen die Erfolgswahrscheinlichkeit für ein passendes Kommunikationskomplexitätsproblem folgt. Dies ist eine direkte Verallgemeinerung der Ergebnisse von [7] auf  $m$  Messeinstellungen. Die Verallgemeinerung auf mehr als ein Bit Kommunikation pro Partei wurde angedeutet wo es sich ohne Mühe ergab. Dieser Punkt ließe sich in weiteren Forschungen ausarbeiten (siehe Bemerkung in [7]). Anschließend wurden Beispiele zu Bellschen Ungleichungen angegeben, die zu Standardproblemen der Kommunikationskomplexität (Größer-Gleich, Inneres Produkt und Disjunktheit) passen. Die Größer-Gleich-Funktion und Disjunktheit wurden meines Wissens noch nicht innerhalb im Rahmen der Kommunikationskomplexität mit Verschränkung behandelt.

Mit Hilfe der in Kapitel 2 erarbeiteten Zusammenhänge wurde in Kapitel 3 die Detektoreffizienz untersucht, die benötigt wird um einen quantenmechanischen Vorteil gegenüber klassischen Kommunikationskomplexitätsprotokollen zu ermöglichen. Dazu wurde zunächst ein Protokoll verwendet, welches in [11] beschrieben wird: Die Parteien beginnen mit dem quantenmechanischen Protokoll, d.h. sie führen die Messungen entsprechend ihres Inputs durch. Sollten diese Messungen scheitern können sie das Messergebnis nicht senden. Stattdessen senden sie das Bit des optimalen klassischen Protokolls. Auf diese Weise ist das Protokoll auch erfolgreich wenn alle Messungen scheitern. Davon ausgehend wurden verschiedene Aspekte der Quantenkommunikationskomplexität mit nichtidealen Detektoren untersucht. Die wichtigsten Punkte davon sind:

- Die benötigte Detektoreffizienz  $\eta_{\min}$  für das oben beschriebene Quantenkommunikationskomplexitätsprotokoll hängt mit der kritischen Detektoreffizienz  $\eta_{\text{crit}}$  zum Schließen des Detektor-Schlupfloches über  $\eta_{\text{crit}} \leq \eta_{\min}$  zusammen. Dies wurde in Abschnitt 3.1 bewiesen, indem eine Bell-Ungleichung angegeben wurde, die Nichtdetektion als Ergebnis 0 berücksichtigt und ab der Detektoreffizienz  $\eta_{\min}$  verletzt wird.
- Es wurde begründet, warum im Fall von zwei Parteien und vielen Messeinstellungen ein quantenmechanischer Vorteil schon bei sehr niedriger Detektoreffizienzen möglich scheint. Ein Protokoll für zwei Parteien mit  $\eta_{\min} < 83\%$ , was also eine kleinere

Detektoreffizienz als die CHSH-Ungleichung benötigt, konnte aber nicht gefunden werden. Wegen der Relevanz für eventuelle experimentelle Realisierungen, insbesondere mit Photonen als Qubits, könnten sich hier weitergehende Forschungen lohnen. Ein möglicher Ausgangspunkt ist [30]. Hier konnte die benötigte Detektoreffizienz zum schließen des Detektor-Schlupfloches verbessert werden, indem Zustand und Messeinstellungen für eine bestimmte Detektoreffizienz optimiert wurden. Es zeigt sich, dass dann nicht mehr maximal verschränkte Zustände optimal sind.

- Es wurde gezeigt, dass das zur Mermin-Ungleichung gehörende Kommunikationskomplexitätsproblem eine geringere Detektoreffizienz ( $\eta_{\min} \approx 71\%$ ) als bei der CHSH-Ungleichung ( $\eta_{\min} \approx 83\%$ ) benötigt.
- Weiter wurde untersucht, ob zusätzliche Kommunikation einen Vorteil für quantenmechanische Protokolle darstellen kann. Dort können die Parteien dann mitteilen, ob ihre Messungen erfolgreich waren. Es wurde der Fall betrachtet, dass für  $k$  Wiederholungen des Protokolls ein zusätzliches Bit Kommunikation pro Partei erlaubt wird. Unter Annahme einer plausiblen Erfolgswahrscheinlichkeit mit dieser zusätzlichen Kommunikation im klassischen Fall konnte diese Frage positiv beantwortet werden. Dafür wurden Beispiele angegeben, aber auch der Bereich der Parameter  $P_Q$  (ideale quantenmechanische Erfolgswahrscheinlichkeit),  $P_C$  (klassische Erfolgswahrscheinlichkeit ohne zusätzliches Bit) und  $k$  (Anzahl Wiederholungen) in dem eine niedrigere Detektoreffizienz für eine quantenmechanische Überlegenheit gegenüber dem Fall ohne zusätzliche Kommunikation benötigt wird.



# Danksagung

Ich möchte meinem Betreuer Prof. Dr. Caslav Brukner meinen herzlichen Dank aussprechen. Mit seinem Gespür für die wissenschaftlich interessanten Punkte hat er meine Forschung so gelenkt, dass ich im nachhinein mit großer Zufriedenheit auf die gemachten Erfahrungen zurückblicke. Durch die freundliche Atmosphäre in der Gruppe und seine unkomplizierte Art habe ich mich sehr wohlfühlt.

Ich danke den PhD-Studenten und meinem Bürokollegen B.Sc. Matthias Kaiser für die anregenden Diskussionen. Für interessante Gespräche über das Thema der Arbeit und Tipps bei Beweisen danke ich meinem Freund Dipl.-Math. Thomas Leßmann.

Meinen Eltern danke ich für ihre vielseitige Hilfe während meines Studiums in Wien. Unter anderem hat ihre finanzielle Unterstützung mein Studium an der Universität Wien erst möglich gemacht.

# Literaturverzeichnis

- [1] A. Einstein, B. Podolsky und N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev. 47 777 (1935)
- [2] J. S. Bell, *On the Einstein Podolski Rosen Paradox*, Physics Vol. 1, No. 3, 195-200 (1964)
- [3] S. Barz, *Eine Quelle polarisationsverschränkter Photonenpaare für das physikalische Praktikum für Fortgeschrittene*, Examensarbeit Universität Mainz (2008)
- [4] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter und A. Zeilinger, *Violation of Bell's inequality under strict Einstein locality conditions*, Phys. Rev. Lett. 81, 5039-5043 (1998)
- [5] A. Zeilinger et al., *Violation of local realism with freedom of choice*, Proc Natl Acad Sci USA., Vol. 107(46): 19708-19713 (2010)
- [6] D. M. Greenberger, M. A. Horne, A. Shimony, A. Zeilinger, *Bell's theorem without inequalities*, Am. J. Phys. 58, Nr. 12, S. 1131-1143 (1990)
- [7] C. Brukner, M. Zukowski, J. Pan und A. Zeilinger, *Bell's Inequalities and Quantum Communication Complexity*, Physical Review Letters, Vol. 92, No. 12 (2004)
- [8] R. Cleve, W. van Dam, M. Nielsen und A. Tapp, *Quantum Entanglement and the Communication Complexity of the Inner Product Function*, Lect. Notes Comput. Sci. 1509, 61-74 (1998)
- [9] L. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) S. 212 (1996)
- [10] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing. 26/1997, S. 1484-1509 (arXiv:quant-ph/9508027) (1997)
- [11] R. Predevel, M. Aspelmeyer, C. Brukner, T. D. Jennewein und A. Zeilinger, *Photonic entanglement as a resource in quantum computation and quantum communication*, JOSA B, Vol. 24, Issue 2, pp. 241-248 (2007)
- [12] G. Copacean, M. Epping und P. Schiаны, *Versuchsprotokoll Bell-Ungleichung*, Universität Wien, Praktikumsprotokoll (2011)
- [13] E. Kushilevitz und N. Nisan, *Communication Complexity*, Cambridge University Press (1996)

- [14] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Zukowski und H. Weinfurter, *Experimental quantum communication complexity*, Phys. Rev. A 72 (2005)
- [15] J. Zhang, X. Bao, T. Chen, T. Yang, A. Cabello und J. Pan, *Experimental "Guess my number" protocol using multiphoton entanglement*, Phys. Rev. A 75 (2007)
- [16] Laser Components, *Single Photon Counting Module COUNT-Series*, Datenblatt zur Produktreihe, abgerufen von <http://www.lasercomponents.com> (2012)
- [17] J. Yngvason, *Quantenmechanik II*, Skriptum zur Vorlesung an der Universität Wien (2011)
- [18] M. Hinterhöller, *Poppers kritischer Realismus: Realismus und Induktionskritik im Werk von K. R. Popper: Nach einem Aufsatz von H. Fetz und Texten von K. 2 R. Popper*, Grin Verlag (2010)
- [19] M. Zukowski, *Quantum Theory and Quantum Information: an Introduction to „Paradoxes“ and their Applications*, Vorlesung an der Universität Wien (2010)
- [20] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000)
- [21] S. Kochen and E.P. Specker, *The problem of hidden variables in quantum mechanics*, Journal of Mathematics and Mechanics 17, 59-87 (1967)
- [22] D. Bohm, *A Suggested Interpretation of the Quantum Theory in Terms of „Hidden“ Variables. II*, Phys. Rev. 85, 180-193 (1952)
- [23] D. Bacon und B. Toner, *Bell Inequalities with Auxiliary Communication*, Physical Review Letters, Vol. 90, No. 15 (2003)
- [24] A. Garg und N. D. Mermin, *Detector inefficiencies in the Einstein-Podolsky-Rosen experiment*, Phys. Rev. D, Vol. 35, No. 12 (1987)
- [25] S. Gröblacher, T. Paterek, R. Kaltenbaek, C. Brukner, M. Zukowski, M. Aspelmeyer und A. Zeilinger, *An experimental test of non-local realism*, Nature, Vol. 446, S. 871-875 (2007)
- [26] A. Cabello, J. Larsson und D. Rodriguez, *Minimum detection efficiency required for a loophole-free violation of the Braunstein-Caves chained Bell inequalities*, Phys. Rev. A, 79 (2009)
- [27] A. Cabello, D. Rodriguez und I. Viallanueva, *Necessary and Sufficient Detection Efficiency for the Mermin Inequalities*, Physical Review Letters, Vol. 101, No. 12 (2008)
- [28] G. Brassard, *Quantum Communication Complexity (a survey)*, ISMVL, S. 56, (2004)
- [29] B. Toner und D. Bacon, *The Communication Cost of Simulating Bell Correlations*, Phys. Rev. Lett. 91, 187904 (2003)
- [30] P. H. Eberhard, *Background level and counter efficiencies required for a loophole-free Einstein-Podolski-Rosen experiment*, Physical Review A, Vol. 47, No. 2 (1992)

# Anhang

## A Zusammenfassung

In dem Forschungsgebiet der Quanteninformation werden Auswirkungen der Quantentheorie auf die klassische Informationstheorie untersucht. Diese schließen Quantenkommunikation, Quantenkryptographie und Quanteninformationsverarbeitung (zum Beispiel mit Quantencomputern) ein. In dieser Arbeit werden Fragestellungen der Quantenkommunikationskomplexität behandelt. In der hier betrachteten Variation von Kommunikationskomplexitätsproblemen wird die Wahrscheinlichkeit untersucht, mit der eine binäre Funktion richtig berechnet werden kann, dessen Argumente auf mehrere Parteien verteilt sind. Die Kommunikation zwischen den Parteien ist eingeschränkt. In der Quantenkommunikationskomplexität wird nun der Vorteil untersucht, der entsteht, wenn die Parteien Messungen an Teilen eines verschränkten Systems durchführen dürfen. In dieser Arbeit werden  $n$  Parteien betrachtet, die jeweils  $m$  Bit Input erhalten. Dafür wird ein Zusammenhang zu Bell-Ungleichungen mit  $n$  Teilchen und je  $m$  Messeinstellungen mit zwei Messergebnissen hergestellt. Die Messungen können wegen nichtidealen Detektoren scheitern. Es wird untersucht, wie effizient die Detektoren sein müssen, damit ein Vorteil durch Verschränkung entsteht. Diese benötigte Detektoreffizienz kann unter bestimmten Umständen kleiner sein, wenn zusätzliche Kommunikation erlaubt wird. Außerdem wird ein Zusammenhang mit der kritischen Detektoreffizienz des Detektorschlupfloches in Bell-Experimenten hergestellt.

## B Abstract

Research in quantum information science focuses on the impact of quantum theory on information science. This includes quantum communication, quantum cryptography and quantum computing. The present thesis discusses questions related to quantum communication complexity. Consider the problem of calculating a binary function of several inputs which are distributed to separated parties. The communication between those parties is restricted. In this thesis the success probability for the parties to give the correct value of the function is analyzed. The possibility to increase this success probability by the use of entanglement is studied in the area of quantum communication complexity. In this work each of the  $n$  parties receive  $m$  bits input. The success probability is calculated by linking it to Bell inequalities for  $n$  particles,  $m$  measurement settings and two outcomes. The quantum protocol includes measurements which can fail due to imperfect detectors. Here the detector efficiency required for an improvement over classical protocols is calculated. Under certain circumstances this minimal detector efficiency can be lower when additional communication is allowed. Furthermore a link to the critical detector efficiency needed to close the detection loophole in a Bell test experiment is established.

## C Notationsübersicht

Zeichen	erstes Auftauchen im Text	Erklärung
$\otimes$	Abschnitt 1.1	Tensorprodukt
$\bar{\cdot}$	Abschnitt 1.1	komplexe Konjugation
$\mathcal{A}_i(x_i)$	Abschnitt 1.1	$x_i$ -te Observable der $i$ -ten Partei
$A$	Abschnitt 1.4	Antwortfunktion eines Protokolls
$a_i(x_i)$	Definition 1.2	Messergebnis der $x_i$ -ten Observablen der $i$ -ten Partei (in einer realistischen Theorie)
$B$	Gleichung 1.3	Lokalrealistische Schranke
$E$	Abschnitt 1.1	Erwartungswert quantenmechanisch bzw. klassisch
$f$	Abschnitt 1.4, Gleichung 2.1	von den Parteien zu berechnende Funktion
$g$	Gleichung 1.2	Koeffizienten der Bellschen Ungleichung
LRT	Abschnitt 1.2	Lokalrealistische (=klassische) Theorie
$P_C$	Satz 2.1	beste klassische Erfolgswahrscheinlichkeit
$P_Q$	Gleichung 2.7	quantenmechanische Erfolgswahrscheinlichkeit
$ \psi\rangle$	Abschnitt 1.1	präparierter (reiner) Zustand
$Q$	Gleichung 2.3	Wahrscheinlichkeitsverteilung der Inputs
$\rho$	Abschnitt 1.1, Definition 3.1	Dichtematrix des Zustandes
$S$	Definition 1.6	Bell-Parameter
$\text{sgn}(\cdot)$	Gleichung 2.2	Vorzeichen-Funktion
$\Sigma$	Gleichung 2.3	Normierungsfaktor der Wahrscheinlichkeitsverteilung $Q$
$\vec{\sigma}$	Abschnitt 1.1	Vektor der Pauli-Matrizen
$X$	Abschnitt 1.1	erste Pauli-Matrix
$Y$	Abschnitt 1.1	zweite Pauli-Matrix
$Z$	Abschnitt 1.1	dritte Pauli-Matrix

## D Algorithmus zum Berechnen der klassischen Schranke für zwei Parteien

Es wird nur der Fall von zwei Parteien betrachtet. Ein naiver Algorithmus um die klassische Schranke zu berechnen besteht darin, alle möglichen Messwerte durchzugehen, die Summe zu bilden und das Maximum zu ermitteln. Für eine feste Wahl der Messwerte der ersten Partei ist die Wahl der Messwerte von Partei Zwei klar: Die Messwerte werden genau so gewählt, dass jede Spalte positiv ist. Deswegen werden die Spaltensummen betragsmäßig aufsummiert.

---

### Algorithmus 1 SimpleBound-Algorithmus

---

```

1: function s(i,n) ▷ i-tes Bit von n gesetzt?
2:   if n & 2i then
3:     return 1
4:   else
5:     return -1
6:   end if
7: end function
8: function SIMPLEBOUND(g) ▷ Klassische Schranke von  $\sum gE$ 
9:   max ← 0
10:  grenze ← 2M
11:  for 0 ≤ n < grenze do ▷ Für alle Strategien von Alice
12:    sum ← 0 ▷ Bilde sum =  $\sum gE$ 
13:    for 0 ≤ j < M do
14:      ssum ← 0
15:      for 0 ≤ i < M do
16:        ssum ← ssum + gij · s(i, n)
17:      end for
18:      sum ← sum + abs(ssum)
19:    end for
20:    if sum > max then ▷ und finde Maximum
21:      max ← sum
22:    end if
23:  end for
24:  return max
25: end function

```

---

## E Mögliche Messwerte zur CHSH-Ungleichung

Tabelle 1 zeigt simulierte Messwerte im Belleexperiment für die CHSH-Ungleichung für verschiedene Detektoreffizienzen. In einem realen Experiment werden die Koinzidenzraten der beiden Detektoren gemessen. Die gezeigten Daten sollen zum besseren Verständnis des Detektor-Schlupflochs beitragen. Die CHSH-Ungleichung wird sowohl für  $\eta = 0.5$  ( $S = 3.1 \pm 0.4$ ) als auch für  $\eta = 0.9$  ( $S = 3.0 \pm 0.2$ ) verletzt. Die auf die gesamten Messdaten erweiterte Ungleichung wird für  $\eta = 0.9$  verletzt ( $S = 2.3 \pm 0.2$ ), aber nicht für  $\eta = 0.5$  ( $S = 1.1 \pm 0.2$ ).

Tabelle 1: Simulierte Messwerte für unterschiedliche Detektoreffizienzen. Eine 0 als Messergebnis steht für Nichtdetektion. Die Observablen  $\mathcal{A}_{x_1}$  bzw.  $\mathcal{A}_{x_2}$  sind optimal bzgl.  $S$  gewählt.

(a) $\eta = 0.5$								(b) $\eta = 0.9$							
$x_1$	$x_2$	$a_1$	$a_2$	$x_1$	$x_2$	$a_1$	$a_2$	$x_1$	$x_2$	$a_1$	$a_2$	$x_1$	$x_2$	$a_1$	$a_2$
0	1	0	1	0	0	-1	1	0	1	0	1	1	0	0	-1
0	1	-1	0	0	0	1	-1	0	1	1	1	0	0	1	-1
0	0	-1	1	0	1	-1	0	0	0	1	-1	0	0	1	-1
0	1	1	-1	1	1	0	-1	1	1	1	1	0	0	-1	1
0	0	0	-1	0	0	0	1	1	1	1	1	1	1	-1	-1
1	1	-1	-1	1	0	0	1	0	1	1	1	0	1	1	1
0	1	-1	-1	1	1	0	0	1	1	-1	-1	1	1	-1	-1
0	0	0	1	1	1	0	0	1	1	-1	-1	0	1	-1	-1
1	0	-1	0	1	0	-1	1	1	1	1	1	0	1	1	1
0	1	0	-1	1	0	1	0	0	1	-1	-1	0	0	-1	1
0	1	-1	-1	1	1	0	-1	0	0	-1	1	1	0	-1	-1
1	1	0	1	0	1	0	-1	1	1	-1	-1	1	1	1	-1
0	1	0	0	1	0	0	1	1	0	-1	-1	0	0	-1	1
0	0	1	-1	1	0	1	0	1	0	-1	0	0	1	-1	1
0	0	-1	1	0	1	0	1	0	1	1	-1	1	0	-1	-1
1	0	0	-1	1	0	0	-1	0	1	1	0	1	0	-1	-1
1	1	-1	-1	1	0	1	1	1	1	1	-1	0	1	-1	-1
0	1	1	1	1	1	-1	-1	0	0	1	-1	1	0	-1	1
1	0	1	0	0	0	-1	1	0	1	0	-1	1	1	-1	-1
0	0	0	1	0	0	0	0	0	0	0	-1	1	0	1	1
1	0	-1	-1	1	0	-1	-1	0	0	0	1	0	1	1	-1
1	0	0	-1	0	1	-1	0	0	0	-1	0	1	0	-1	-1
0	1	0	-1	0	0	0	-1	1	1	1	1	1	0	1	0
1	1	1	0	0	1	0	0	0	1	-1	-1	0	1	0	1
1	1	-1	-1	0	0	0	1	1	1	1	0	0	0	1	-1
1	1	1	0	-1	1	0	1	0	0	1	-1	1	0	0	1
0	1	0	1	1	0	-1	0	0	0	1	-1	0	1	0	1
0	1	0	0	1	0	0	-1	1	1	0	0	1	0	0	1
0	1	0	0	0	1	1	-1	1	0	1	1	0	1	0	-1
1	0	1	1	1	0	1	-1	0	0	-1	1	0	1	-1	0
1	1	1	1	1	1	0	0	0	0	-1	1	1	0	1	-1
0	1	0	0	0	1	1	1	0	1	1	1	0	1	1	1
0	1	-1	-1	0	0	0	0	0	0	1	0	1	0	-1	-1
0	0	-1	1	1	0	1	1	1	0	-1	-1	0	0	-1	1
0	0	-1	0	1	0	1	0	1	0	1	1	1	0	-1	-1
0	0	1	0	1	1	1	0	0	0	1	-1	0	1	-1	-1
1	1	1	0	1	0	1	0	1	1	-1	1	1	0	-1	-1
1	0	-1	-1	0	0	0	1	1	1	0	-1	0	1	1	0
1	1	0	-1	0	1	0	0	0	1	-1	-1	0	1	0	1
1	0	-1	0	0	1	-1	0	0	1	-1	-1	0	1	-1	0
1	0	1	1	0	1	1	1	0	0	1	-1	1	1	1	-1
0	1	0	0	0	1	1	1	1	0	-1	0	1	0	1	0
0	0	-1	0	1	0	0	0	1	1	1	1	1	1	1	1
1	0	0	-1	1	0	1	0	1	1	-1	0	0	1	1	1
0	0	0	0	0	1	0	1	1	0	-1	0	0	0	-1	1
0	0	0	1	1	1	0	0	1	1	1	1	0	1	1	1
1	0	0	0	0	0	1	-1	0	1	1	1	0	0	-1	1
1	1	-1	0	1	1	-1	0	0	0	-1	1	0	1	-1	-1
0	0	1	0	0	0	0	1	1	1	1	1	0	0	-1	-1

## F Beweis zu Abschnitt 3.2.1

Die Bell-Ungleichung zum  $i$ -ten Element der angegebenen Folge von Funktionen  $f_i$  ist  $g_i = g_1^{\otimes i}$ . Sei  $d$  die Dimension von  $g_1$ , hier ist also  $d = 3$ . Weiter sei  $M = d^{i+1}$  die Dimension von  $g_{i+1}$ . Die optimalen Winkel der Bell-Ungleichung mit Koeffizienten  $g_1$  seien  $\phi_0^{A/B}, \dots, \phi_{d-1}^{A/B}$ . Der Zustand sei  $|GHZ\rangle$  und alle Messungen in einer Ebene (was hier optimal ist), sodass der Erwartungswert die Form

$$E_{\cos}(x_1, \dots, x_n) = \cos\left(\sum \varphi_i\right)$$

hat. Im Beweis wird durch ein Additionstheorem

$$E_{\sin}(x_1, \dots, x_n) = \sin\left(\sum \varphi_i\right)$$

auftauchen, was sich nur dadurch vom Erwartungswert unterscheidet, dass der Kosinus durch Sinus ersetzt ist. Mit den Winkeln

$$\phi_{x_{1/2}}^{A/B} = \sum_{k=0}^{i-1} \phi_{\frac{x_{1/2}}{d^k}}^{A/B} \pmod{d}$$

wird der Wert  $S_i = S^i$  für die linke Seite der Bell-Ungleichung erreicht. Beweis geht mit vollständiger Induktion über  $i$ . Die Idee hierbei ist, in der Bellschen Ungleichung die Summation über alle  $x_1, \dots, x_n$  in eine Summation über die Teilblöcke aufzuteilen, deren Größe genau der Größe der Bell-Ungleichung in der Induktionsvoraussetzung entspricht. Es wird  $x_i = du_i + v_i$  geschrieben.  $u_i$  läuft von 0 bis  $M/d - 1$ , zählt also die  $d \times d$ -Blöcke durch.  $v_i$  nimmt die Werte 0 bis  $d - 1$ , zählt also innerhalb der  $d \times d$ -Blöcke durch.

- Induktionsanfang:  $S_1 = S$  gilt per Definition der Winkel  $\phi_0^{A/B}, \dots, \phi_{d-1}^{A/B}$ .
- Induktionsvoraussetzung:  $S_i = S^i$  gilt bis  $i$ .
- Induktionsschritt von  $i \rightarrow i + 1$ :

$$\begin{aligned} S_{i+1} &= \sum_{x_1, \dots, x_n=0}^{M-1} g_{i+1}(x_1, \dots, x_n) E(x_1, \dots, x_n) \\ &= \sum_{u_1, \dots, u_n=0}^{M/d-1} \sum_{v_1, \dots, v_n=0}^{d-1} g_{i+1}(du_1 + v_1, \dots, du_n + v_n) E(du_1 + v_1, \dots, du_n + v_n) \\ &= \sum_{u_1, \dots, u_n} \sum_{v_1, \dots, v_n} g_i(u_1, \dots, u_n) g(v_1, \dots, v_n) E(du_1 + v_1, \dots, du_n + v_n) \\ &= \sum_{u_1, \dots, u_n} g_i(u_1, \dots, u_n) \left( \underbrace{E(du_1, \dots, du_n) \sum_v g(v) E(v)}_{=S} - \underbrace{E_{\sin}(du) \sum_v g(v) E_{\sin}(v)}_{=0} \right) \\ &= S \sum_{u_1, \dots, u_n} g_i(u_1, \dots, u_n) E(du_1, \dots, du_n) \\ &= S \sum_{u_1, \dots, u_n} g_i(u_1, \dots, u_n) E(u_1, \dots, u_n) = SS_i = SS^i = S^{i+1} \end{aligned}$$

# Lebenslauf

## Michael Epping

Geboren am 11. August 1987 in Arnsberg

Adresse Tendlergasse 12 / 112  
1090 Wien

Staatsbürgerschaft Deutsch

Eltern Josef Epping  
Hedwig Epping

Geschwister Drei Schwestern, ein Bruder

## Ausbildung

1993-1997 Grundschule

Juni 2006 Abitur am St.-Ursula-Gymnasium, Arnsberg

Juli 2006 - Juli 2007 Grundwehrdienst

Juli 2010 Bachelor of Science (Physik), erlangt an der Universität Siegen

seit Oktober 2010 Studium an der Universität Wien, Studienziel: Master of Science im Fach Physik

Wien, 6. Februar 2012